FinRegLab

The Use of Cash-Flow Data in Underwriting Credit

Market Context & Policy Analysis

FEBRUARY 2020

About FinRegLab

FinRegLab is a non-profit research organization that was founded on the premise that independent, rigorous research is a primary ingredient in helping develop market norms and policy solutions that enable responsible innovation in financial services.

Acknowledgments

This report, *The Use of Cash-Flow Data in Underwriting Credit: Market Context & Policy Analysis*, and the accompanying *Policy Overview* were made possible through founding support from Flourish/Omidyar Network. Additional support was provided by the Milken Institute, which enabled FinRegLab to evaluate cash-flow data in small business credit underwriting. Detailed information on our funders can be found on the inside back cover.

We would like to extend a special note of appreciation for their leadership and facilitation of FinRegLab's policy working groups to Melanie Brody, Mayer Brown; Mark Schultz, Capital One; P-R Stark, Oliver Wyman; and Corey Stone, Financial Health Network. Thanks also to the Fintech Team at the Federal Reserve Bank of San Francisco for co-hosting a symposium entitled "The Role of Consumers in the Data Ecosystem."

FinRegLab would also like to recognize the individuals and organizations who participated in the policy working groups as listed in Appendix A, the participants of the Data Ecosystem symposium, and stakeholders who participated in interviews.

We are particularly grateful to Marsha Courchane and Arthur Baines, Charles River Associates, for the role they played in designing and executing the empirical research analysis. We are also grateful to Thomas P. Brown and Stephen J. Bandrowsky, Paul Hastings, for legal assistance throughout the course of the research process.

We would also like to thank the following individuals who provided feedback on this report. They include:

Alex Acree; Mitchell Sandler; Kaitlin Asrow; Melanie Brody & Tori Shinohara, Mayer Brown; Thomas P. Brown, Paul Hastings; Jonah Crane, Klaros Group; Eric Goldberg, Akerman; David Medine, Consultative Group to Assist the Poor; Karen Mills & Annie V. Dang, Harvard Business School; Chuck Muckenfuss, Gibson Dunn; Larry Rosenberger; David Silberman; David Stein, Covington & Burling; Corey Stone, Financial Health Network; Diane Thompson; ChiChi Wu, National Consumer Law Center

We would also like to acknowledge the FinRegLab team who worked on the research, convenings, and reports. They include: Jennifer Chasseur, Kelly Thompson Cochran, Sarada Dhulipala, Aaron Milner, Kerrigan Molland, P-R Stark, Stephen Stolzenberg, and Michelle Wu.

CONTENTS

1. EXECUTIVE SUMMARY

As digital information has exploded in the past 15 years, the U.S. financial sector has accelerated its search for "alternative" or "non-traditional" data to strengthen credit underwriting. One of the most promising sources is cash-flow information, particularly data from deposit and prepaid accounts. Because the data shows inflows, outflows, and reserves, it can provide a more detailed and timely picture of how applicants manage their finances than traditional credit reports.

This information could be vital for millions of consumers and small businesses that struggle to access affordable credit because of information barriers. Approximately 20 percent of U.S. consumers lack sufficient traditional credit history to predict their repayment risk using traditional scoring models.[1] Millions of small businesses also struggle to access credit because they have not yet built financial track records.[2] And even for more established applicants, traditional credit reports only reflect certain information for particular types of debts. A more complete picture of applicants' finances can potentially help lenders better differentiate risks, particularly when deciding whether and on what terms to extend credit to borrowers with non-prime credit scores.

Cash-flow data is also increasingly easy to access in electronic form. Approximately 96 percent of U.S. households have bank, credit union, or prepaid accounts, and small businesses are generating increasing amounts of data through checking accounts, accounting software, and payment processing systems.[3] In addition, intermediaries called data aggregators have emerged as the hub of a new system to transmit account data at customers' direction to support a broad range of financial products and services, including credit. As of 2019, that system reportedly can obtain data from at least 95 percent of U.S. deposit accounts.[4]

These developments suggest that widescale adoption of cash-flow data in credit underwriting could produce substantial benefits for borrowers and lenders alike, most notably by:

- **Expanding access to credit**: Because of its scope and greater availability relative to traditional credit reports, cash-flow data has the potential to facilitate extending credit to

1 Consumer Financial Protection Bureau, Data Point, Credit Invisibles 4-6 (2015).

2 FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Small Business Spotlight 4-11 (2019).

3 Federal Deposit Insurance Corporation, 2017 FDIC National Survey of Unbanked and Underbanked Households 1, 7, 9-11, 12, table ES.5, 34-38, 48-58 (2018); FinRegLab, Small Business Spotlight at 11-12.

4 Michael Deleon, A Buyer's Guide to Data Aggregation, Tearsheet (Feb. 19, 2019); Ron Miller, Plaid Expands Financial Service API to Include All US Banks, techcrunch.com (Feb. 5, 2019).

applicants who would otherwise be rejected, open substantial new markets to lenders, and serve broader societal aims regarding inclusion.

- **Improving risk prediction and lender efficiency:** Improving risk prediction and facilitating more efficient underwriting could have substantial benefits for lenders, for instance by lowering their costs of supplying credit over time, as well as improving portfolio performance and market stability.
- **Enhancing customer-led competition and innovation:** In credit and other markets, empowering consumers and small businesses to transfer their financial data makes it easier to seek out new providers and new products and services. This in turn may create greater urgency for incumbents to improve their product offerings and servicing in order to retain customers.

Yet despite these potential benefits, use of cash-flow data is uneven in U.S. credit markets today. Non-bank fintech companies and some credit reporting and scoring incumbents have developed cash-flow models, and a diverse range of companies have begun using electronic cash-flow data in small business lending. But banks' and credit unions' use of such information is limited in many consumer credit markets, despite their access to account data for their existing customers. Federal regulators issued joint guidance in December 2019 noting the potential benefits of cash-flow data, but it remains to be seen how banks and credit unions will react in light of remaining market and regulatory uncertainties.[5]

FinRegLab has been investigating the use of cash-flow data in credit underwriting by conducting an empirical assessment of its benefits and risks, as well as market and policy analyses of the challenges to its wider adoption. We viewed the project as a useful case study at the intersection of two broader financial innovation trends: (1) the transformation of automated credit underwriting as firms experiment with new data and analytical techniques; and (2) efforts to structure the new data transfer system to enhance customer control and spur greater competition and innovation in financial services markets.

This *Market Context & Policy Analysis* is the third in our series of research reports.[6] It provides detailed snapshots of both the use of cash-flow data in U.S. consumer lending and the development of the system for transferring data between firms, in addition to in-depth analyses of policy and regulatory issues raised by cash-flow underwriting in both consumer and small business credit markets.

The report builds on our previous publications, stakeholder interviews, and the deliberations of three working groups that FinRegLab convened to solicit insights from more than 80 representatives of fintech companies, banks, data aggregators, advocacy organizations, and research institutions. It was also informed by a November 2019 symposium on "The Role of Consumers in the Data Ecosystem" that we co-hosted with the Fintech Team at the Federal Reserve Bank of San Francisco. Stakeholder discussions shaped our understanding of particular issues, but our reports reflect FinRegLab's independent analysis in all respects.

As detailed below, we find the following with regard the use of cash-flow data in consumer and small business credit underwriting:

5 Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration & Office of the Comptroller of the Currency, Interagency Statement on the Use of Alternative Data in Credit Underwriting (Dec. 3, 2019) (hereinafter Interagency Alternative Data Statement).

6 FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (2019); FinRegLab, Small Business Spotlight; Sections 3.1-3.3. A shorter document is being released along with this report to provide an overview of the analyses provided in Sections 5-7 below. FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Policy Overview (2020).

BOX 1.1 OTHER FINREGLAB CASH-FLOW REPORTS

FinRegLab's research on the use of cash-flow data in credit underwriting is summarized in multiple reports:

The ***Empirical Research Findings (2019)*** summarizes our applied research based on data from six non-bank financial services providers—Accion, Brigit, Kabbage, LendUp, Oportun, and Petal—that are using cash-flow data in an effort to provide unsecured, relatively short-term credit to consumers and businesses who may have difficulty obtaining loans from traditional sources. We retained Charles River Associates to help us design and conduct an independent analysis of the participants' cash-flow variables and scores based on actual loan performance. We found compelling evidence that the cash-flow metrics were predictive of credit risk across the diverse set of providers, populations, and products studied.

The ***Small Business Spotlight (2019)*** details the evolution of the use of cash-flow data in small business lending. It explained the reasons why electronic cash-flow data may be particularly useful in the small business context, presented evidence of its increasing use by a diverse range of incumbents and new entrants, and noted market and policy issues that may affect the nature and pace of further expansion.

This ***Market Context & Policy Analysis (2020)*** is being released along with a shorter ***Policy Overview (2020)***. FinRegLab expects to release a fourth report later in 2020 with the Financial Health Network and Flourish to provide a detailed description of existing federal consumer financial laws that implicate credit underwriting and the broader system for customer-permissioned data transfers.

- **Substantial promise:** Our research and outreach indicate that cash-flow data is beginning to expand access to credit and deliver the other benefits discussed above. While its most obvious use in underwriting is to evaluate consumers and businesses that lack traditional credit scores, our research suggests that the information adds meaningful predictive power for a substantially broader swath of applicants. The data could be particularly important for increasing access to credit for African-American and Hispanic populations, though it is not likely to close all gaps in credit availability and use between demographic groups.
- **Challenges to adoption:** Whether cash-flow underwriting can reach scale will depend largely on the extent to which: (1) banks and investors determine that the information is sufficiently useful to warrant changes to their business processes; and (2) lenders of all types are able to secure reliable data access. Although market developments are reducing some operational hurdles, competitive dynamics and coordination challenges are affecting both issues. And open questions with regard to regulatory compliance and liability issues are creating substantial uncertainty in affected markets.
- **Emerging risks:** While the increasing use of cash-flow data in credit underwriting is providing benefits for consumers and small businesses, it also raises privacy tradeoffs and potential concerns about fairness, accuracy, data security, and transparency. These issues are not limited to loan origination, but also can arise in connection with loan servicing and firms' re-use of cash-flow data for other commercial purposes. Although some positive developments are occurring, uncertainty about the application of existing laws and inconsistency among market actors could become an increasing source of risk as the market continues to expand and evolve.
- **Need for action:** The question whether cash-flow underwriting achieves its potential to foster more inclusive, efficient, and competitive markets or whether it evolves in ways that heighten risks and tradeoffs for underserved borrowers will likely depend on how stakeholders respond to several challenging market and policy issues within the next few years. Constructive action by industry, regulators, and Congress may each be needed to improve outcomes with regard to both cash-flow underwriting and the broader data transfer system.

The report analyzes both current initiatives and future options to address these emerging policy issues, including accelerating the adoption of safer and more efficient data transfer technologies, developing processes and tools to foster meaningful customer control over their data, clarifying and strengthening existing customer protections, and increasing supervision of non-bank actors. In the course of analyzing these options, the report also identifies certain cross-cutting questions that have broader implications for innovation in credit underwriting, the system for customer-permissioned data transfers, and other data-driven innovations.

The first question is the potential role for consistent standards—whether developed through market-led efforts, imposed by policymakers, or both—in scaling innovation and increasing customer-friendly competition. While policymakers are often reluctant to intervene too early in emerging innovations for fear of chilling the market, a lack of standards and regulatory certainty can have important implications for the pace at which firms adopt new technologies and processes, for market structure, and for efficiency and transparency for both firms and customers. There are some signs that cash-flow underwriting and more particularly the broader data transfer system are reaching the stage at which some level of standardization with regard to the scope of data, transfer technologies, and business practices could promote greater efficiency and risk mitigation.

A second critical question is the relationship between customer control and customer protection in data use and sharing. The fact that applicants must generally authorize access to their cash-flow data for credit underwriting is a fundamental distinction from the traditional credit reporting system, and many stakeholders view it as an opportunity to empower consumers and small business owners to take a more active role in managing their financial lives. Yet while there is high level support for improving authorization processes and other control mechanisms, stakeholders disagree over particular details and the role that control should play in the broader market. Some suggest that customer control mechanisms could substitute for more traditional protections, while others assert that stronger prescriptive safeguards are also needed as the volume of data sharing increases rapidly.

A third question is the potential need for federal legislation to provide more consistent, comprehensive frameworks to govern different sources of data for credit underwriting, customer-permissioned data transfers for all types of financial services, and/or the use of customer data in financial services more generally. While the financial services sector is heavily regulated relative to general commerce, the major laws governing credit activities and financial data were adopted in much different times. And the border between finance and commerce is eroding. Thus, existing federal protections are not providing a consistent level of protection in the way that consumers may expect. Federal regulators can modernize and increase consistency in some respects, but only Congress can harmonize the underlying structures.

In the near term, the report concludes that increased engagement by federal regulators through research, monitoring, and interpretive activities could be particularly useful, in part by providing sharper focus and greater certainty to industry self-governance and legislative initiatives. In particular, addressing market challenges and customer protection issues in the underlying data transfer system in the next few years could set the stage for more rapid expansion in cash-flow underwriting in years to come. These issues are potentially important for helping beneficial practices to reach scale and for reducing risks to both borrowers and firms.

In the near term, the report concludes that increased engagement by federal regulators through research, monitoring, and interpretive activities could be particularly useful, in part by providing sharper focus and greater certainty to industry self-governance and legislative initiatives.

FinRegLab does not view its role to include advocating for specific policy alternatives, but hopes that these analyses may facilitate deeper and more efficient engagement by private stakeholders and policymakers going forward. The goal is a balanced set of market norms and regulatory requirements that allows both borrowers and firms to benefit from cash-flow data.

Collectively, we believe our research and analyses underscore the importance of focused engagement by all stakeholders to address the policy issues raised by cash-flow underwriting, both for its own sake and as a stepping stone to managing evolution in credit markets and data transfer systems more generally. With thoughtful development, cash-flow underwriting has the potential to benefit borrowers and financial services providers alike. It may also inform and help drive the development of a comprehensive framework to facilitate data-driven innovation in financial services.

2. BACKGROUND

The Promise of Cash-Flow Data

The U.S. credit information system is one of the largest in the world. By providing standardized data about applicants' credit usage and repayment history, it has helped to facilitate a transition to automated underwriting that has lowered lender costs and losses, increased competition, and improved consistency in underwriting over several decades. Yet for all of these benefits, millions of consumers and small businesses still face substantial information barriers in accessing affordable credit.

Such access can play a major role in improving the financial health of individual applicants, both by smoothing short-term gaps between inflows and outflows and by expanding long-term financial capacity through investments in housing, education, transportation, and business expansion. These individual benefits in turn can increase the size and vitality of the national economy, or conversely when credit underwriting is mishandled cause substantial disruption as evidenced by the financial crisis of 2008. In the aftermath of that crisis, financial service providers, consumer advocates, and policymakers have renewed efforts to secure additional information to improve the accuracy and efficiency of credit underwriting.

Cash-flow data is one of the most promising sources of non-traditional information, yet there has been a lack of public research on its efficacy, and adoption rates to date have been uneven. FinRegLab set out to conduct an empirical assessment of the benefits and risks of using cash-flow data in credit underwriting and a policy analysis of issues that may affect the nature and pace of its further adoption.

2.1 Traditional underwriting and credit information flows

Prior to the 1970s, most lending decisions were entrusted to individual loan officers and analysts who evaluated applicants on an individual basis in so-called manual or judgmental underwriting processes. Such processes often consider objective information about applicants' income, expenses, and past repayment history, but it is difficult for them to account consistently for the interaction of many factors simultaneously. Such systems also tend to be labor-intensive and to leave room for personal

bias.[7] Accordingly, as advances in computing and empirical methods permitted, large lenders began developing and relying primarily on automated underwriting systems to make credit decisions.[8]

Improvements in the availability of credit history data were critical to facilitating the transition to automated underwriting. Local credit bureaus had existed since the late 1800s, but consumer credit reporting underwent a period of substantial growth in the 1970s and early 1980s. Several factors contributed to the development of a national credit reporting system, including the adoption of the Fair Credit Reporting Act (FCRA), the emergence of three "nationwide consumer reporting agencies" (the NCRAs), self-governance efforts to standardize both credit reporting inputs and outputs, and rapid expansion of the credit card industry as both a major consumer of and source of credit history.[9] Because credit reports from the NCRAs reflect both current credit obligations and past repayment history, they help lenders assess whether applicants have both the *financial capacity* to repay a new loan and the *willingness* to do so.[10]

Another important development was the spread of so-called credit scoring models that use data from credit reports or other sources to group applicants into bands based on the groups' predicted likelihood of default. In particular, companies such as the Fair Isaac Corporation (FICO) and a joint venture by the NCRAs called VantageScore began producing "generic" credit scores based solely on data in NCRA files.[11] The spread of credit scoring in turn fueled further evolution in automated underwriting, for instance as lenders began to use scores not just to make eligibility determinations but also to implement risk-based pricing systems that charge higher prices to customers who are scored as posing higher risk of default.[12]

Today, consumer credit markets are heavily dependent on credit reports from the three NCRAs—Equifax, Experian, and TransUnion—and on generic credit scores derived from their files. Some sources estimate that these traditional credit scores are used in more than 90 percent of underwriting decisions for mortgages, credit cards, and auto loans.[13] And because they facilitate consistent

7 Board of Governors of the Federal Reserve System, Report to the Congress on Credit Scoring and its Effects on the Availability and Affordability of Credit, 0-4, 3, 10-11 (2007) (hereinafter FRB, Credit Scoring Report). To manage these various risks and disadvantages, such systems often rely on relatively rigid thresholds based on debt-to-income ratios or other individual criteria. If an applicant fails to meet a particular threshold, they are never evaluated against other criteria. *Id.* at 11.

8 *Id.* at O-4, 3, 12-13; FinRegLab, Small Business Spotlight at 5-9.

9 Consumer Financial Protection Bureau, Key Dimensions and Processes in the U.S. Credit Reporting System: A Review of How the Nation's Largest Credit Bureaus Manage Consumer Data 2-3, 7-8 (2012); FRB, Credit Scoring Report at 13-16; Mark Furletti, An Overview and History of Credit Reporting, Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper 3-8 (2002). In addition to the three NCRAs, so-called "specialty CRAs" produce reports that may focus on repayment of specific types of expenses, such as rent or very short-term loans that are not typically reported to the NCRAs. Consumer Financial Protection Bureau, List of Consumer Reporting Companies (2020). The commercial credit reporting market also includes a mix of companies, including Dun & Bradstreet, Equifax, and Experian, as well as various niche bureaus. FinRegLab, Small Business Spotlight at 7.

10 These concepts are often described as the ability and propensity to repay. As discussed further below, however, credit reports do not provide a complete answer to either question since they do not include information about income and assets and may reflect financial difficulties that were beyond consumers' control. National Consumer Law Center, Solving the Credit Conundrum: Helping Consumers' Credit Records Impaired by the Foreclosure Crisis and the Great Recession (2013).

11 FRB, Credit Scoring Report at O-4 to O-6, 8-13, 22-27; CFPB, Key Dimensions at 10-12.

12 FRB, Credit Scoring Report at 27-32. These pricing systems allow lenders to offer more competitive pricing to low-risk applicants, without turning away higher-risk applicants entirely. However, critics argue that such systems increase the likelihood of default for high-risk borrowers because loan payments are less affordable and sometimes charge more money than necessary to cover lenders losses. *See, e.g.*, Luke Herrine, Credit Reporting's Vicious Cycles, 40 N.Y.U. Rev. Law & Social Change 305, 322-31 (2016); Michael Staten, Risk-Based Pricing in Consumer Lending, Center for Capital Markets Competitiveness 10-14 (2014); Kevin A. Park, Policy Brief, Risks of Risk-Based Pricing, UNC Center for Community Capital (2014); Wendy Edelberg, Risk-Based Pricing of Interest Rates for Consumer Loans, 53 J. Monetary Econ. 2283 (2006); Alan M. White, Risk-Based Mortgage Pricing: Present and Future Research, 15 Housing Policy Debate 503 (2004).

13 PaymentsJournal, FICO Scores Used in Over 90% of Lending Decisions According to New Study, Mercator Advisory Group (Feb. 27, 2018); Peter Carroll & Cosimo Schiavone, 2018 VantageScore Market Study Report, Oliver Wyman (2018). The ways in which individual lenders use the scores and underlying credit reports vary widely. Some lenders establish a minimum third-party score below which they will not consider lending, but use proprietary algorithms to evaluate applicants above that score. Others feed traditional scores and/or individual attributes from credit reports into judgmental evaluations or proprietary automated evaluations that also incorporate data from other sources. Reliance on generic credit scores and/or individual credit report attributes is particularly heavy in situations in which instant credit may be an important part of a consumer's purchase decision, such as at a department store or auto dealer. FRB, Credit Scoring Report at 9; CFPB, Key Dimensions at 11.

BOX 2.1.1 THE TRADITIONAL CREDIT REPORTING SYSTEM

Local credit bureaus emerged in the 1800s as companies decided to pool information about whether customers paid their debts. When FCRA was adopted in 1970, it imposed various requirements to address concerns about privacy, fairness, and accuracy. However, it did not change the basic parameters of the industry, which depended on companies voluntarily deciding whether to furnish information, regardless of whether consumers consented to the transfer and use of their data.

After credit bureaus began consolidating, industry actors organized via the Consumer Data Industry Association in the late 1970s to set common standards for reporting to the NCRAs. The standards promoted efficiency, accuracy, and consistency, but implementing voluntary updates has proven challenging. "Metro 2" was adopted in 1997, but furnishers were not required to use it until the NCRAs entered settlements with several states in 2015 to stop accepting reports in previous formats by mid-2018.

Today, the NCRAs each maintain more than 200 million credit files with information drawn from the following sources:

- Creditors and some other firms that provide "trade line" information on the status of current and past loans, leases, and non-credit related bills;
- Certain public records relating to such items as bankruptcy and foreclosure;
- Information from debt buyers and collections agencies that are attempting to collect delinquent credit accounts or unpaid non-credit related bills; and
- A list of inquiries made by creditors and other firms about the individual's credit record.

Yet coverage gaps and inaccuracies remain a substantial concern. Because companies are not required to report information and some types of firms do not report positive payments data, the amount of information in individual credit files varies widely. For example, banks tend to report both positive and negative payment history, while landlords and utilities may report only cases involving serious delinquencies. As a result, renters may tend to have less robust credit histories than homeowners, even if they have similar finances and repayment histories.

Companies also have incentives to withhold certain information for competitive reasons. For example, before regulations were changed to require furnishers to report credit limits, some credit card lenders withheld that information for fear that competitors would use it to target their most profitable customers. This tended to lower consumers' credit scores by changing the assessment of their credit utilization. Non-prime lenders reportedly also sometimes withhold positive performance information for competitive advantage, and student lender Sallie Mae was subject to substantial criticism for withholding data in the early 2000s.

In some cases, laws also restrict reporting. For example, some sources interpret the Privacy Act of 1974 to limit information sharing by affordable housing owners or operators who benefit from federal assistance. And a few state laws restrict reporting by utilities.

Inaccuracies have also been a significant problem historically due to inadvertent errors by consumers and furnishers, as well as the processes NCRAs use to merge sources. For example, the NCRAs combine information based on partial matches in names, Social Security numbers, and other identifying information, which may itself contain errors. This can result in "mixed files" that combine information from other consumers as well as "orphan" trade lines that are missing from the correct consumer's file.

A 2012 study by the Federal Trade Commission found that 21 percent of participants had errors in their credit reports, 13 percent had errors that affected their credit scores, and 5 percent were able to obtain corrections that were so large that they changed credit risk tiers. The Consumer Financial Protection Bureau has since increased supervision of furnishers and NCRAs, but more recent statistics are not available.

Commercial credit bureaus and reports are not subject to FCRA or Metro 2. In the last decade, the commercial credit system has moved toward more standardized records of payments to vendors, equipment purchases, and creditors. Nevertheless, commercial reports and scores are not as consistent as in consumer markets.

Sources: Cheryl R. Cooper & Darryl E. Getter, Consumer Credit Reporting, Credit Bureaus, Credit Scoring, and Related Policy Issues, Congressional Research Service (2019); CFPB, Credit Reporting System at 3, 7-9, 13-17, 19-20, 23-25; Federal Trade Commission, Report to Congress under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 at i to vi, 57-64 (2012); FRB, Credit Scoring Report at 15-17; Robert B. Avery et al., Credit Report Accuracy and Access to Credit, Fed. Res. Bull. 297-322 (June 2004); Robert M. Jaworski, US National Credit Reporting Agencies to Amend Practices, E-Finance & Payments Law & Policy (2015); Policy & Economic Research Council & Brookings Institution Urban Markets Initiative, Give Credit Where Credit Is Due 36 (2006); Eric Dash, Up Against the Plastic Wall, N.Y. Times (May 21, 2005); Michelle Singletary, Sallie Mae, Moving in Slo-Mo, Wash. Post (Feb. 29, 2004); Furletti; FinRegLab, Small Business Spotlight at 7.

BOX 2.1.2 GENERIC CREDIT SCORING MODELS

The best known generic credit scoring models use information from NCRAs' files to group consumers based on the likelihood that they will become seriously delinquent on any of their credit accounts in the near future (typically 18 to 24 months). The models are proprietary, but FICO reports that 35 percent of its scores depend on payment history, 30 percent on amounts owed, 15 percent on the length of credit history, and 10 percent each on new credit and credit mix. VantageScore reports that total credit usage, balance, and available credit are most influential in its models, followed in descending order by credit mix and experience, payments history, age of credit history, and new accounts.

Scoring models can be built in different ways. A traditional method is to take snapshots of the credit records for a representative sample of consumers at two points in time, typically 18 to 24 months apart. Model developers then perform statistical analyses to determine which credit file attributes are most predictive of a consumer becoming seriously delinquent for any credit product as reflected in the second snapshot and assign weights to reflect the characteristics' relative importance. They may also break consumers into "scorecards" or "panels" based on particular characteristics to provide more sensitivity with regard to particular sub-groups. For more discussion of predictive methodologies, see Box 2.4.1.

A more recent innovation in credit scoring is to incorporate "trended data" that accounts for how various attributes are changing over time. For example, two consumers with the same credit utilization rates might be scored differently depending on how their rates have changed in recent months. VantageScore produced a model in April 2017 that used trended data, and one version of a new FICO model to be released in summer 2020 will also use such information.

While scoring models can group applicants by relative risk levels, they cannot predict which applicants within a particular score band may be more likely to default than others. Scores may change either because of shifts in the individual consumer's behavior or in the behavior of other consumers. And the overall likelihood of default may change over time due to shifts in economic conditions. Thus, a score is a rough ranking of a particular consumer relative to other consumers at a specific point in time.

Sources: CFPB, Key Dimensions at 10-12; FRB, Credit Scoring Report at 8-9, 22-27; AnnaMaria Andriotis, FICO Changes Could Lower Your Credit Score, Wall St. J. (Jan. 23, 2020); VantageScore, Improved Assessment of Credit Health Using Trended Credit Data (2019); MyFico, What's in my FICO Score?, myfico.com (visited Feb. 8, 2020); VantageScore, What Influences Your Score?, yourvantagescore.com (visited Feb. 8, 2020); Yuliya Demyanyk, Your Credit Score Is a Ranking, Not a Score, Federal Reserve Bank of Cleveland Economic Commentary (2010); Peter Carroll & Saba Rehmani, Alternative Data and the Unbanked, Oliver Wyman 4-5, 14-16 (2017).

comparisons, even lenders who rely upon proprietary scoring models to seek a competitive advantage may use generic scores to monitor portfolios, expedite securitization, and engage with investors.[14] Traditional small business lenders also frequently use owners' personal credit history and/or commercial credit reports as underwriting inputs, although the degree of reliance on generic scores and automation is not as heavy as in consumer markets.[15]

Together, these three reinforcing developments—automation, a nationwide credit information infrastructure, and use of generic credit scoring models—are credited with helping to fuel a substantial expansion in U.S. credit markets over the last several decades. In particular, the ability to access information that previously would only have been available to companies that have already done business with a particular applicant has been transformational. Studies suggest that it has tended to lower underwriting costs and default losses, improve the consistency of applicant evaluations, and increase competition for borrowers, particularly in consumer markets.[16]

14 FRB, Credit Scoring Report at 3, 8-9, 29-32. Such lenders typically rely on attributes from traditional credit reports but may have developed internal scoring models as an alternative to relying on generic scores. Such an approach may provide additional predictive power for particular products or markets but can create challenges in dealing with investors and the secondary market, as discussed further in Section 2.3 and 5.2.1.4.

15 FinRegLab, Small Business Spotlight at 5-9; Section 3.3.

16 FRB, Credit Scoring Report at S-2, S-3 to S-4, O-4 to O-6, 32-49; Hollis Fishelson-Holstine, Credit Scoring's Role in Increasing Homeownership for Underserved Populations, in Nicolas P. Retsinas & Eric S. Belsky, eds., Building Assets, Building Credit (2005); John M. Barron & Michael Staten, The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience, in Margaret J. Miller, ed., Credit Reporting Systems and the International Economy (2003). For studies on the impacts of the initial adoption of small business credit scoring, see Allen N. Berger & W. Scott Frame, Small Business Credit Scoring and Credit Availability, 47 J. of Small Bus. Mgmt. 5 (2007); W. Scott Frame et al., Credit Scoring and the Availability of Small Business Credit in Low- and Moderate-Income Areas, 39 Fin. Rev. 35-54 (2004).

Yet for all of these benefits, the traditional credit information system is still subject to significant limitations. Because reporting is voluntary and most information comes from particular categories of lenders, there is relatively little data about consumers or small businesses who do not already have and use those types of credit products. There are incentives for companies to withhold information, and accuracy has been a substantial concern historically though it may have improved in recent years. More fundamentally, even for applicants with relatively robust, accurate credit files, reports from the three NCRAs cannot provide a complete assessment of their finances because they do not provide direct information on applicants' incomes, balance sheets, or even a complete picture of all recurring expenses.[17]

Lenders can fill these gaps by collecting additional information from applicants and other third-party sources. But gathering, verifying, and analyzing a detailed picture of applicants' full financial situations can take substantial time and labor. These costs must also be balanced against competitive pressures to process and approve credit applications quickly. Thus, where such information is not sufficiently easy to access, lenders may reject applicants not because they in fact pose too much default risk, but rather because accurately assessing their default risk requires substantially more time and expense than other applicants.

2.2 Challenges for particular populations

The limitations of the traditional credit information system tend to affect some populations more intensely than others. Research has identified several groups who have a particularly difficult time accessing credit due to continuing information barriers:

- **Thin and no file consumers:** An estimated 45 to 60 million American adults cannot be scored using traditional models because they either have no credit files with NCRAs or their files are too limited to produce reliable predictions. African-Americans, Hispanics, recent immigrants, young borrowers, and lower-income consumers are particularly likely to be "thin file" or "no file."[18] For example, some studies have found that nearly 30 percent of African-Americans and Hispanics lack traditional credit scores, compared with about 16 percent of whites and Asians.[19]
- **Applicants with marred credit:** Adverse events generally remain on consumers' reports for seven to 10 years. Although many scoring and underwriting models place less weight on older data, major events such as foreclosures and bankruptcies can reduce credit scores initially by as much as 100 to 250 points on FICO and VantageScore scales.[20] Because credit scores and reports are used for multiple purposes, these events can negatively impact consumers' ability to obtain jobs and rent homes in addition to increasing credit prices, all of

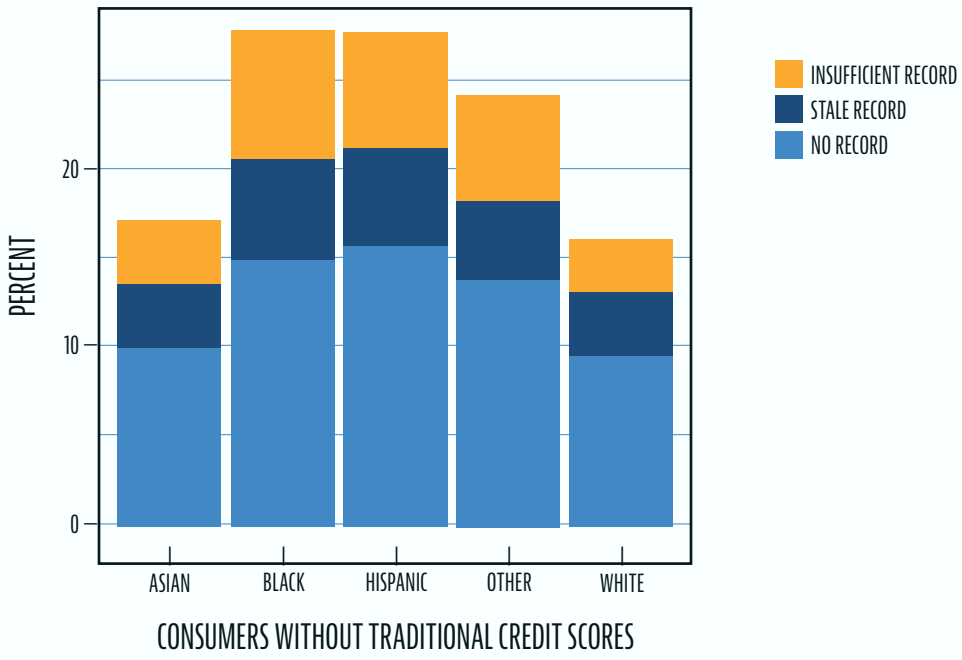
17 FRB, Credit Scoring Report at 15-17; CFPB, Key Dimensions at 8-10, 14.

18 CFPB, Credit Invisibles at 4-6; FICO Decisions, Can Alternative Data Expand Credit Access, White Paper No. 90 (2015); Carroll & Rehmani at 5.

19 CFPB, Credit Invisibles at 6, 17.

20 Wei Li et al., The Lasting Impact of Foreclosures and Negative Public Records, Urban Institute Housing Policy Finance Center (2016); CFPB, Credit Invisibles at 11-12; Bob Sullivan, The Simple Chart That Can Explain Why Your Credit Score Dropped, credit.com (Jan. 13, 2015). FICO and VantageScore consumer score scales range from 300 to 850. The FCRA generally requires that consumer reporting agencies omit negative adverse events from consumer reports after 7 to 10 years, although there is an exception for cases involving credit of more than $150,000 in principal. 15 U.S.C. § 1681c(a), (b). Research indicates that negative impacts on some consumers' scores can linger even after foreclosures are removed from their reports, particularly for borrowers who previously had prime credit scores. Li et al.; Kenneth P. Brevoort & Cheryl R. Cooper, Foreclosure's Wake: The Credit Experiences of Individuals Following Foreclosure, 41 Real Estate Econ. 747 (2013). And even after the credit scores of consumers who have gone through bankruptcy have recovered to original levels, lenders often substantially restrict credit limits. Julapa Jagtiani & Wenli Li, Credit Access After Consumer Bankruptcy Filing: New Evidence, 89 Am. Bankruptcy L.J. 327 (2015).

FIGURE 2.2.1 PERCENT OF CONSUMERS WHO LACK TRADITIONAL CREDIT SCORES BY RACE OR ETHNICITY (2010 DATA)



Source: Consumer Financial Protection Bureau Office of Research, Data Point: Credit Invisibles 17 (2015)

which can further increase the risk of future defaults.[21] And if consumers largely avoid or lose access to mainstream credit after an adverse event, their credit reports may not show payments history for other types of obligations.

» **Small business owners:** Like young borrowers, start-up companies do not have credit histories in their own right. Various other considerations have also made traditional lenders reluctant to provide business credit to companies that fall below certain sales and/or maturity thresholds. As a result, many owners are forced to rely on their personal credit histories and on consumer credit products to finance their businesses. Businesses owned by minorities, recent immigrants, and women tend to have particular challenges obtaining credit. And for owners whose personal credit is damaged in the course of standing up their business, there can be substantial hangover effects for their companies (and the owners themselves), since lenders often require owners of even mature companies to provide their personal credit histories as part of the application process.[22]

Beyond these specific populations, stakeholders have also raised broader concerns about heavy reliance on generic credit scores and credit bureau data. For example, many lenders use generic credit scores to set a threshold below which they will not lend, based on the overall predicted default rate for the cohort of consumers or small businesses with that particular credit score. But

21 NCLC, Solving the Credit Conundrum at 11-12; Herrine at 336-343; Brevoort & Cooper. Estimates of the number of landlords and employers that check credit reports range from roughly one-third to one-half. Casey Bond, How Employment Credit Checks Work, U.S. News & World Report (Oct. 31, 2019); Rourke L. O'Brien & Barbara Kiviat, Disparate Impact? Race, Sex, and Credit Reports in Hiring, American Sociological Association Socius (May 2018); TransUnion, Press Relase, TransUnion Reveals Almost Half of Landlords Consider Renters' Credit Health as a Key Factor in Leasing Decision, transunion.com (May 12, 2014). Credit reports are also used in setting certain types of insurance premiums, establishing eligibility for checking accounts, and some hospital admissions. CFPB, Key Dimensions at 2, 5; Nate Cullerton, Note, Behavioral Credit Scoring, 101 Georgetown L.J. 807, 810 (2013).

22 Karen G. Mills, Fintech, Small Business and the American Dream, Chapters 2-4 [eBook] (2019); FinRegLab, Small Business Spotlight at 4-11.

BOX 2.2.2 FAIR LENDING LAWS AND ANALYSIS

The Equal Credit Opportunity Act (ECOA) prohibits discrimination in "any aspect of a credit transaction" for both consumer and commercial credit on the basis of race, color, national origin, religion, sex, marital status, age, or certain other protected characteristics. The Fair Housing Act (FHA) prohibits discrimination on many of the same grounds in connection with consumer mortgage credit.

Fair lending enforcement actions and lawsuits are generally brought on two grounds. The first is "disparate treatment," in which creditors are alleged to have treated applicants differently based on protected characteristics. The second is "disparate impact," in which use of facially neutral practices has a disproportionately negative effect on members of a protected class, unless those practices are meeting a legitimate business need that cannot reasonably be achieved by less impactful means.

Automated underwriting models are generally recognized as reducing the risk of disparate treatment because they decrease subjectivity and the risk of personal bias. The models are generally prohibited from factoring in protected characteristics, and because they apply algorithms to standardized credit information, a given set of inputs produces the same outputs each time. This promotes consistent treatment even when dealing with a large number of variables that may have complex relationships with each other.

However, automated systems can still pose concerns about disparate impact—and fairness in a broader sense—because of both data and process issues. For example, if algorithms are developed based on data that is biased or incomplete, they may replicate the bias or fail to predict default risk for other types of borrowers. Monitoring model performance over time is also important, since changes in borrower behavior, economic conditions, or lender policies can cause models to lose predictiveness with regard to particular groups or overall. For more discussion of disparate impact analysis, see Box 3.2.1 below.

Sources: 15 U.S.C. 1691(a); 12 C.F.R. §§ 1002.4(a), 1002.6(a), 1002.6(b)(1); *id.* Supp. I, cmt. 4(a)-1, 6(a)-2; 1002.6(a)-2; CFPB, Key Dimensions at 11; FRB, Credit Scoring Report at O-5, 11, 36-37, 52; Carol A. Evans, Keeping Fintech Fair: Thinking About Fair Lending and UDAP Risks, Consumer Compliance Outlook 4-9 (2nd Issue 2017); Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues 27-32 (2016); Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Cal. L. Rev. 671 (2016).

BOX 2.2.3 FAIR LENDING RESEARCH ON TRADITIONAL CREDIT SCORING MODELS

The most comprehensive analysis of generic credit scoring models using traditional data from nationwide consumer reporting agencies was published in 2007 and 2012 by economists at the Federal Reserve Board. Because credit scoring models are proprietary, the study had to rely in significant part on a model that the economists constructed using attributes from traditional consumer reports by the NCRAs and general industry practices.

The report first looked at differences in average credit scores that were available from TransUnion as well as scores generated by the Board's model. It also evaluated differences in performance outcomes for different demographic groups relative to what the various scores predicted. The report found substantial differences in the median scores of African-Americans and Hispanics relative to whites and Asians. Many of these differences were reduced to the extent that the study authors were able to factor in a census-tract-based estimate of income, but they lacked the data to account fully for differences in such factors as wealth, employment, and education.

Turning to a more sophisticated multivariate analysis of the Board's model, the study found that it was predictive of credit risk for the population as a whole and for all major demographic groups. When the researchers controlled for demographic characteristics, the model remained predictive across groups. However, they identified a slight benefit to older individuals and a slight disadvantage to younger individuals (as well as recent immigrants), apparently due to the impact of factors related to the length of credit history.

Overall, the study concluded that the variables used in the scoring model did not serve as proxies for race, ethnicity, or gender, and that the negative impacts of using length of credit history were outweighed by its substantial independent predictive power.

Sources: FRB, Credit Scoring Report; Avery et al. (2012)

even at that threshold, the majority of borrowers may be likely to pay the loan back; the problem is just that using current data sources and methodologies, the credit scoring model by itself cannot predict which particular applicants within the band are more likely to default than others.[23] Accordingly, even "full file" applicants can find themselves shut out if their scores are not sufficiently high. Approximately 80 million U.S. adults currently have non-prime scores, which may cause them to be denied credit or charged substantially higher prices than consumers in higher credit bands.[24]

Advocates have also argued that traditional credit reports and scoring systems both reflect and perpetuate previous inequities created by historical discrimination on the basis of race, ethnicity, and gender in such fields as employment, education, housing, and lending. Studies frequently find large differences in traditional credit scores between different demographic groups, but due to data limitations they have had difficulty controlling fully for the fact that income, assets, and wealth also tend to vary between the study populations.[25] Concerns have also been raised that racial minorities' payment histories may be disproportionately negatively affected to the extent that they may lack geographic access to banks and are targeted by lenders who offer credit products with higher prices and riskier structures.[26] Although a 2007 Federal Reserve Board study concluded that traditional credit scoring models had substantial predictive value across different demographic groups, advocates have continued to raise concerns about differentials in traditional consumer credit scores.[27]

2.3 The quest for non-traditional data

In light of these various concerns, credit reporting agencies, scoring vendors, and other stakeholders have been working for more than a decade to expand traditional information flows and improve the predictiveness of generic scoring models. For example, various initiatives have focused on the benefits of funnelling more information from landlords, utilities, and lenders into NCRA credit files,[28] advocated

23 Carroll & Rehmani at 2, 4-6, 14-16; Itay Goldstein et al., FinTech and the New Financial Landscape, Banking Perspectives 3 (Mar. 12, 2019); *see also* Demyanyk, Your Credit Score Is a Ranking (explaining how credit scoring works to rank order consumers before translating the scores to "odds ratios" that estimate likely cohort default rates under particular economic conditions).

24 Consumer Financial Protection Bureau, The Consumer Credit Card Market 21-23 (2019); Aite, Alternative Data Across the Loan Life Cycle: How FinTech and Other Lenders Use It and Why, experian.com 5 (2018); Sarah Skidmore Sell, FICO to Test New Type of Credit Score That May Help Those with Weaker Credit, Chicago Times (Oct. 22, 2018). The number of non-prime borrowers has been declining for almost a decade thanks both to the economic recovery and to changes in the underlying data. It is unclear whether the introduction of the next generation of FICO models later in 2020 will change that trend. FICO is projecting that approximately 110 million consumers' scores will change by less than 20 points, but that about 40 million consumers at the high end and low end of the spectrum, respectively, may experience larger changes under its "FICO 10" models. Chris Arnold, FICO Is About to Change Credit Scores. Here's Why It Matters, npr.org (Jan. 30, 2020); Tara Siegel Bernard, Your Credit Scores May Soon Change. Here's Why, N.Y. Times (Jan. 25, 2020); AnnaMaria Andriotis, Why Your FICO Score Could Get a Boost in 2019, Wall St. J. (Oct. 21, 2018). As discussed further in Section 2.3, there can be substantial variations in how quickly lenders and other market actors adopt new scoring models.

25 FRB, Credit Scoring Report at S-4 to S-6, O-12 to O-24; Box 2.2.2.

26 Lisa Rice & Deidre Swesnik, Discriminatory Effects of Credit Scoring on Communities of Color, 46 Suffolk L. Rev. 935 (2013); National Consumer Law Center, Past Imperfect: How Credit Scores and Other Analytics "Bake In" and Perpetuate Past Discrimination (2016).

27 FRB, Credit Scoring Report at S-4 to S-6, O-12 to O-24; Robert B. Avery et al., Does Credit Scoring Produce a Disparate Impact? 40 Real Estate Econ. 965 (2012); Rice & Swesnik at 943-48; NCLC, Past Imperfect at 2.

28 Michael Turner & Patrick Walker, Potential Impacts of Credit Reporting Public Housing Rental Payment Data, U.S. Department of Housing & Urban Development & Policy and Economic Research Council (2019); Steven Melendez, Now Wanted by Big Credit Bureaus Like Equifax: Your 'Alternative' Data, fastcompany.com (Apr. 6, 2019); New York City Comptroller, Making Rent Count: How NYC Tenants Can Lift Credit Scores and Save Money (2017); Sarah Chenven & Carolyn Schulte, The Power of Rent Reporting Pilot, Credit Builders Alliance 7 (2015); TransUnion, Press Release, TransUnion Analysis Finds Reporting of Rental Payments Could Benefit Renters in Just One Month (2014); Experian RentBureau, Credit for Renting: The Impact of Positive Rent Reporting on Subsidized Housing Residents (2013); Experian, Blog, The Benefits of Full-File Credit Reporting and Why Communication Providers Should Consider It (June 25-29, 2011) (three-part blog). *See also* Box 4.1.1.2 regarding recent initiatives regarding utility payments information.

for legal changes to encourage utility reporting,[29] and adjusted model parameters or develop new models to improve predictiveness generally and to score additional thin file applicants.[30] The credit information industry has also responded to public research and criticism about sources of information that are relatively weak predictors of default and/or have disproportionate error and mis-match rates, for instance by changing processes for collecting public records and scoring medical debt.[31]

Yet while many of these efforts have emphasized potential inclusion benefits, they have sometimes triggered concern and even active opposition from stakeholders who argue that particular changes will negatively impact low-income consumers and/or prove insufficiently predictive of default risk.[32] And take-up rates for new scoring models have been uneven among lenders, secondary market investors, and other firms. Each company has to weigh the potential improvements in prediction and inclusion against the time and money required to purchase the new product, validate it for purposes of risk management, and coordinate with business partners who may not be ready to make the same transition.

The most severe illustration of these dynamics can be seen in the mortgage market, where the government sponsored entities Fannie Mae and Freddie Mac essentially require lenders to use FICO models that were developed in the late 1990s, despite the availability of several generations of more recent models that have been designed to improve predictiveness and better manage data concerns.[33] Although recent legislative and regulatory action is expected to break the logjam, piloting and implementation of new models is expected to take up to four years.[34]

29 Experian, The State of Alternative Credit Data 9 (2018); Experian, Let There Be Light: The Impact of Positive Energy-Utility Reporting on Consumers (2014). Some states directly restrict certain types of credit reporting by utilities without customer consent. Cal. Pub. Utilities Code §§ 2891(a)(2); N.J. Stat. Ann. § 48:3-85(b)(1); Wis. Stat. § 196.137. In others, states and local jurisdictions have enacted protections that make it difficult to cut off energy utilities to consumers that have fallen behind in their payments during peak months. Consumer advocates argue it would be inconsistent with these laws to report consumers who fall modestly behind on their bills in reliance on such protections, and some utilities reported that they have been told by state regulators that they are not permitted to report information to consumer reporting agencies. H.R. Rep.115-568 at 3 (Feb. 16, 2018); National Consumer Law Center, Access to Utility Service 91 (6th ed. 2018); Sara Burr & Virginia Carlson, Utility Payments as Alternative Credit Data: A Reality Check, The Brookings Institution Metropolitan Policy Program Discussion Paper (2007).

30 *See, e.g.,* Bev O'Shea, FICO XD: A Credit Score for Those with No Credit, nerdwallet (Jan. 24, 2019); Experian, The State of Alternative Credit Data at 19; Kristy Welsh, New Scoring Model Aimed at Those with No Credit Score, creditinfocenter.com (Sept. 26, 2017); Nick Zulovich, TransUnion's New Scoring Tool Blends 2 Data Sets Together, autoremarketing.com (Oct. 9, 2015); FICO Decisions at 9; Jeffrey Feinstein, LexisNexis White Paper, Alternative Data and Fair Lending (2013).

31 *See, e.g.,* Cooper & Getter at 10, 12-14; Consumer Financial Protection Bureau, Supervisory Highlights Consumer Reporting Special Edition 5-6 (2017); Consumer Financial Protection Bureau, Consumer Credit Reports: A Study of Medical and Non-Medical Collections (2014); Kenneth P. Brevoort & Michelle Kambara, Data Point, Medical Debt and Credit Scores, Consumer Financial Protection Bureau (2014). In part as a result of changes required by CFPB supervision and a settlement with a group of over 30 state attorneys general, tax liens and judgments have nearly been eliminated from credit reports. Consumer Financial Protection Bureau, Quarterly Consumer Credit Trends: Public Records (2018); Penny Crosman, Will Dropping Tax Lien Data from Credit Reports Lead to Bad Loans?, Am. Banker (Apr. 2, 2018).

32 For instance, stakeholders have been debating whether routine full-file reporting of energy utility data would help or harm consumers for more than a decade. *See, e.g.*, Gillian B. White, Can the Flaws in Credit Scoring Be Fixed? Not Easily, The Atlantic (Jan. 10, 2017); ChiChi Wu, National Consumer Law Center, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology (July 25, 2019); John Howat, Full File Utility Credit Reporting: Harms to Low Income Consumers, National Consumer Law Center (2009); Policy & Economic Research Council, Alternative Data in the US: Progress, Promise, and Paralysis (2019); Policy & Economic Research Council & Brookings Institution Urban Markets Initiative. The balance between inclusion and predictiveness has also been fiercely debated in mortgage markets as discussed in notes 35-36 and accompanying text. Some consumer advocates have also raised concerns that FICO's new models may make it more difficult for consumers who have experienced a job loss or other instability to get back on their feet. Arnold; Siegel Bernard. Although the new models have not specifically been touted for their inclusive effects, FICO is projecting that its "FICO 10T" model would permit mortgage and credit cards lenders to approve roughly 5 percent more applications than under previous models without increasing defaults.

33 *See, e.g.,* James B. Lockhart III, Why Fannie and Freddie Need Newer Credit Scoring Models, Roll Call (Apr 8, 2019); Pete Sepp & Thomas Aiello, Risky Road: Assessing the Costs of Alternative Credit Scoring, National Taxpayers Union (Mar. 21, 2019); Laurie Goodman, In Need of an Update: Credit Scoring in the Mortgage Market, Urban Institute (2017); Tom Parrent & George Haman, Updated Credit Scoring and the Mortgage Market, Quantilytic (2017) (research sponsored by FICO); Carroll & Schiavone (research sponsored by VantageScore). Announcements about the upcoming FICO 10 model indicate that it would reduce defaults by 17 percent relative to the FICO model currently used in the mortgage industry. FICO, FICO Introduces New FICO Score 10 Suite, PR Newswire (Jan. 23, 2020).

34 Credit Union National Association, Compliance: Final FHFA on Alternative Credit Scoring, news.cuna.org (Sept. 3, 2019); Andrew Ackerman, Fannie, Freddie to Consider Alternatives to FICO Scores, Wall St. J. (Aug. 13, 2019).

BOX 2.3.1 WHAT IS ALTERNATIVE OR NON-TRADITIONAL DATA?

"Alternative data" and "non-traditional data" are broad umbrella terms that may be used to refer to any information that is not typically contained in traditional credit reports and/or credit applications (such as annual income). For example, stakeholders sometimes use the two terms to refer to any and all of the following:

- Initiatives to increase reporting of items that have historically been reflected in traditional credit reports only to a limited extent, such as rental history, utility payments, and public records;
- Electronic cash-flow data from bank and prepaid accounts, small business accounting software, and other sources, even though traditional underwriting has long considered information about income, expenses, and reserves from other sources;
- Items that may relate to income and assets, such as education and employment history, professional licenses, and property ownership; and
- Items that are less clearly tied to applicants' finances, such as how applicants interact with lenders' websites, their type of phone lines and/or electronic devices, other information about their on-line footprints, magazine subscriptions, and social media use patterns.

Some stakeholders distinguish between "financial" alternative data and "non-financial" or "behavioral" information, though drawing clean lines between categories can be difficult. For example, cash-flow data from transaction accounts reveals some non-financial information, such as the time and location of particular retail transitions or the company from which purchases are made. And shopping at particular retailers or using particular types of electronic devices may have some correlation with income.

The use of non-financial data is beyond the scope of FinRegLab's cash-flow research, but is important to note given growing interest in the market. Non-financial data is being used internationally, and there is some research based on data from other countries suggesting that it can be predictive of default. News reports indicate that some U.S. lenders and model developers are also using this data, though it is often difficult to distinguish between use for identity verification and fraud screening, marketing, loan origination/underwriting, and/or ongoing monitoring and servicing of loans.

Particularly in the U.S., regulators, advocates, and other stakeholders have expressed significant caution about using non-financial information for underwriting in particular in light of concerns about privacy, fair lending, broader fairness, accuracy, and transparency. See Section 6.1.1 for further discussion of related issues.

Sources: Tobias Berg et al., On the Rise of the FinTechs: Credit Scoring Using Digital Footprints, Review of Fin. Studies (Sept. 2019); Penny Crosman, 'Out of the Shadows': Use of Alternative Data in Lending Gains Ground, Am. Banker (Dec. 16, 2019); AnnaMaria Andriotis, Hairdresser, Plumber, Lawyer: A Job License Could Help You Get a Loan, Wall St. J. (Nov. 6, 2019); AnnaMaria Andriotis, Need Cash? Companies Are Considering Magazine Subscriptions and Phone Bills When Making Loans, Wall St. J. (Sept. 12, 2019); AnnaMaria Andriotis, Shopping at Discount Stores Could Help Get You a Loan, Wall St. J. (Mar. 4, 2019); Aite at 7-13; Deirdre Fernandes, Lenders Eye Social Media for Clues, Boston Globe (Sept. 4, 2016); Kelly Dilworth, New Lenders Shun FICO, Create Their Own Scores, creditcards.com (Feb. 26, 2016); Nick Clements, 5 Reasons New Lenders Are Ignoring FICO Credit Scores, Forbes (Apr. 21, 2015); Brian Browdie, Can Alternative Data Determine a Borrower's Ability to Repay, Am. Banker (Feb. 24, 2015).

With the explosion in digital data over the last two decades,[35] stakeholders are also turning to "alternative" or "non-traditional" data sources that have never been a part of the traditional credit reporting system. Cash-flow data is one of the most promising candidates, both because it bears directly on applicants' finances and because it is increasingly available in electronic form.[36] Indeed, some stakeholders argue that cash-flow information should not be considered alternative or non-traditional in the first instance because lenders have long relied on such basic inputs as income,

35 Estimates of the volume of data worldwide increased from just three exabytes in 1986 to an estimated 300 exabytes by 2011, and trends have only accelerated since then. A 2016 report estimated that nearly 90 percent of the data in the world had been generated in the previous two years, and a 2018 report projects that the amount of data is expected to grow annually by 60 percent through 2025. David Reinsel et al., Data Age 2025: The Digitization of the World from Edge to Core, IDC (2018); McKinsey Global Institute, The Age of Analytics: Competing in a Data-Driven World 22-23 (2016); IBM Marketing Cloud, 10 Key Marketing Trends for 2017 (2016).

36 In the small business context, transaction records from payment processors or e-commerce platforms can also be useful because such sources provide a detailed history of income flows, though not a complete picture of how the small business manages its expenses. FinRegLab, Small Business Spotlight at 22. In the consumer context, credit card or electronic wallet records could provide expense data, though such records would not directly provide insight into income and reserves.

FIGURE 2.3.2 ILLUSTRATIVE EXAMPLES OF CASH-FLOW DATA THAT COULD BE USED IN CONSUMER AND SMALL BUSINESS UNDERWRITING MODELS

UNDERWRITING DATA SOURCE	UNDERWRITING DATA TYPES	
BANK AND PREPAID ACCOUNTS (DIRECT DEPOSIT ACCOUNTS, COULD INCLUDE GENERAL PURPOSE RELOADABLE PREPAID CARDS)	**FINANCIAL DATA** » Inflows (Paystubs, direct deposits, etc.) » Outflows (Expenses) » Fees (Overdraft)	**INFERRED FINANCIAL DATA** » Monthly balance / cushion » Income » Balance history
	NON-FINANCIAL DATA » Time of day transaction made » Merchant identity or purchase type	**INFERRED NON-FINANCIAL DATA** » Frequency (of deposits, transactions)
SMALL BUSINESS SOURCES (PAYMENT PROCESSING RECORDS, E-COMMERCE PLATFORMS, ACCOUNTING SOFTWARE)	**FINANCIAL DATA** » Business credit card transaction data » Accounts receivable » Checking account data	**INFERRED FINANCIAL DATA** » Gross / Net profit margin » Income » Business efficiency (sales / assets) » Liquidity ratios » Free cash flows
	NON-FINANCIAL DATA » Business inventory	**INFERRED NON-FINANCIAL DATA** » Business efficiency (inventory turnover)

NOTES: Inferred Data refers to data that is an interactive variable generated from multiple variables. E.g., available monthly balance equals average monthly inflow variables minus average monthly outflow variables.

expenses, and payment history to evaluate applicants' potential default risk. Although it has not been much used in practice, a federal regulation called the Shoebox Rule actually requires lenders who consider credit history or other information from credit bureaus in their underwriting processes to consider alternate sources of comparable information if requested to do so by applicants.[37]

Yet in other ways, regularized electronic access to cash-flow data is potentially revolutionary because it facilitates faster, more sophisticated, and more consistent analyses of applicants' overall finances than relying solely on traditional credit information or collecting equivalent data from paper sources. While lenders may not have embraced consideration of paper cash-flow records under the Shoebox Rule, interviews with stakeholders suggest that there are several aspects of electronic cash-flow data that make it particularly appealing for evaluating credit risk in both consumer and small lending markets:

- **Sensitivity and timeliness:** Particularly when it is derived from bank accounts or from small business accounting software, electronic cash-flow data can provide a more detailed and timely view of applicants' overall finances than traditional credit reports and scores. While traditional credit reports typically only reflect payment history for selected types of expenses and are updated on a monthly batch basis, bank account and bookkeeping software data can provide a detailed picture of inflows, outflows, and cushions. Several bodies

37 12 C.F.R. § 1002.6(b)(6); supp. I cmt. 6(b)(6)-1. The provision is called the Shoebox Rule because it requires lenders to give further consideration when consumers bring in a shoebox of bank statements or receipts. However, the rule does not explain exactly how such information should be treated, and it is not well known among consumers. Some commentators have called it the "best kept secret in lending," asserting that it has been "conveniently forgotten by both the industry and regulators" to the detriment of consumers. National Consumer Reporting Association, A Position on Non Traditional or Alternative Credit Data and the Equal Credit Opportunity Act. Regulation B (visited Feb. 8, 2020); John Ulzheimer, Blog, The Best Kept Secret in Lending, Bar None, mint.com (March 14, 2011). Other stakeholders note that even if the rule was used more regularly, it would not necessarily yield the same kind of benefits as wide-spread incorporation of electronic data because of consistency and efficiency challenges.

FIGURE 2.3.3 PERCENT OF HOUSEHOLDS WITHOUT ACCOUNTS BY RACE OR ETHNICITY (2017 DATA)

Source: Federal Deposit Insurance Corporation

of recent research suggest that income patterns, volatility, and financial reserves are important determinants of repayment capacity and general long-term financial health for both consumers and small businesses.[38] Recent cash-flow data may also be particularly helpful to assessing the extent to which applicants with marred credit have stabilized their finances.

» **Coverage:** A 2017 survey by the Federal Deposit Insurance Corporation found that 96 percent of American households had at least one checking, savings, or prepaid account,[39] compared with only 80 percent of households that had used at least one "mainstream" credit product that was likely to be reported to traditional credit bureaus in the past year. Although African-American and Hispanic households are more likely to operate without bank or prepaid accounts than Asian and white households, the disparities were substantially smaller than with regard to use of credit products.[40] Similarly, business checking accounts are also cheaper and easier to obtain than commercial credit products, and other types of cash-flow data are becoming more widely available as small businesses' reliance on accounting software, e-commerce platforms, and payment processors has increased.[41]

38 See Appendix C.

39 Over the past two decades, prepaid accounts offered by non-banks have increasingly become an alternative to traditional bank checking or savings accounts for many households. The prepaid accounts that can be accessed via "general purpose reloadable cards" can receive direct deposits and be used for transactions at multiple, unaffiliated merchants for goods or services, for ATM withdrawals, and for person-to-person transfers. Their fee structures are often simpler than checking accounts, and many issuers have developed business arrangements with banks that provide deposit insurance to cover the funds. From 2009 to 2017, the proportion of "unbanked" U.S. households using prepaid cards increased from 12.2 percent to 26.9 percent. Under rules that took effect in April 2019, prepaid card users generally have access to at least 12 months of electronic history and at least 24 months of written history upon request. This could facilitate use of cash-flow data from prepaid accounts for credit underwriting. 12 C.F.R. § 1005.18(c)(1); 81 Fed. Reg. 83,934 (Nov. 22, 2016); FDIC, 2017 National Survey at 34-39; Federal Deposit Insurance Corporation, 2011 FDIC National Survey of Unbanked and Underbanked Households 6 (2012).

40 FDIC, 2017 National Survey at 1, 7, 9-12, 18-19, 34-38, 48-58. Note that the FDIC survey focuses at the household level, while the CFPB's research estimating the number of no file and thin file consumers in 2010 focused at the individual level. CFPB, Credit Invisibles at 4-6; notes 18-19 and accompanying text.

41 FinRegLab, Small Business Spotlight at 12.

» **Specialization:** The third feature that makes electronic cash-flow data particularly useful is that it can help lenders build expertise and tailor credit risk models with regard to particular sub-groups of applicants. For example, small business lenders report that it can be useful to evaluate particular types of companies that local lenders may not have much familiarity with. Similarly, cash-flow data may also be particularly useful in evaluating "gig" economy workers, who by some estimates make up one-third of the nation's workforce.[42]

Of course, there are also limitations to what cash-flow data can reveal about applicants' finances. For instance, transaction account history reveals what account holders have paid historically but not what they owe currently or what additional debt they may already be approved to take on.[43] Determining which payments are made for purposes of particular recurring expenses may require additional information or analysis.[44] Forecasting gross household income based solely on transaction account records can also be somewhat inexact due to differences in withholding taxes and benefits, the possibility that household members maintain multiple accounts, and other factors.[45] And collection and processing of cash-flow data involves additional costs and coordination where a particular applicant has multiple accounts[46] or none at all.[47]

Nevertheless, the potential cost-benefit analysis is sufficiently appealing that as a new system has emerged to facilitate transfers of account data for other purposes, a growing range of credit market stakeholders have begun to take notice. As described in Sections 3.3 and 4.1 below, a new generation of fintech firms and certain credit reporting and scoring incumbents have begun to develop cash-flow based underwriting and scoring models. In the small business context, some banks and other types of tech firms have also begun to use such data for credit underwriting. However, while some banks and credit unions are using cash-flow data in limited ways in consumer

42 *Id.*; Ron Shevlin, Gig Economy Banking Is Booming (And Banks Are Missing The Boat), Forbes (Sept. 23, 2019); Maija Palmer, Fintech for Gig Workers Is the Next Big Untapped Market, Sifted (May 13, 2019); Jann Swanson, Lenders: Income Verification Needs for "Gig" Economy, Mortgage News Daily (May 21, 2018); Gallup, The Gig Economy and Alternative Work Arrangements 2 (2018); Elizabeth Buchwald, The Government Has No Idea How Many Gig Workers There Are, and That's a Problem, MarketWatch (Jan. 7, 2019). For a discussion of predictive modelling of low-wage workers with high levels of income instability in the context of personal financial management, see Wenyu Zhang et al., Financial Forecasting and Analysis for Low-Wage Workers (2018). Federal regulators' interagency statement on alternative data specifically noted that cash-flow data could be useful for this purpose. Interagency Alternative Data Statement at 2.

43 In this respect, the data is largely positive in nature, except in cases in which the account itself runs a negative balance. In addition, some sources of cash-flow data that are used in the small business context, such as feeds from accounting software or payment processing and e-commerce records, may not always be as complete or reliable standing alone as transaction account data, although stakeholders often still find them valuable. FinRegLab, Small Business Spotlight at 22.

44 See note 203 and accompanying text.

45 Because of these variations, lenders who want to calculate and/or verify gross household income precisely may obtain additional information from applicants or other sources to supplement transaction account records. For details of one attempt to forecast gross household income by quintile for research purposes based solely on transaction account records at a single bank, see JPMorgan Chase Institute, Estimating Family Income from Administrative Banking Data: A Machine Learning Approach (2018) (reporting that the best algorithm predicted the correct quintile about 55 percent of the time as compared to income information on file from mortgage and credit card applications, and within one quintile for about 90 percent of cases studied).

46 Statistics on financial account ownership vary. *See, e.g.*, PaymentsJournal, How Many Bank Accounts Do Consumers Have?, Mercator Advisory Group (July 2, 2019) (average of 5.3 accounts); Cameron Huddleston, 50% of Americans Are Cheating—on Their Bank, GOBankingRates.com (Jan. 17, 2019) (50 percent of survey respondents had checking, savings, certificates of deposit, or money market accounts with more than one bank). However, maintaining multiple transaction accounts for low to moderate income households can be relatively expensive because of the risk of incurring either up-front account fees or overdraft charges. Surveys suggest that underserved populations—particularly prepaid account users—are relatively sensitive to such costs, though some households that have bank accounts do use prepaid accounts for specific budgeting or spending functions, such as on-line transactions. *See, e.g.*, FDIC, 2017 National Survey at 4, 34-37; The Pew Charitable Trusts, Why Americans Use Prepaid Cards: A Survey of Cardholders' Motivations and Views 7-8, 11-17 (2014).

47 For consumers who lack bank accounts, some lenders will accept physical copies or phone snapshots of bills and other third-party records. Collecting this information may take additional time and effort, and there are some concerns about falsified documents particularly in the electronic context. However, some companies are providing digitization services to make it easier to combine information pulled from data aggregators, PDF documents, and paper materials. PYMNTS, Open Banking Overcomes the Data Obstacle of Paper, pymnts.com (Dec. 30, 2019); Lisa Goetz, How Do Mortgage Lenders Check and Verify Bank Statements?, Investopedia (Jul. 7, 2019); Ray Birch, Time to Beef Up Fraud Detection Here?, CUToday.info (Jan. 3, 2019).

credit, they do not to date appear to be broadly incorporating the data into their core automated underwriting models for various consumer products.

2.4 FinRegLab's research

This background informed FinRegLab's decision to focus its first major research and policy analysis project on the use of cash-flow data in credit underwriting. FinRegLab is a non-profit research organization that was founded in 2018 to provide independent, rigorous research to support the development of market norms and policy solutions that enable responsible innovation in financial services. This report, along with its companion documents, is our first effort to provide such research and begin a conversation on themes that we expect to recur in our subsequent work.

We organized two initiatives to support the broader project, in addition to other stakeholder engagement and internal analysis:

- In the first, we retained Charles River Associates to help us design and conduct an independent empirical analysis of the predictiveness of cash-flow variables and scores that are being used in consumer and small business markets by six non-bank financial services providers—Accion, Brigit, Kabbage, LendUp, Oportun, and Petal. The analysis evaluated the cash-flow metrics based on actual loan performance. We also compared the predictiveness of the cash-flow metrics to traditional scores and variables, as well as to combined models using both types of information.
- In the second, we convened more than 80 representatives of lenders, banks, data aggregators, advocacy organizations, and researchers to engage in an extended dialogue about the challenges that are shaping both the adoption of cash-flow based underwriting and the underlying system for customer-permissioned data transfers. Representatives of several federal banking agencies and the Consumer Financial Protection Bureau attended the sessions in an observer capacity. Over the course of approximately eight weeks in late 2018, the participants met in three policy working groups to discuss issues relating to fair and inclusive access to credit, consumer understanding and consent in connection with both cash-flow based underwriting and related data transfers, and other policy concerns raised by the emergence of a new kind of data-sharing system.

We supplemented these workstreams in 2019 with dozens of one-on-one interviews with different types of stakeholders across consumer and small business markets. Our analysis was also informed by the discussion that occurred at a November 2019 symposium on "The Role of Consumers in the Data Ecosystem" that we co-hosted with the Fintech Team at the Federal Reserve Bank of San Francisco.

Our goal across both workstreams was to use cash-flow based underwriting as a stepping stone to broader questions about how customer-permissioned data sharing can be structured to promote customer access and control, while preserving space for firms to use that data to create financial products and services that better serve the public. Because of the nature of the data needed and the potential stakes for both borrowers and lenders, cash-flow underwriting presents some additional policy challenges relative to transfers for other types of financial services.

We also viewed the project as a potentially useful case study concerning the adoption of innovations in credit underwriting more generally. That field is undergoing a transformation as lenders experiment with non-traditional data and new techniques for predictive forecasting. Although this project focused on information sources that are less controversial than other types of alternative

data and did not focus on machine learning algorithms, many of the issues that are raised by the adoption of cash-flow underwriting are also relevant to other credit innovations.

This report is intended to work in tandem with our earlier two cash-flow publications by providing both additional market context for consumer lending and deeper policy analysis of issues that cut across consumer and small business markets. Specifically, Section 3 provides a summary of our two previous publications, although readers are encouraged read the *Empirical Research Findings* and *Small Business Spotlight* reports for additional context. Section 4 provides a detailed snapshot of the use of cash-flow data in consumer credit underwriting today, as well as the system that has emerged over the last twenty years to facilitate customer-permissioned transfers of transaction account data. The next three sections provide the policy analyses, with Section 5 focusing on the potential benefits to cash-flow underwriting and challenges to reaching scale, Section 6 on customer protection and customer control issues, and Section 7 on potential considerations for industry, regulators, and Congress in addressing particular public policy concerns. Section 8 concludes the report.

Four appendices are also provided for reference: Appendix A lists the organizations whose employees participated in FinRegLab's policy working group discussions; Appendix B defines common terms and acronyms; Appendix C summarizes recent published research on related topics; and Appendix D summarizes principles for data sharing and related activities that have been issued by various government agencies and private organizations.

BOX 2.4.1 BROADER TRENDS IN CREDIT UNDERWRITING

The growing use of cash-flow data in credit underwriting is just one of many innovations that are occurring in credit markets today. Lenders and model developers are also experimenting with other types of alternative and non-traditional data, as discussed in Box 2.3.1, and with new computer science techniques that are often described as involving machine learning or artificial intelligence, as distinguished from models based on traditional techniques such as linear or logistic regressions.

Use of machine learning methods is beyond the scope of FinRegLab's cash-flow research, but we expect to focus on it in future research given growing interest in the market. Traditional regression methods provide a precise explanation of how each input contributes to the output, but they have difficulty where several inputs are closely correlated to each other or where the relationship between the variables is highly complex. The types of machine learning techniques that are being explored in the underwriting context are able to process large amounts of data, even in situations involving high degrees of correlation or other complex relationships. They generally are recognized as providing higher levels of predictiveness, even when using only traditional data sources. But because of their complexity, it is often difficult to determine exactly how they are reaching their predictions particularly where some models evolve over time in response to new data.

Because of questions about the ability to explain the models and manage fairness concerns, use of machine learning in credit decisions is limited to date, though it is being used in fraud detection and marketing programs. While some stakeholders point to the potential for increasing inclusion and lowering default risk in underwriting, others raise concerns that machine learning algorithms could increase fair lending risk or increase losses to lenders if they are relying on relationships between variables that prove to be ephemeral over time.

Many lenders—particularly banks—are reluctant to adopt machine learning techniques in credit underwriting while industry, academia, and regulators are exploring ways to better manage explainability and fairness concerns. Some firms may use such techniques to explore potential new inputs, but then use the most promising variables in a more traditional regression model for actual credit decisioning. This approach helps to manage regulatory compliance concerns but reduces some of the predictiveness gains relative to the original machine learning algorithm.

Sources: 82 Fed. Reg. 11183, 11184-85 (Feb. 21, 2017); Majid Bazarbash, FinTech in Financial Inclusion: Machine Learning Applications in Modelling Credit Risk, IMF Working Paper 19-109 (2019); Aite at 16; Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services (2017); Andriotis, Shopping at Discount Stores; Trevor Dryer, How Machine Learning Is Quietly Transforming Small Business Lending, Forbes (Nov. 1, 2018); Bart van Liebergen, Machine Learning: A Revolution in Risk Management and Compliance?, 45 Capco Inst. J. of Fin. Transformation 60 (Apr. 2017); Penny Crosman, Is AI Making Credit Scores Better, or More Confusing?, Am. Banker (Feb. 14, 2017).

3. SYNTHESIS OF PRIOR RESEARCH

The *Empirical Research Findings* report provides an independent, quantitative analysis of cash-flow scores and variables that are being used by several non-bank financial services providers to underwrite a range of unsecured credit products for consumers and small businesses. The *Small Business Spotlight* provides additional market context and policy analysis specific to small business lending.

With assistance from Charles River Associates, we defined three specific research questions for consideration in the *Empirical Research Findings* report:

- Are cash-flow variables and scores useful in predicting credit risk in the underwriting process, as compared with traditional credit scores and/or credit bureau attributes?
- Do cash-flow variables and scores expand the availability of credit, particularly with respect to consumers and small business owners who may have experienced constrained access to credit under more traditional underwriting criteria?
- What, if any, risks of creating a disparate impact among different demographic groups appear to arise from the use of cash-flow variables and scores in highly automated underwriting processes?

We structured the empirical research to focus on evaluating the predictiveness of the particular cash-flow scores and metrics supplied by the study participants.[48] The participants did not provide us with the underlying bank account or other records or the algorithms by which they generate cash-flow scores and metrics, make credit eligibility determinations, or determine prices. They commonly use additional information and attributes in their automated underwriting processes beyond the cashflow metrics that were the focus of our analysis, and they did not provide the weights assigned by their algorithms to each cash-flow attribute. Thus, the participants' cash-flow metrics permitted Charles River Associates and FinRegLab to evaluate the predictiveness and fair lending effects of the variables and scores in general, but our analysis does not evaluate their particular proprietary models.

The diversity of the participants and data prevented combining the data to perform a consolidated analysis. Accordingly, the *Empirical Research Findings* report provides separate summaries of the results for each participant. Given each participant's interest in protecting proprietary information, we agreed to anonymize the firms in the findings and present the research results in

48 For more discussion of the research questions and methodology, see FinRegLab, Empirical Research Findings at 14, 18-23.

a way that does not identify individual participants or individual cash-flow variables. In addition, the results for participants who are focused on small business markets are not separately identified from those who focus on consumer populations. Finally, discussion of certain aspects of the participants' lending processes is provided only at a group level.

The *Small Business Spotlight* provides additional context and analysis based on one-on-one interviews, insights from the policy working group process, and our own internal work.

3.1 Research participants and underwriting processes

The six participants in the empirical research provided data concerning their use of cash-flow variables and/or scores in underwriting unsecured, relatively short-term credit products.[49] They are heterogeneous with respect to a wide range of factors, including business models, geographic footprint, operational structure, product offerings, application channels, tenure in specific markets, and overall lending volumes. They also take different approaches to acquiring and using cash-flow data.

To illustrate just some of these differences, four companies focus on consumer lending, while two serve small businesses. The participants include five for-profit firms and one non-profit; in addition, two of the six are certified Community Development Financial Institutions (CDFIs).[50] All of the credit products studied are unsecured, but the products vary as to closed-end and open-end structures and as to whether they are issued by the participants or by partner banks. Other terms also vary significantly. For example, repayment periods vary from the borrower's next account deposit to 46 months. Fee and rate structures also vary depending on the product type and in some cases the amount borrowed and other factors relating to borrowers' credit characteristics. Several of the participants are nationally based, while others are highly concentrated in selected geographies.

The following provides a brief overview of each of the participants' target markets, product types, and distribution channels:

- **Petal:** Petal partners with Web Bank, an FDIC-insured industrial bank chartered in Utah, to provide an unsecured credit card to consumers in amounts that range from $500 to $10,000. Marketing is aimed at consumers who have a limited credit record. Applications are accepted online.
- **Oportun:** As a certified CDFI, Oportun provides unsecured installment loans to low- and moderate-income consumers. Loans range in size from $300 to $9,000 and in length from 6 to 46 months. The maximum loan amount varies by state, and loans above $6,000 are available specifically to qualified returning customers. Consumers can apply for the loans via retail locations in some states, online, or by phone.[51]
- **LendUp:** LendUp offers installment loans and a single payment loan that is marketed as a payday loan alternative. The company uses a point system based on consumers' repayment history and completion of free online education courses; consumers who reach certain point levels can qualify for installment loans with larger loan amounts and lower rates, and opt

49 See FinRegLab, Empirical Research Findings at 15-17 for a more detailed summary. Some of the participating companies provide access to credit by partnering with or acting as service providers to financial institutions that extend loans or other credit products, but do not consider themselves to be lenders and do not themselves extend credit.

50 CDFIs are certified by the Community Development Financial Institutions Fund within the U.S. Department of the Treasury based on a mission of serving low-income communities, and are eligible for various types of CDFI Fund assistance and programs. CDFI Fund, CDFI Certification: Your Gateway to the CDFI Community (2016).

51 Oportun loans are available in twelve states with retail locations in the following nine states: Arizona, California, Florida, Illinois, New Jersey, New Mexico, Nevada, Texas, and Utah. Loans for residents of Idaho, Missouri, and Wisconsin are online only.

to have those loans reported to build credit history. Loans meeting certain size and pricing thresholds are automatically reported to consumer reporting agencies. Data on the unsecured single payment loan was evaluated in this research. That product ranges in amount from $100 to $500, with repayment due in two to four weeks. Applications are accepted online.

- **Brigit:** Brigit provides cash advances and financial monitoring tools to consumers who have an active bank account. The company uses a flat monthly subscription fee. Brigit monitors consumers' account balances to identify when a customer's balance is likely to become negative. The company will deposit an amount up to $250 to prevent an overdraft. Consumers are also permitted to request advances manually but can only request one at a time. Payment is due after the next account deposit. The Brigit product can be applied for online.
- **Kabbage:** Kabbage provides small businesses with access to unsecured lines of credit between $2,000 and $250,000 through its technology service provider relationship with Celtic Bank, an FDIC-insured industrial bank chartered in Utah. Celtic Bank requires one year of operating history and, on average, revenues of $50,000 annually or $4,200 monthly for the last three months to qualify. Average credit lines are $25,000 and average draws are $6,000; draws are treated as installment loans with terms of 6, 12 or 18 months. All business loans available through Kabbage are issued by Celtic Bank. Applications are accepted online.
- **Accion in the U.S.:** Accion in the U.S. (Accion) is a non-profit small business lender that provides installment loans of $300 or more to underserved entrepreneurs. Repayment periods are typically 24 months. Accion provides small businesses loans nationwide through four independent, regional CDFIs and a national office that coordinates technology and knowledge sharing to benefit the network. Data from one location was evaluated in this research. Accion accepts applications online.

All participants use highly automated underwriting systems. From available cash-flow sources, they distill financial variables reflecting applicants' income, expenses, balances, and activity levels. In the small business context, for example, the participants use cash-flow data to assess the business's historical and projected performance. The data includes incoming revenue, receivables, expenditures, and business obligations. The firm's financial performance may also be evaluated based on such metrics as average monthly revenue and transaction volume.

Although the consumer participants evaluate cash-flow data for periods up to twelve months, the small business participants sometimes consider longer periods depending on the data source and availability. Some participants pull data over time, for instance to monitor whether adjustments in the terms for open-end credit products are warranted.[52]

Across one or more participants, sources of cash-flow data included transaction account data from banks, business accounting software, payments processors, and e-commerce platforms, as well as copies of pay stubs, invoices, bill statements and similar materials provided by applicants. The latter is part of a broader underwriting process that may allow some participants to extend credit to customers who may lack access to bank accounts and thus do not have digital cash-flow data. The participants generally use one or more data aggregators, which are discussed further in Section 4.2, to access bank account data.

52 We did not have access to any information regarding data that was pulled after the participants' original decisions in connection with later monitoring or decisionmaking.

All of the participants use the cash-flow data to create proprietary assessments of repayment risk, but they vary as to the stage at which they use that information, the weight that they assign it in evaluating ability and/or propensity to repay, and the extent to which they rely upon traditional scores or attributes in sequence or in combination with cash-flow variables. The participants also vary as to their use of traditional credit bureau attributes and scores. Most participants will grant credit to applicants who do not have traditional credit scores, though they may factor traditional scores and attributes into their underwriting processes where available. The small business participants differ as to how they approach use of business credit scores and/or the personal scores of business owners.

3.2 Empirical results and areas for further research

As further detailed in the *Empirical Research Findings* report, our analysis found encouraging results with regard to all three of the research questions. More specifically:

Predictiveness: For the participants for which loan-level data was available, we found compelling evidence that indicates that the cash-flow variable and scores tested were predictive of credit risk and loan performance across the heterogenous set of providers, populations, and products studied. The results appeared to be robust across both consumer and small business populations as well as across the credit spectrum, including among borrowers with no or very low traditional credit scores. The cash-flow metrics were both predictive in their own right and also frequently improved the ability to predict credit risk in combination with traditional credit scores or other metrics.

Two implications of the results are particularly important. First, the overall strength of the results and the nature of the participating companies' underwriting practices suggest that cash-flow variables and scores can provide meaningful predictive power among populations and products similar to those studied where traditional credit history is not available or reliable. Second, the fact that cash-flow attributes and scores frequently improved predictiveness in combination with traditional credit history is noteworthy. The improvement in predictiveness for combined models and our other analyses suggest that cash-flow information separates risk in somewhat different ways than traditional metrics. Overall, the results suggest that with regard to populations and products similar to those studied, cash-flow data can provide meaningful insights by differentiating predictions of credit risk among borrowers that are scored by traditional systems as presenting similar risks of default.[53]

Inclusion: We found evidence that the study participants are serving borrowers who may have historically faced constraints on their ability to access credit, although data limitations did not permit a consistent quantitative analysis to be applied across all participants. Instead, we used a variety of benchmarks depending on what data was available, including the percentage of borrowers with low or no traditional credit scores, borrower income levels, and residence in zip codes in which racial minorities exceed 50 percent or 80 percent of the total population.

For example, we were able to study the percentage of borrowers who had no or low traditional credit scores for three of the participants. This group is likely to include relatively high numbers of no file or thin file applicants, as well as borrowers with marred credit. The percentage of the three participants' borrowers with traditional scores below approximately 650 was roughly 45 percent to 50 percent and the percentage of their borrowers below approximately 600 ranged from 0 to 25

53 FinRegLab, Empirical Research Findings at 24-29.

percent. In addition, two participants reported that attempts to pull traditional scores for 3.5 percent and 8 percent of their borrowers were unsuccessful, respectively.[54]

Fair lending effects: Finally, for four of the participants where data was available for analysis, we evaluated potential disparate impact risks in using the cash-flow variables and scores in underwriting algorithms.[55] We found that the degree to which the cash-flow data was predictive of credit risk appeared to be relatively consistent across borrowers who likely belong to different demographic groups.[56] Rather than acting as proxies for race and ethnicity or gender, the cash-flow variables and scores appeared to provide independent predictive value across all groups. Moreover, when compared to traditional credit scores and attributes, the cash-flow based metrics appeared to predict creditworthiness within the subpopulations at least as well as the traditional metrics, and better in selected cases. These results suggest that cash-flow variables and scores do not create a disparate impact among protected populations.[57]

Areas for further research: While the results are instructive, we lacked the data to conduct several additional inquiries that would potentially be helpful to regulators, firms, and advocates in developing a deeper understanding of the data's value and limitations in modelling credit risk. Potential additional research topics include:

- A more granular analysis of which specific types of cash-flow variables and attributes are most predictive for underwriting small business and consumer products similar to those in our original research.
- Evaluation of the predictiveness of cash-flow data in underwriting loans with longer durations, larger principal amounts, and different product structures, such as secured loans.
- Evaluation of predictiveness more globally during different stages in credit and business cycles, on a pro forma basis if actual performance data is not available.
- Additional analysis of the extent to which cash-flow data is useful both in helping to underwrite populations that are largely shut out of the traditional credit reporting system as well as applicants who have more conventional credit histories.
- Evaluation of how companies may factor cash-flow variables and data into risk-based pricing models, which are often designed separately from eligibility algorithms though they may rely on some of the same data.
- Evaluation of the potential usefulness of cash-flow data in working with individual borrowers who have encountered financial difficulties due to an income or expense shock.

Thus, caution is needed with regard to extrapolating our empirical results beyond the parameters of the study. Nevertheless, we view the results as generally encouraging and as broadly consistent with the expected benefits of cash-flow based information based on the interviews with stakeholders as discussed above.

54 *Id.* at 30. The failure to obtain a traditional score may not indicate that a particular applicant is "credit invisible." For example, due to differences in coverage by the three nationwide consumer reporting agencies, some borrowers may lack a credit file with one company but still be scoreable by others. There are also differences in scoring thresholds and coverage among third-party scoring models. CFPB, Credit Invisibles at 4-6; FRB, Credit Scoring Report at 16-17.

55 As discussed in Box 3.2.1, fair lending law has two principal doctrines of liability. We focused on disparate impact risk because the participants used highly automated underwriting systems.

56 As discussed in Box 3.2.2, fair lending law prohibits the collection of demographic information in connection with the kinds of loans studied. Accordingly, we applied proxy methodologies to determine borrowers' likely demographics.

57 FinRegLab, Empirical Research Findings at 31.

BOX 3.2.1 DISPARATE IMPACT ANALYSIS

As discussed in Box 2.2.1, lending discrimination cases are brought on two principal bases: Disparate treatment cases focus on decisions made on the basis of protected characteristics, while disparate impact cases focus on situations in which a facially neutral practice has a disproportionately negative effect on members of a protected class, unless the practice meets a legitimate business need that cannot reasonably be achieved by less impactful means.

The Supreme Court confirmed in 2015 that both doctrines are available under the Fair Housing Act, but it has not yet ruled on the Equal Credit Opportunity Act. Federal regulations, agency guidance, and lower court decisions have recognized the disparate impact doctrine under both laws for several decades, following the same three-step analysis that applies in the employment discrimination context:

- At the first step, a plaintiff must make an initial showing that the particular practice causes a disproportionate adverse effect on protected classes.
- If that showing is made, the burden shifts to the creditor to show that the practice furthers a legitimate business need.
- In the third stage, the burden shifts to the plaintiff to demonstrate whether the legitimate business need can reasonably be achieved by using an alternative practice that would have less adverse impact on protected classes.

Statistical tests can be important at each stage, and more generally when lenders set out to evaluate their degree of fair lending compliance risk in adopting or changing their underwriting models. However, case law and regulatory guidance do not provide precise mathematical thresholds or definitions. With regard to the existence of a "legitimate business need," for example, regulatory guidance typically focuses on whether there is a "demonstrable relationship" between the variable or requirement and credit risk. For instance, banking agency guidance on credit scoring models focuses on whether the variable is statistically related to loan performance and has an understandable relationship to creditworthiness.

As discussed in Section 6.1.1, the Department of Housing and Urban Development and the Consumer Financial Protection Bureau have announced plans to reexamine the disparate impact doctrine in light of the Supreme Court's 2015 decision.

Sources: 12 C.F.R. § 1002.6(a); *id.* Supp. I, cmt. 6(a)-2; 59 Fed. Reg. 18267 (Apr. 15, 2014); Office of the Comptroller of the Currency, Bulletin 1997-24, app. at 11 (May 20, 1997); *Texas Dep't of Housing & Community Affairs v. Inclusive Communities Project, Inc.*, 135 S. Ct. 2507 (2015); 84 Fed. Reg. 42854 (Aug. 19, 2019); Consumer Financial Protection Bureau, Statement of the Bureau of Consumer Financial Protection on Enactment of S.J. Res. 57 (May 21, 2018); David Skanderson & Dubravka Ritter, Fair Lending Analysis of Credit Cards, Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper 34-40 (August 2014).

BOX 3.2.2 PROXY METHODOLOGIES

Federal law prohibits lenders from collecting demographic information on credit applicants and borrowers for most credit products. As a result, disparate impact analyses often can be conducted only by first applying proxy methodologies to estimate the likelihood that a particular borrower belongs to a particular demographic group.

Federal regulators and industry often use a method called Bayesian Improved Surname Geocoding to assess the likely race/ethnicity of borrowers. The technique uses surnames and geography of residence to calculate the likelihood of belonging to particular subpopulations based on a comparison to U.S. Census data. Proxy methodologies for gender often focus primarily on first names as reported by the Social Security Administration.

While such methods are commonly used and accepted by federal financial regulators, by their nature they are somewhat inexact. Academic research indicates that proxy methodologies can produce measurement errors in certain circumstances as both overinclusive (by assigning a high probability of belonging to the wrong group) and underinclusive (by assigning a low probability of belonging to the correct group).

Sources: 12 C.F.R. § 1002.5(b); Consumer Financial Protection Bureau, Using Publicly Available Information to Proxy for Unidentified Race and Ethnicity: A Methodology and Assessment (2014); Patrice Ficklin, Blog, Preventing Illegal Discrimination in Auto Lending, Consumer Financial Protection Bureau (Nov. 4, 2013); Yan Zhang, Assessing Fair Lending Risks Using Race/ Ethnicity Proxies, 64 Management Science 178 (2018); Jiahao Chen et al., Fairness Under Unawareness: Assessing Disparity When Protected Class Is Unobserved, Conference on Fairness, Accountability, and Transparency (FAT* '19) (January 2019).

3.3 Small business overview

The *Small Business Spotlight* provided a broader picture of cash-flow based underwriting in the small business market and an overview of policy issues that may be particularly important in determining the pace of expansion going forward. The report found evidence that reliance on electronic sources of cash-flow data for purposes of credit underwriting is growing more rapidly in small business markets than in consumer credit. More specifically:

Inherent underwriting challenges: Underwriting credit for small businesses is more challenging than lending to consumers or larger businesses due to a variety of factors, including high risks of business closure, lack of information, and relatively high operational costs relative to loan size. Lenders typically collect a wide variety of information to assess the health of small businesses, including cash-flow and other financial statements, bank records, tax records, business plans, and credit history to the extent it is available. Automation is also less widespread in small business lending. In the aftermath of the 2008 financial crisis traditional lenders that had pushed the farthest toward automated underwriting by relying on owners' personal credit scores and other relatively standardized inputs moved back toward judgmental underwriting and increased lending thresholds in ways that effectively excluded many smaller applicants, for instance by requiring two years of operations prior to extending any credit.[58]

Businesses owned by racial minorities, recent immigrants, and women face particular challenges in accessing credit. Substantial disparities in income and assets among demographic groups can impact owners' access to start-up equity funding and personal payment histories. As a result, small businesses owned by racial minorities, immigrants, and women may tend to have greater need for access to credit, but also more difficulty in obtaining it. Geographic access to lenders and heavy reliance on relationships and judgmental underwriting may also present challenges. Surveys and studies show substantial disparities in denial rates, particularly for traditional business loans. In addition, women and minority business owners are less likely to apply for business credit products because of fear of denial and may tend to rely relatively heavily on credit cards or personal credit compared to other businesses.[59]

Expanding use of cash-flow data: In part because there is a strong desire to facilitate automation and because traditional lenders have long relied on cash-flow data in other forms, use of electronic sources appears to be viewed as a relatively intuitive evolution in small business lending. After a group of new non-bank fintech companies pioneered use of transaction account records and other data in the aftermath of the financial crisis, it has since spread to a number of banks and community development organizations. It has also attracted a second group of new entrants such as e-commerce platforms, payment processors, and accounting software developers that are using data from their primary business activities to begin offering credit to small businesses.[60]

Research is not publicly available for many of these initiatives, but studies of fintech credit providers who are the most likely to use electronic cash-flow data suggest that they are having an impact on access to credit for underserved populations. Some sources estimate these lenders' share of the small business market for loans under $250,000 will reach 20 percent by 2020. This is a particularly important development because smaller, younger businesses tend to have high demand for loans of this size, but banks find them particularly difficult to make due to relatively high overhead

58 FinRegLab, Small Business Spotlight at 5-9.

59 *Id.* at 9-11.

60 *Id.* at 20-22 (noting news reports of use by such banks as Wells Fargo, JPMorgan Chase, Bank of America and various smaller institutions; community development financial institution Opportunity Fund; and new entrants Amazon, PayPal, Square, and Intuit).

BOX 3.3.1 SMALL BUSINESS BORROWER PROTECTIONS

Most federal consumer financial laws do not apply to small business borrowers. For example, standardization of disclosures about prices and product features is not required by federal law because the Truth in Lending Act is limited to products used primarily for personal, family, and household purposes. The Fair Credit Reporting Act has limited application in the commercial space, and Gramm-Leach-Bliley Act requirements regarding information security and data sharing apply only to consumers. However, the Equal Credit Opportunity Act and federal prohibitions against unfair and deceptive acts and practices have been applied to protect commercial borrowers.

The relative lack of federal protections for small business lending is attracting increased attention as product types and providers have diversified over the last two decades. Various stakeholders have raised concerns about the fact that many newer, technology-reliant providers of small business financing are providing products that are substantially more expensive than traditional sources of small business credit and that rely on different repayment provisions, such as daily or weekly remittances based on sales volume. Defenders assert that such practices are driven by higher costs and that structuring repayment terms to vary with sales volumes can be advantageous to small businesses. Critics assert that some products and practices are predatory and may trap borrowers in debt that will jeopardize their ability to maintain their businesses and access more favorable credit over time.

The U.S. Department of the Treasury called for greater borrower protections for small businesses in 2016. No new federal laws or regulations have been adopted since that time, although the Federal Trade Commission announced an enforcement initiative in 2019 looking at potentially unfair and deceptive acts and practices in merchant cash advances and other small business financing.

A New York law signed in August 2019 has restricted the use of certain contract provisions called "confessions of judgment," which allow lenders to get court orders to support collections on loans that they allege are delinquent without allowing borrowers a chance to dispute the allegations. California adopted a disclosure law in late 2018 that will take effect once proposed regulations are finalized. As part of a broader coalition of lenders, investors, and advocates, about 60 companies have also voluntarily adopted a "Small Business Borrowers' Bill of Rights" that addresses transparency, product structures, and various practices; the same group is advocating for federal truth in lending legislation.

Sources: Federal Trade Commission, "Strictly Business" Forum: Staff Perspective (2020); Barbara J. Lipman & Ann Marie Wiersch, Uncertain Terms: What Small Business Borrowers Find When Browsing Online Lender Websites, Board of Governors of the Federal Reserve System 19-20 (2019); U.S. Department of the Treasury, Opportunities and Challenges in Online Marketplace Lending 23-24, 28 (2016); FinRegLab, Small Business Spotlight at 25.

costs.[61] However, while use of cash-flow data is increasing, current initiatives appear to reflect a diversity of approaches as to the specific sources and uses of cash-flow data, such that the period of experimentation has not yet settled into standardization.

Policy issues: While these results are generally encouraging, stakeholders identified several issues that may affect the nature and pace of further growth going forward. These issues include the need for public research to inform further market development, such as securitization and resolving potential concerns from prudential regulators about whether cash-flow models will perform well during economic downturns; further assessment of cash-flow data's inclusion and fair lending effects; the need to structure lending processes consistently with broader notions of fairness, transparency, and privacy; concerns about the system that is used to transfer cash-flow information between companies; and technology and cost issues, particularly for smaller banks.[62]

61 *Id.* at 22 (reporting survey results suggesting that African-American and Hispanic applicants have higher approval rates for loans sourced through online lenders than small or large banks). However, satisfaction levels with online loans are typically lower among both minority and non-minority borrowers due to price and product terms. *Id.* at 22, 25.

62 *Id.* at 24-34.

4. MARKET SURVEY

The Use of Cash-Flow Data Today

Use of cash-flow data is spreading in consumer credit markets, but is uneven among different types of lenders. Data aggregators are playing a critical role in both consumer and small business lending by facilitating the transfer of cash-flow data between companies. But competitive, coordination, and compliance issues are a substantial source of uncertainty as cash-flow underwriting continues to evolve.

This section provides a snapshot of the business and technological processes that are used to effectuate cash-flow underwriting activities in U.S. consumer credit markets today, as well as describing the underlying transfers of cash-flow data between companies to facilitate both small business and consumer underwriting. While the latter topic was briefly discussed in our *Small Business Spotlight*, this report provides a more detailed description of transfer processes, technologies, and implementation challenges given the importance of the system for customer-permissioned data transfers to both credit markets.

4.1 How cash-flow data is being integrated into consumer credit underwriting processes

Fintech firms have pioneered the use of electronic cash-flow data in consumer underwriting over the last decade, in much the same way as in small business markets. Cash-flow data has also attracted interest from community development lenders working to reach underserved populations, and more recently from certain incumbents in the traditional credit reporting and scoring markets. But to date banks and credit unions have been using the data only to a limited extent in consumer underwriting.

This section focuses separately on describing the activities of non-bank actors and on the scope of bank activity.

4.1.1 Non-bank lenders and model developers

Fintech firms have grown over the last decade to supply approximately 40 percent of the market for unsecured personal loans.[63] Some fintechs act as direct lenders in their own right, while others have partnered with traditional financial institutions to originate loans. These companies, which are often called marketplace lenders, rely heavily on technology to manage customer acquisition, underwriting analyses, and service delivery.[64] Marketplace lenders generally do not provide transaction account services and may offer only a few types of credit products.[65] Some have also particularly emphasized increased use of non-traditional data in their highly automated underwriting systems, though not all fintechs use such data or cash-flow information in particular.[66]

Fintech companies that are using cash-flow data are generally focusing on unsecured loans, credit cards, and cash advances. Many products are for relatively small dollar amounts and short terms, though some student loan refinancing products are larger and longer.[67] Many of these companies are specifically targeting populations that are underserved by mainstream lenders in an attempt to build new markets for themselves and/or develop mission-driven brands that are distinct from traditional financial services providers. Some community development financial institutions have also begun using cash-flow data as a means of increasing access to underserved consumers.[68]

Non-bank data intermediaries and model developers are also developing scoring models and data reports that incorporate cash-flow data for sale to lenders. Three of these efforts are led by incumbents in the traditional consumer reporting and scoring markets who have partnered with data aggregators to obtain transaction account information. As discussed in Section 2.3, many of the credit reporting incumbents' initial alternative data initiatives focused on obtaining more data directly from landlords, utilities, or other primary sources, but in 2019 FICO, Experian, and Equifax announced projects that use traditional consumer-permissioned cash-flow data to supplement traditional information sources and/or scores.[69] Some data aggregators are also offering to assist

63 TransUnion, Press Release, FinTechs Continue to Drive Personal Loan Growth, transunion.com (Feb. 21, 2019) (reporting 38 percent market share based on loan volumes in 2018); Experian, Fintech vs. Traditional FIs: Trends in Unsecured Personal Installment Loans 3 (2019) (reporting 49 percent market share based on loan originations as of spring 2019). These sources treat unsecured personal loans separately from credit cards and student loans.

64 David W. Perkins, Marketplace Lending: Fintech in Consumer and Small-Business Lending, Congressional Research Service (updated Sept. 4, 2018); U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation 86-95 (2018) (hereinafter Treasury, Fintech Report); U.S. Department of the Treasury, Opportunities and Challenges in Online Marketplace Lending (2016) (hereinafter Treasury, Marketplace Lending Report).

65 However, a number of fintech lenders are diversifying their credit product offerings and beginning to offer payment services even if they do not provide transaction accounts. In small business credit markets, some payment processors are also crossing over to provide credit products. J. Christina Wang, Technology, the Nature of Information, and FinTech Marketplace Lending, Federal Reserve Bank of Boston Current Policy Perspectives No. 18-3, at 8 (Oct. 2018); S&P Global Market Intelligence, 2018 US Digital Lending Market Report 6 (2018); Nimayi Dixit, Payment Fintechs Leave Their Mark on Small Business Lending, S&P Global Market Intelligence (2018).

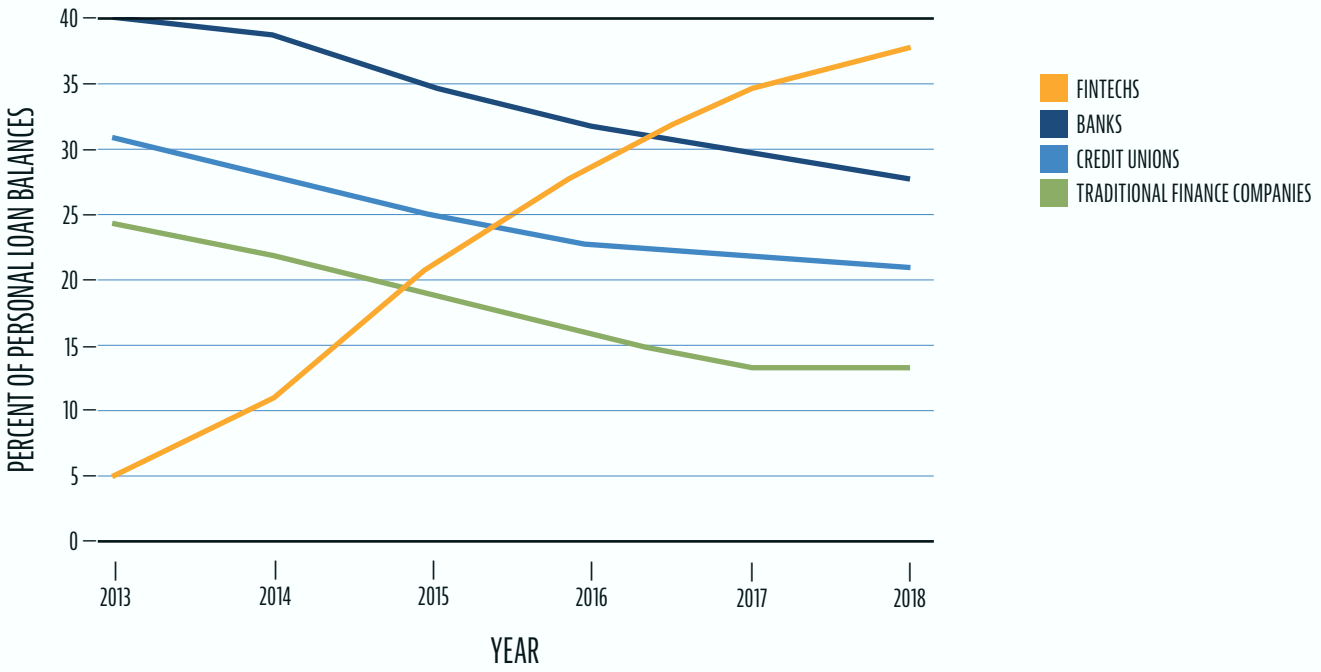
66 *See, e.g.,* Penny Crosman, Online Lenders Make Case for Cash-Flow Data While Acknowledging Pitfalls, Am. Banker (Aug. 5, 2019); Aite at 8-9, 12-14; Box 4.1.1.3. As discussed in Appendix C, sources analyzing marketplace lenders' customer bases vary but suggest that some lenders may not go as deep into non-prime populations as they are sometimes portrayed. In addition, some lenders have tightened standards in recent years in response to frustration with default rates among investors. *See, e.g.*, Andrew Latham, 2019 Personal Loans Industry Study, Supermoney (Aug. 9, 2019); Experian, Fintech vs. Traditional FIs at 5-8; Shahien Nasiripour, Fintech Lenders Tighten Standards, Become More Like Banks, Bloomberg (Dec. 16, 2019).

67 Many student loan refinancing companies are relying on some form of "free cash flow" metric to evaluate applicants' residual income after expenses rather than using a traditional debt-to-income ratio, though practices vary as to the sources of information and calculation methods. Jonathan Riber & Christopher D'Onofrio, U.S. Structured Finance Newsletter: Student Loan Refinance Sector—Not All Free Cash Flow Is Created Equal, Morningstar/DBRS (2019)/; Box 4.2.1 (discussing residual income analysis). Fintech companies that serve small business markets also offer longer and larger loans than in consumer markets, though they are relatively small and short-term products compared to the small business market as a whole. Because it generally costs traditional lenders about as much money to originate a loan of $100,000 as it does to originate a loan of $1 million, traditional lenders have tended to increase loan minimums over time, which in turn created an opening for marketplace lenders and other technology-oriented entrants to join the market. FinRegLab, Small Business Spotlight at 6-9, 19-22.

68 Section 3.1; FinRegLab, Small Business Spotlight at 20-22.

69 Stefan Lembo Stolba, Blog, What Is Experian Boost?, experian.com (Oct. 15, 2019); FICO, Introducing the Ultra-FICO Score, fico.com (visited Feb. 8, 2020).

BOX 4.1.1.1 MARKETPLACE LENDERS GAINING MARKET SHARE



Source: TransUnion, Press Release, FinTechs Continue to Drive Personal Loan Growth, transunion.com (Feb. 21, 2019)

Following the financial crisis, non-bank marketplace lenders have played an increasingly important role in providing credit to individuals and businesses. Some of these companies keep most of their loans on their own balance sheets, while others operate as "platform" lenders that partner with issuing banks to originate loans and match the loans to investors that want to purchase them. The latter companies consider themselves to be service providers rather than lenders in their own right for purposes of various state and federal laws, but both groups are sometimes referred to collectively in this report as fintech or marketplace lenders.

In both cases, marketplace lenders tend to operate almost entirely online, with no physical retail space. Their heavy reliance on technology and data tends to give them lower loan processing costs than traditional lenders, but they often have higher costs of funds and customer acquisition than depository institutions that can rely on deposits and existing customer bases.

Marketplace lenders now provide a greater share of the market for unsecured personal loans (not including credit cards or student loans) than traditional banks or finance companies. That segment of the consumer credit market has been growing extremely rapidly over the last several years, including among prime and near-prime borrowers.

Marketplace lenders' share of the small business market for loans under $250,000 has been estimated at approximately 4 percent as of 2015 and forecasted to reach 20 percent by 2020. Recent annual surveys of small businesses seeking loans, lines of credit, and cash advances indicate that more than 30 percent are applying to online lenders.

Sources: Perkins; Treasury, Fintech Report at 86-95; Treasury, Marketplace Lending Report; Federal Reserve Banks, 2018 Small Business Credit Survey: Report on Employer Firms 16 (2019); Federal Reserve Banks, 2017 Small Business Credit Survey: Report on Nonemployer Firms 16 (2018); Latham; TransUnion, Press Release, FinTechs Continue to Drive Personal Loan Growth; Experian, Fintech vs. Traditional FIs at 3; Business Insider Intelligence, One Area of US Alt Lending Is Recovering, Business Insider (Feb. 23, 2017).

BOX 4.1.1.2 RECENT CREDIT REPORTING INITIATIVES REGARDING CASH-FLOW DATA AND UNSECURED CREDIT

Several recent initiatives by credit reporting and scoring incumbents have potential implications for the use of cash-flow data in credit underwriting and for markets for unsecured personal credit in particular.

Experian Boost: NCRA Experian and data aggregator Finicity launched "Experian Boost" in 2019 to augment consumers' credit files where they authorize pulling positive payments information for designated utilities and telecommunications companies from their checking accounts. The results are reflected in scores that are generated based on Experian credit files for as long as consumers' bank accounts are connected, without lenders having to purchase a separate score.

As of late 2019, more than 1 million consumers representing 61 percent of all participants had improved their scores, with an average increase of 13 points using the FICO Score 8 model. However, improvement rates were higher (86 percent) among users with non-prime scores and/or thin files. Experian has not reported how many consumers' scores declined, but has noted that consumers can disconnect their accounts if that occurs and that their scores will revert to being calculated without the supplemental information.

UltraFICO: FICO, Experian, and Finicity are piloting a new model called UltraFICO that relies on consumers' permission to access their checking, savings, or money market data to generate a separate credit score using both cash-flow and traditional sources. The cash-flow elements include an analysis of such factors as the length of time that accounts have been open, recency and frequency of transactions, evidence of consistent cash on hand, and history of positive account balances. Lenders have to purchase UltraFICO scores separately.

Pilots include but are not limited to using the model as a "second look" for consumers who do not qualify for credit or for favorable terms using traditional scores. UltraFICO organizers have estimated that 15 million consumers can be scored using the new model even though they may lack sufficient credit history to generate a traditional FICO score. The information does not become a part of consumers' traditional credit files with Experian. The program is expected to expand in early 2020.

Equifax initiatives: Equifax announced two partnerships to take effect in 2020 that will provide consumers and small business applicants with opportunities to provide lenders with cash-flow data. One is a partnership with data aggregator Envestnet/Yodlee focused on U.S. markets to produce reports of cash-flow data and particular inferred variables (often called attributes), but not a specific score. The second is a worldwide partnership with a data aggregator called Urjanet that works with utility companies rather than banks. In both cases, the data will be provided separately from Equifax credit reports for applicants that authorize account access. Equifax already partnered with FICO in its capacity as manager of the National Consumer Telecom and Utilities Exchange to provide utility data to help fuel an earlier alternative credit score product called FICO XD.

FICO 10: FICO announced in early 2020 that it will roll out the next edition of its main generic scoring model later in the year. Though it does not involve cash-flow data, it has attracted attention from fintech lenders because it will analyze unsecured personal credit separately from installment loans. For instance, the new models will lower scores of consumers who take out unsecured loans to consolidate credit card debt and then run up their balances on their cards again.

Sources: Matt Tatham, Blog, More Than 1 Million Americans Have Improved Their FICO® Scores with Experian Boost, experian.com (Dec. 13, 2019); Stefan Lembo Stolba, Blog, Can Experian Boost Lower My Credit Score?, experian.com (Oct. 4, 2019); FICO, Introducing the Ultra-FICO Score; Bev O'Shea, UltraFICO Score Could Boost Credit Access for Consumers, nerdwallet (Jan. 24, 2019); Equifax, Equifax Enters into Credit Bureau-Exclusive Relationship with Envestnet/Yodlee to Further Extend Alternative Data Leadership, equifax.com (Nov. 7, 2019); AnnaMaria Andriotis, Need a Loan? Equifax Plans to Sell More Utility, Phone Records, Wall St. J. (Sept. 18, 2019); Equifax, Equifax Continues Leadership in Alternative Data with Worldwide Urjanet Partnership, investor.equifax.com (Sept. 18, 2019); O'Shea, FICO XD; Lisette Voytko, Report: FICO Credit Score Adjustments Could Hurt Consumers With Growing Debt, Forbes (Jan. 23, 2020); Arnold; Siegel Bernard.

lenders in building credit risk models with anonymized cash-flow data and/or analytics as an outgrowth of their primary role as data transmitters.[70]

Although multiple types of information can be derived from transaction account history and other sources of cash-flow data, the cash-flow scoring and underwriting models of which we are aware focus on financial variables that are reflected directly in the account history or can be derived from it. For example, current models may evaluate such attributes as:

70 See note 99 and accompanying text.

- The frequency, amount, and other measures of income deposited into the applicant's account;
- Payment and expense history, particularly for recurring obligations such as rent or mobile phone bills;
- Fluctuations in account balances and transfers to savings as a measure of financial reserves; and
- Patterns in how applicants manage their finances under different conditions, such as prioritization of particular expenses in low-balance periods.
- Lenders and model developers

Lenders and model developers may also be testing the ability to predict credit risk based on other types of non-financial data that may be revealed in transaction account information, such as the time and location of particular retail transactions or the company from which the purchase is made. However, as discussed in Section 6.1.1.1, there is caution about using such information for credit underwriting because of concerns about privacy, fair lending, and other risks.

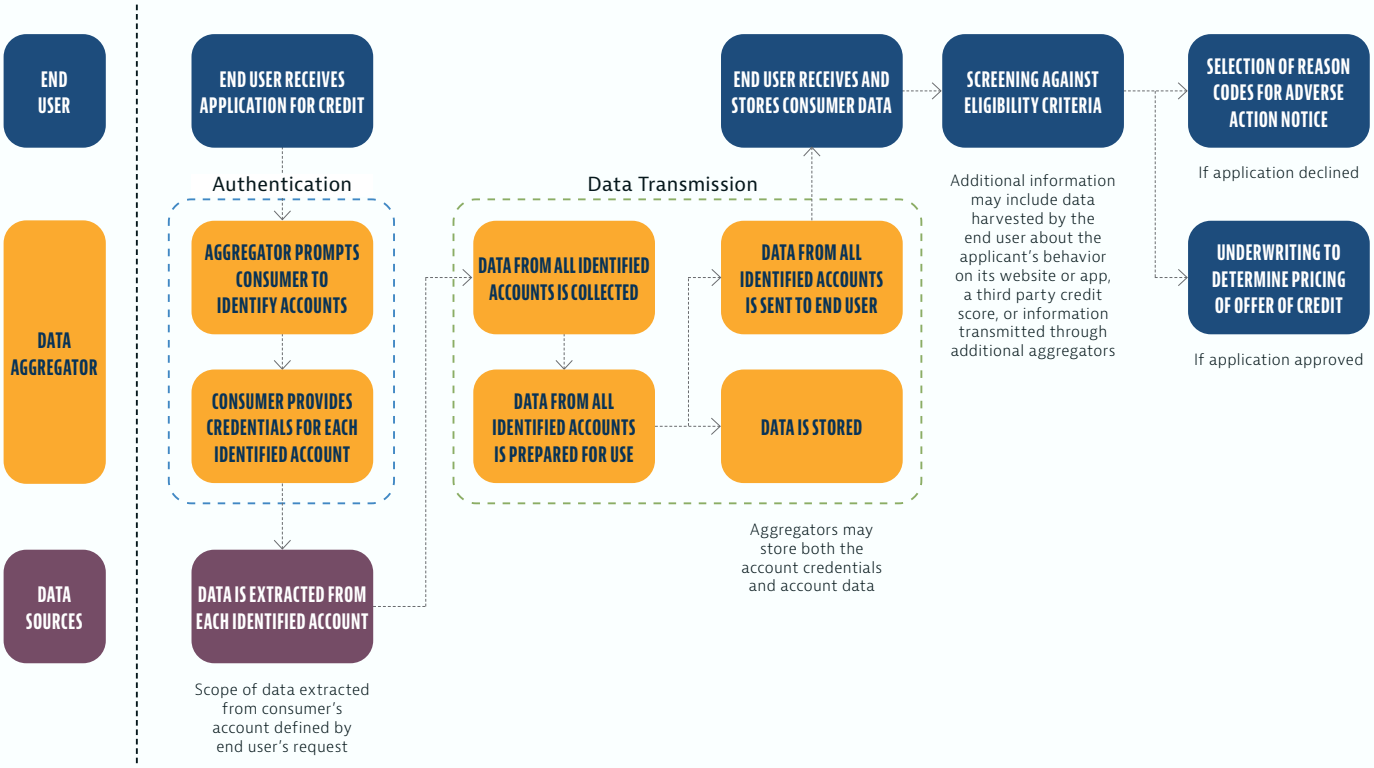
Lenders typically use cash-flow data both to help evaluate an applicant's eligibility for credit, as well as the price and amount of credit to be offered. However, firms vary as to whether they rely on proprietary or third-party models, the specific cash-flow variables they use, and where and how they obtain the data. Some use cash-flow information in initial decisionmaking, while others use it only in "second look" processes to consider applicants that were not approved initially using traditional criteria. Lenders also differ as to the extent to which they rely on traditional credit scores and other attributes from traditional credit reports: Some do not use traditional credit report information at all, others use such information where it is available but do not require that borrowers have scores in order to be underwritten, and some require traditional scores above particular thresholds. The particular empirical methodologies that lenders and model developers are using to analyze cash-flow data may also vary.[71]

Practices also vary as to whether cash-flow data is only pulled once during the initial application process, or whether it is pulled over time. For example, lenders who provide open-end credit and those who provide pricing discounts or other upgrades based on demonstrated performance may monitor borrowers' credit usage and financial status periodically to determine whether adjustments to credit terms are warranted. Providers of overdraft alternative products may also monitor balances regularly to determine when an advance may be warranted. Lenders and model developers may also reuse cash-flow data that was pulled initially for credit purposes for model refinement or other business activities, as discussed further in Section 6.1.3.

A final point of variation concerns the content, channel, and timing of customer communications relating to both the underwriting process and the transfer of the underlying data between companies. Although underwriting procedures are not typically a major focus of lender marketing, some firms have begun highlighting their reliance on cash-flow data to potential customers prior to the start of the application process. Depending on the company, such communications may be conveyed through general public website content or more targeted messages. The nature of the content also varies, with some communications primarily emphasizing the extent to which firms focus on transaction account data rather than traditional credit reports or scores, and others providing some degree of detail as to the actual criteria considered. The communications may reflect several motivations: conveying a mission-driven focus on expanding access to credit, differentiating

71 As discussed above in Box 2.4.1, traditional credit scoring models and other automated underwriting systems have generally relied upon statistical techniques such as logistic regressions to assess variables' ability to predict default. In recent years, some lender and model developers have begun to experiment with a variety of other computerized analytical methods involving machine learning or artificial intelligence.

BOX 4.1.1.3 HOW DATA SHARING HAPPENS



As discussed further in Section 4.2, transfers of transaction account data are typically effectuated using an intermediary called a data aggregator. The following discussion describes a somewhat stylized aggregation process for how a lender obtains cash-flow data from a bank via an aggregator in order to evaluate an application for credit.

Data sharing begins when an individual applies for credit and authorizes the lender to obtain information from the bank or other financial institution that holds the applicant's transaction accounts. The specific disclosures provided to the applicant vary from lender to lender, but generally most details are specified in the lenders' terms and conditions.

In the course of providing authorization, applicants identify the account(s) from which data will be drawn and typically provide their user identification and password for the relevant banking platform(s). The interface to collect this information is often provided by the lender's aggregator, in part because lenders do not want access to login credentials. However, labelling on the interfaces may vary, for instance as to the use of banks' logos. Some stakeholders have raised concerns that it may not be clear to applicants that they are not actually logging on to their banks' websites, but instead are providing their credentials to the aggregator and/or lender so that those firms can subsequently log on to obtain the information in accordance with the lender's terms and conditions. The interfaces do not generally restate key terms and conditions or provide mechanisms for applicants to tailor their authorizations as to particular data elements, the time periods covered, or other issues.

Where data is collected using tokenization and an application programming interface (API) rather than through credential sharing, the authorization processes are somewhat different. The applicant in that case generally will log into their bank's website, specify the accounts and the general type of data that they want to be shared, and the bank will send tokens to the applicant or the end user to use in initiating the collection process. Tokens cannot be used to conduct transactions on the underlying accounts and generally expire after specified periods.

Once applicant authorization is obtained, the aggregator extracts the relevant data from the accounts identified by the applicant, processes it, and transmits it to the lender. The lender or other end user will then evaluate that data as part of its underwriting process, which may also incorporate other sources of information such as traditional credit reports and generic credit scores, information from other aggregators, data for accounts that the applicant already has with the user, and/or information about the applicant's interaction with the user's website or app.

The underwriting process will determine whether the applicant satisfies the eligibility criteria and if so, the price at which credit will be offered. The eligibility and pricing determinations effectively happen simultaneously, without additional data pulls.

the product or offering as innovative, and/or signaling improved prospects for success to the pool of potential applicants that comprises the lender's target clientele.

During the application process itself, lenders provide additional information in the course of obtaining consumer permission to pull the cash-flow data for use in the underwriting process. The information may be provided in standalone disclosures and/or more generalized terms and conditions documents. Again, content varies, both as to whether and in how much detail lenders describe the potential benefits and risks of using cash-flow data and of the transfer of the underlying information. The interface for authorizing the data transfers may actually be operated by the data aggregator rather than the lender. See Section 4.2.2. for a more detailed discussion of the technologies and processes used for data transfer.

4.1.2 Bank activity

Banks have long used cash-flow data to operate overdraft programs for checking account customers, and more recently may have begun obtaining such data electronically to verify mortgage applicants' income and employment as required by federal law.[72] Yet they have not publicly embraced cash-flow data for consumer credit underwriting in the same way that many have in small business markets. Although some sources have predicted that use of transaction account data in consumer credit underwriting will become the norm among depository institutions within a few years, both published reports and stakeholder interviews suggest that current use is limited and uneven in consumer markets.[73]

For example, a 2018 survey of 22 large fintech and bank lenders found that while cash-flow data was the most popular source of alternative data among respondents as a whole, bank participants reported that their institutions were largely only using it in pilot phases and only as a supplemental source of information for existing customers, perhaps in a second-look posture.[74] Other sources suggest that banks may be considering transaction account history in deciding where to concentrate their efforts in cross-selling credit products to existing customers, and may be more willing to provide credit cards with modest limits to help existing deposit account customers build credit histories.[75] But compared to small business lending, there are very few published reports of banks launching specific consumer lending initiatives based on leveraging cash-flow data, either on their own initiative or in partnership with fintechs.[76] Thus, even if they are using it in limited ways when dealing with existing customers, banks do not generally appear to have built cash-flow data into

72 Overdraft programs have generally been treated as distinct from other types of credit activity for various historical and regulatory reasons. *See generally* 79 Fed. Reg. 77102, 77116-120 (Dec. 23, 2014). For general discussions of the pressures encouraging automation in mortgage verification requirements, see 12 C.F.R. § 1026.43(c)(3), (4); Oliver Wyman, A New Age in Mortgage (2017); CBInsights, Data Is Unlocking the Mortgage Tech Business, cbinsights.com (June 29, 2017).

73 *See, e.g.,* Aite at 11-13; Carroll & Rehmani at 9 (reporting as of 2017 that a few banks had begun developing systems to use checking account data and predicting that it will become the norm over the next 5 to 10 years); Browdie; McKinsey & Co., New Credit-Risk Models for the Unbanked 5 (2012) (noting that many large banks did not use transaction account data in underwriting credit for existing customers).

74 Aite at 11-13. With regard to alternative data overall, banks were less likely to use such data for marketing, fraud prevention, or underwriting, and more likely to use it for account monitoring and collections. In contrast, all fintech and other non-bank respondents reported using alternative data for underwriting, and the majority also used it for marketing and preventing fraud. *Id.*

75 Consumer Financial Protection Bureau, Data Point, Becoming Credit Visible 33-34 (2017) (questioning whether some commercial banks may be offering unsecured credit cards to customers with deposit accounts).

76 Robert Clark et al., Digital Lenders Price Loans Inside a Black Box of Alternative Data, S&P Global Market Intelligence (Nov. 8, 2018); PYMNTS, US Bank Launches Loan to Compete with Payday Lenders, pymnts.com (Sept. 11, 2018); Browdie (reporting in 2015 that Regions Bank found that cash-flow data allowed it to approve applicants for credit cards whose FICO scores tend to be 20 points below what the bank otherwise requires and that a few other banks reported using some internal data); FinRegLab, Small Business Spotlight at 20-22. A number of fintech companies are providing automated services and online platforms to facilitate banks' consumer lending originations, but it is not clear that these services involve substantial changes to the data that banks are considering in their underwriting models. *See generally* Will Hernandez, The Changing Shape of Bank-Fintech Partnerships, Am. Banker (Oct. 29, 2019); Zack Miller, Al Goldstein on Avant's Move into Powering Digital Lending for Banks with Amount, Tearsheet (Sept. 13, 2019); American Bankers Association, The State of Digital Lending 7 (2018).

their core underwriting models for use in evaluating all applicants, particularly including potential first-time customers.

Given that banks have direct access to large amounts of account data, they are relatively well positioned to evaluate research questions about the predictiveness of the data through modelling and pilot programs. Nevertheless, several factors may be slowing the pace at which they embark on such initiatives in consumer credit markets relative to small business lending. And in both markets, various factors often slow the pace at which banks adopt technology and process innovations relative to non-bank competitors. Relevant factors include:

- **Market distinctions:** Perhaps because automated underwriting and traditional credit scoring have penetrated more deeply in traditional consumer credit markets than in small business lending, there may simply be less motivation for banks to make substantial investments to change their current practices in the first instance. Forecasting future income and analyzing cash flows have always been important but challenging aspects of small business lending, so lenders of all types may be more open to adopting new electronic sources that permit more streamlined and sophisticated analyses. Another factor may be banks' general approach to different market segments; although some banks that pulled back from small business lending markets after the 2008 financial crisis have since made substantial efforts to return, many have not returned to non-prime consumer lending over the last decade. For instance, while large banks have increased their exposure by providing warehouse lines of credit to non-bank lenders in the last few years, they appear relatively reluctant to increase direct lending.[77] As discussed further in Section 5.2, a range of economic and regulatory factors may be influencing their approach to this market segment.
- **Technology and resource constraints:** Particularly for smaller banks and credit unions, technology hurdles and other resource constraints can be substantial. While improvements in computer capacity and data access have made it easier for small companies to build their own scoring and underwriting models, developing automated underwriting systems (or adjusting existing systems) still requires up-front investment and can be cumbersome when dealing with legacy technology systems. Smaller banks and credit unions are also substantially dependent on the vendors that manage their deposit platforms, and in the past few years have complained that these core processors are not sufficiently responsive in facilitating digital capabilities and fintech partnerships. Some core processors' fee structures can also make it expensive for small banks (or their partners or customers) to access their own data.[78] Finally, human capital can also be a significant limitation, both in

77 *See, e.g.,* Matt Phillips, Risky Borrowing Is Making a Comeback, but Banks Are on the Sideline, N.Y. Times (June 11, 2019); Michelle Davis, JPMorgan Leads Banks Flight from Poor Neighborhoods, Bloomberg (Mar. 6, 2019); Clark et al.; Ben Cukier, In the Battle Between Online Lenders and Banks, Data Wins, Forbes (Oct. 3, 2018); Andriotis, Why Your FICO Score Could Get a Boost; Lydia DePillis, Banks Are Walking Away from Low-Income Homebuyers, CNN (May 11, 2018); Peter Rudegair et al., Big Banks Find a Back Door to Finance Subprime Loans, Wall St. J. (Apr. 10, 2018); Goldman Sachs Global Markets Institute, Who Pays for Bank Regulation? 6-10 (2014) (tracking banks' shift toward prime borrowers and higher prices in various consumer lending markets). As discussed further in section 5.2.1.2, banks have a long history of entering and then exiting the market for small dollar credit due to economic considerations and other factors; where they do make investments, it tends to be relatively early in the credit cycle. Todd H. Baker, FinTech Alternatives to Short-Term Small-Dollar Credit: Helping Low-Income Working Families Escape the High-Cost Lending Trap, Harvard Kennedy School Mossavar-Rahmani Center for Business & Government.

78 Cheryl Winokur Munk, How Community Banks Are Innovating from the Core, Independent Banker (Aug. 1, 2019); Telis Demos & Rachel Louise Ensign, Frustrated by the Tech Industry, Small Banks Start to Rebel, Wall St. J. (Apr. 11, 2019); American Bankers Association, Understanding APIs (2019); Will Hernandez, Can Core Providers and Small Banks Settle Grievances in 2019?, Am. Banker (Dec. 28, 2018).

competing with larger institutions and fintech startups to recruit technical expertise and in the expenditure of compliance resources to satisfy regulatory concerns.[79]

» **Regulatory uncertainty:** Banks and credit unions are also subject to ongoing monitoring for both safety and soundness purposes and compliance with consumer protection laws, and thus may tend to be more reluctant to make changes in underwriting models absent interpretive guidance on specific legal questions and positive signals from regulators with regard to particular innovations more generally.[80] While most federal consumer financial

BOX 4.1.2.1 FEDERAL SUPERVISION OF FINANCIAL SERVICES PROVIDERS

Historically, banks and credit unions have been subject to periodic examinations by federal prudential regulators such as the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA), as well as by state regulators for state-chartered institutions. The examinations focus both on the general safety and soundness of the institutions and on compliance with federal consumer protection laws.

However, except for vendors who provide third-party services to banks and credit unions, non-banks historically were not subject to examination by federal agencies and were subject to varying degrees of state monitoring. In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) created the Consumer Financial Protection Bureau (CFPB) and vested it with authority to conduct consumer protection examinations of certain non-banks and very large banks with more than $10 billion in assets. Responsibility for consumer protection examinations for other banks remained with the prudential regulators.

The scope of the Bureau's authority to supervise non-banks varies by market. For instance, the CFPB can examine lenders of any size that extend mortgages, private education loans, or payday loans, but can only examine "larger participants" in other markets after defining the size thresholds for particular markets by rule. The Bureau has defined the thresholds for larger participants in consumer reporting, auto lending/leasing markets, and several other categories of financial services, but has not addressed data aggregators or other types of consumer loans.

Similar to the federal prudential regulators, the CFPB has authority to conduct consumer compliance examinations of vendors who act as third-party service providers to banks and non-banks that are subject to its primary examination authority. It also has authority to examine vendors that serve a substantial number of banks that fall below the $10 billion threshold for direct CFPB supervision. See Boxes 4.1.2.2 and 4.2.3.1.

The Bureau also has authority to examine individual non-banks that it determines to be engaging in conduct that poses risks to consumers after providing notice and an opportunity to respond to the firm. However, the CFPB does not have authority to examine firms of any type with regard to certain information-security related requirements under the Gramm-Leach-Bliley Act (GLBA) and Fair Credit Reporting Act (FCRA), although it occasionally has acted on information security issues pursuant to its authority to prevent unfair, deceptive, or abusive acts and practices. Enforcement authority for the GLBA and FCRA information security requirements as applied to non-banks is vested in the Federal Trade Commission, but the FTC does not have authority to conduct periodic examinations. See Section 5.2.2.

Sources: 12 U.S.C. §§ 1867, 5481(26), 5514-5516; 12 C.F.R. §§ 1090.100-.108; Andrew Smith, Federal Trade Commission, Testimony before the House Committee on Oversight and Reform Subcommittee on Economic and Consumer Policy (Mar. 26, 2019); U.S. Government Accountability Office, Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies 16-29 (2019); Federal Trade Commission, Privacy & Data Security Update: 2018, at 5-6 (2019); U.S. Government Accountability Office, Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach 26 (2018); Consumer Financial Protection Bureau, Complaint for Permanent Injunction and Other Relief, CFPB v. Equifax, Inc., No. 1:19-cv-03300-TWT (N.D. Ga. July 22, 2019); Consumer Financial Protection Bureau, Consent Order, In re Dwolla, Inc., File No. 2016-CFPB-0007 (Mar. 2, 2016).

79 The Financial Brand, Banking's Digital Talent Crisis: Who Will Fill the Tech Void?, thefinancialbrand.com (Jan. 16, 2018); Jim Marous, Can Community Banks and Credit Unions Survive in Today's Digital World?, thefinancialbrand.com (Oct. 19, 2017); Joseph McCafferty, Compliance Staffing a Key Risk for Banks, Internal Audit 360 (May 28, 2019). For an analysis of various factors driving compliance challenges relative to bank size generally, see Drew Dahl et al., Compliance Costs, Economies of Scale, and Compliance Performance: Evidence from a Survey of Community Banks, Federal Reserve Bank of St. Louis (2018).

80 See Section 5.2.1.3.

BOX 4.1.2.2 REGULATORY CONSIDERATIONS FOR LENDERS CHANGING THEIR UNDERWRITING MODELS

Federal consumer financial protection laws generally apply to all lenders regardless of charter type. But lenders who are supervised by the banking regulators and/or the CFPB are subject to additional regulatory expectations when adopting new underwriting models or changing existing ones.

Compliance with federal consumer protection laws: Several federal laws apply when providing credit to consumers and/or small businesses. For example, as discussed in Section 6.1.1, fair lending laws prohibit discrimination on the basis of race, ethnicity, gender, and various other bases in both consumer and commercial lending. The laws have been interpreted not only to prohibit direct consideration of protected class status, but also the use of facially neutral variables or practices that have disproportionately negative effects on protected classes unless those practices are meeting a legitimate business need that cannot be reasonably achieved by less impactful means. Lenders are also prohibited from using medical data in certain ways in connection with consumer credit underwriting.

Federal laws also impose disclosure requirements on various topics in connection with marketing, the application process, and application denials or other "adverse actions." Mandatory disclosures are more extensive for consumers, although adverse action requirements apply to business credit as well. Depending on the circumstances, relevant laws include the Truth in Lending Act (TILA), Equal Credit Opportunity Act (ECOA), Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA).

More broadly, prohibitions on unfair, deceptive, and/or abusive acts and practices under the Federal Trade Commission Act and the Dodd-Frank Act apply both to customer communications and substantive business practices, including both use of data and information security. The FTC has investigated and brought cases for unfair and deceptive acts and practices involving small business owners as well as consumers.

Other laws affecting data access, use, and/or disposal include the FCRA with regard to "consumer reports" as defined under that law and GLBA, which restricts lenders' ability to share consumer data with nonaffiliated companies and requires adoption of information security safeguards to protect customer data. These laws generally do not apply to small businesses. See Box 3.3.1 for more discussion of business borrower protections.

Model risk management: Federal prudential regulators have issued extensive guidance outlining their expectations for steps that banks should take in developing, monitoring, and using models that they use for credit underwriting and other decisionmaking processes to reduce the risk that the models do not produce unexpected losses, compliance problems, or other negative outcomes. The guidance also addresses topics such as governance, policies, and controls.

The guidance notes that banks sometimes rely on vendors to develop and operate models, and acknowledges that exercising due diligence on such arrangements can be challenging because vendors consider their methods to be proprietary. Nevertheless, the guidance emphasizes that banks are expected to conduct their own validation and ongoing monitoring processes, even if they do not have full access to computer coding and implementation details.

Third-party service provider monitoring: In addition to the expectations outlined in the model risk governance guidance, both the federal banking regulators and CFPB have issued separate general guidance about their expectations for firms that are subject to direct supervision by the agencies when dealing with vendors.

The documents emphasize that supervised entities are responsible for the compliance performance of their vendors, and thus should create risk management programs to subject service providers to both initial due diligence and ongoing monitoring. The banking agencies have also issued more specific guidance with regard to technology vendors and information security risks. Each agency has emphasized handling of sensitive customer data as a high-risk activity that warrants greater scrutiny.

Sources: FRB, Supervisory & Regulation Letter 13-19; FRB, Supervisory & Regulation Letter 11-7; OCC, Bulletin 2013-29; OCC, Bulletin 2011-12; FDIC, Financial Institution Letter 19-2019; FDIC, Financial Institution Letter 22-2017; FDIC, Financial Institution Letter 44-2008; CFPB, Compliance Bulletin and Policy Guidance 2016-02; 12 U.S.C. §§ 5531, 6801-6809; 15 U.S.C. §§ 45, 1601-1665, 1681-1681x, 1691-1691f.

protection laws apply regardless of charter type, banks are subject to more rigorous and detailed expectations than many non-bank lenders on topics such as the development, validation, and governance of underwriting and other predictive models[81] and on monitoring the compliance activities of any third-party service providers.[82]

These expectations may lead banks more generally to presume that they will face a high burden of proof to demonstrate that potential gains from any changes to their underwriting models (whether developed in-house or with assistance from vendors) outweigh potential regulatory concerns, and to hesitate to invest the time and resources needed to convince regulators that modifications are warranted.[83] As discussed further in Section 5.2.1.3, the December 2019 statement by five federal agencies may be helpful in this regard because it recognizes that cash-flow information may present both greater benefits and lower risks than other alternative data, and emphasizes that regulated entities can consult the agencies in planning their use of new data sources. However, it does not provide specific guidance on compliance and interpretive issues, either with regard to the underwriting process or the transfer of cash-flow information between companies.[84]

4.2 How acquisition of cash-flow data occurs today

As discussed above, acquisition of data is a critical process for cash-flow underwriting in both consumer and small business markets, particularly for non-bank firms that do not offer account services. While lenders obtain electronic cash-flow data directly from the original sources in limited circumstances,[85] the dominant model in the U.S. particularly with regard to bank account information is for a group of non-bank technology intermediaries called data aggregators to obtain financial data from designated deposit accounts and transmit it to the lender or other downstream user.[86] Because the number of aggregators is quite small compared to thousands of financial institutions, it is currently far

81 Board of Governors of the Federal Reserve System Supervisory & Regulation Letter 11-7 (Apr. 4, 2011); Office of the Comptroller of the Currency, Bulletin 2011-12 (Apr. 4, 2011); Federal Deposit Insurance Corporation, Financial Institution Letter 22-2017 (June 7, 2017).

82 Board of Governors of the Federal Reserve System, Supervisory & Regulation Letter 11-7 (Apr. 4, 2011); Federal Deposit Insurance Corporation, Financial Institution Letter 22-2017 (June 7, 2017); Office of the Comptroller of the Currency, Bulletin 2011-12 (Apr. 4, 2011). There are reports that some banks are being required to obtain pre-launch approval from their examiners for non-traditional underwriting models, though the guidance on model risk governance does not indicate that such approval is required. Bank Policy Institute & Covington, Artificial Intelligence Discussion Draft 19 (2019).

83 These dynamics are not fundamentally different between consumer and small business markets, though there may be fewer outstanding compliance questions in small business lending because certain federal consumer protection laws do not apply in that context and a lack of data creates differences in the enforcement of some requirements. FinRegLab, Small Business Spotlight at 24-34.

84 Interagency Alternative Data Statement at 2, 3; Section 6.1.

85 For example, some small business lenders and lending platforms have negotiated directly with accounting software providers or other sources to transfer information as directed by the applicant via an application programming interface (API), which as discussed below is a software intermediary that allows two websites or applications to exchange information. Small Business Spotlight at 22. A few U.S. banks are also adopting more open forms of data access to fintech companies generally, although it is not clear the extent to which they are providing access to lenders who may compete with the banks' own products. *See, e.g.,* Bryan Yurcan, Open Banking's Early Adopters Bet on 'Tremendous Value," Am. Banker (Feb. 1, 2018).

86 For purposes of this report, we use the term "data aggregators" to refer to intermediaries who focus predominantly on transferring financial data at the specific direction of the consumer or small business to which the data pertains. As discussed further below, data aggregators emerged initially to serve markets for personal financial management and payments, but now sometimes participate in data transfers relating to credit underwriting. Because they operate with applicant permission, they are somewhat operationally distinct from traditional credit bureaus, which generally do not need consumer consent for most of their activities under the Fair Credit Reporting Act as discussed in Box 2.1.1 and in section 6.2. As used in this report, "aggregators" does not include a second set of newer intermediaries called "data brokers," which collect information about consumers for marketing, fraud detection, and other non-credit purposes and which operate largely without consumers' knowledge or consent. The potential application of the Fair Credit Reporting Act to both aggregators and brokers is fiercely disputed. See Section 6.1.1.2; *see also* Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability (2014).

more efficient for end-users to connect to aggregators than to the platforms of individual banks and other account sources.[87]

Over the past 20 years, data aggregators have become the hub of a new information transfer system that has evolved to support a broad range of financial products and services. Although statistics are difficult to obtain, some reports indicate that the customer-permissioned data transfer system now provides coverage for at least 95 percent of U.S. deposit accounts, and some shareholders estimate that as many as 100 million consumers may have authorized transfers for one or more purposes.[88] Transfers to facilitate credit underwriting reportedly represent a relatively small portion of this overall market, although they are growing.[89]

Questions about whether and how activities within this new system should be treated under federal consumer protection laws have not been resolved by federal regulators, although the Consumer Financial Protection Bureau and several private groups have released broad-based principles for how customer-permissioned data sharing should be structured to protect consumer and small business interests.[90] In the absence of more definitive guidance, stakeholders disagree on such issues as application of § 1033 of the Dodd-Frank Act, which vests consumers with the right to obtain transaction and account data from their financial services providers; how liability for unauthorized account activity would be allocated in the event of a misuse of consumer login credentials or data; and whether aggregators are "consumer reporting agencies" under the Fair Credit Reporting Act when they transfer cash-flow data to facilitate credit underwriting. Those issues are analyzed in greater detail in Sections 5 and 6, but as discussed immediately below, uncertainty over these questions is increasing tensions between different actors as they engage with each other through the new data transfer system.

87 Some of the largest U.S. aggregators include Envestnet/Yodlee, Finicity, Fiserv/CashEdge, MX, Morningstar/ByAllAccounts, Plaid, and Quovo, which was bought by Plaid in early 2019. Treasury, Fintech Report at 25 & n.45; DeLeon; Donna Fuscaldo, Plaid Buys Quovo in Its First Major Acquisition, Forbes (Jan. 8, 2019); Jarred Keneally, Blog, Intuit Financial Data APIs (CAD) Update, intuit.com (Mar. 15, 2016). In 2019, Fidelity also announced the formation of a company called Akoya that it described as being intended to act as a hub between banks, data aggregators, and fintechs. See Section 4.2.4 for discussion of Visa's acquisition of Plaid and several large banks' investments in Akoya in early 2020.

88 Indeed, one aggregator alone reportedly has transferred data for about 25 percent of U.S. accounts on behalf of more than 11,000 firms. Deleon; Miller, Plaid Expands Financial Service API; Julie Verhage & Tom Metcalf, Plaid's Founders Are Latest Fintech Royalty with Visa Deal, Bloomberg (Jan. 14, 2020). Statistics on prepaid account coverage are not available, but an April 2019 rule by the Consumer Financial Protection Bureau gives consumers more access to electronic information about their account histories. See note 39.

89 Mary Wisniewski, Data Aggregation's New Frontier: Lending Decisions, Am. Banker (Mar. 6, 2017); Steve Smith, How Data Aggregation Can Shake Up Credit Decisioning, infoworld.com (Dec. 15, 2017).

90 *See, e.g.,* Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (2017) (hereinafter CFPB, Data Sharing Principles); American Law Institute, Tentative Draft, Principles of the Law: Data Privacy (2019); American Bankers Association, Statement for the Record to the Task Force on Financial Technology Regarding 'Banking on Your Data: The Role of Big Data in Financial Services' (Nov. 21, 2019); World Economic Forum, The Appropriate Use of Customer Data in Financial Services (2019); Financial Data Exchange, Organization Overview; World Economic Forum, White Paper, The Appropriate Use of Customer Data in Financial Services (2018); Consumer Reports et al., The Digital Standard (2017); Center for Financial Services Innovation, Liability, Transparency and Consumer Control in Data Sharing (2017); Center for Financial Services Innovation, CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration (2016). See sections 5.2.2.1 and 6.1 for further discussion.

BOX 4.2.1 OVERVIEW OF § 1033 AND DATA SHARING PRINCIPLES

In 2010, Congress adopted a provision in the Dodd-Frank Act that establishes consumers' rights to access their own account and transaction information to the extent that it is maintained by providers of consumer financial products and services in the ordinary course of business. However, the Consumer Financial Protection Bureau has not yet issued rules to implement § 1033 or addressed whether it has taken effect in the absence of regulations. See Box 5.2.2.1.2 for more details.

The Bureau also has not issued guidance addressing the treatment of data aggregators or scenarios involving misuse of consumer login credentials under the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, or Electronic Fund Transfer Act, or whether aggregators are subject to CFPB examination under its rule defining thresholds for supervision in the consumer reporting market.

In 2017, the Bureau issued a set of Data Sharing Principles that express its "vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value." The principles describe the scope of data access by consumers and authorized third parties, list topics that should be fully and effectively disclosed to consumers prior to them providing authorization for data access, call for robust security and accuracy processes, and endorse the provision of mechanisms that allow individuals to monitor data access, revoke consent, and compel data deletion at their discretion. However, the Bureau emphasized that the principles do not by themselves establish binding requirements or obligations, though some aspects may accord with protections that already apply to the market under existing statutes and regulations.

Private organizations have also released principles for data access, transmission, and use in financial services or more broadly. Like the Bureau principles, they tend to emphasize the importance of informed consent, effective transparency and control mechanisms, and data security and integrity.

Sources: 12 U.S.C. § 5533; CFPB, Data Sharing Principles; American Law Institute; American Bankers Association, Statement for the Record; Financial Data Exchange, Operational Overview; World Economic Forum, White Paper.

4.2.1 Data aggregators

Data aggregators first emerged in the U.S. about 20 years ago largely to support various types of wealth advisory and "personal financial management" (PFM) services that provide consumers with consolidated information from and/or access to their credit, payments, and asset management accounts.[91] Later start-ups focused on facilitating payments activity by fintechs.[92] Over the years, aggregators' business models have evolved, with some offering PFM platforms directly to consumers and others partnering with banks, non-bank lenders, and various other types of financial services providers to facilitate data acquisition for a growing range of use cases. In connection with credit products specifically, aggregators provide account data to some users simply to verify income, employment, or assets, and to others who distill particular cash-flow metrics for use in underwriting. More recently, as discussed above, at least two aggregators have begun working with traditional credit reporting agencies and model developers on initiatives to bolster credit underwriting through use of cash-flow data.[93]

Typically, aggregators are paid for transmission services by lenders or other end users, rather than by the consumer or small business applicant or the firm from which that applicant's data is being acquired. Fees may be incurred on a per transmission basis or through volume-based subscriptions. As discussed further below, many aggregators are working to establish agreements with

91 *See generally* 81 Fed. Reg. 83806, 83808 (Nov. 22, 2016); Treasury, Fintech Report at 160-62; Hiroshi Fujii et al., E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific, MIT Composite Information Systems Laboratory Working Paper 2002-06, at 1-4 (September 2002).

92 Kate Rooney, Meet the Start-Up You've Never Heard of That Powers Venmo, Robinhood, and Other Big Consumer Apps, CNBC (Oct. 4, 2018); Alex Konrad, Fintech's Happy Plumbers, Forbes (April 12, 2018).

93 See Box 4.1.1.2.

BOX 4.2.1.1 DATA AGGREGATOR USE CASES

Data aggregation started to facilitate personal financial management (PFM) and other wealth advisory services. PFM platforms, which are provided both by fintechs and banks, help users consolidate their financial account data in one place so that they can manage their finances. Many applications provide budgeting analysis and advice, such as visualizations of trends, budgets, and net worth. Over time, providers have added a number of additional features, such as balance and suspicious transaction alerts, savings programs, bill pay options, investment management services, and/or product recommendations.

A second cluster of use cases for data aggregation involve account verification and payments-related support activities. Using account aggregation technology can eliminate the risk that consumers will mistype their account and routing numbers and the need for "micro-deposits" over one or more days to confirm account ownership before conducting larger transactions. Payment services providers may also use account aggregation services to verify account balances before effectuating transfers or to retrieve billing information to help consumers pay bills electronically. Companies that provide international money transfers, person-to-person transfers, and digital currency services are particularly likely to use data aggregators.

Credit-related use cases have also increased in recent years. For example, some lenders use data aggregators to verify information that is reported by applicants regarding income, assets, and employment, particularly in the context of mortgage lending where federal law generally requires lenders to collect third-party documentation in the course of assessing consumers' ability to repay. Fannie Mae and Freddie Mac have partnered with data aggregators to provide verification services to mortgage underwriters. For example, mortgage underwriters can use Fannie Mae's "Day 1 Certainty" to have borrowers connect their financial accounts and validate income, assets, and employment from their cash-flow data. Fannie Mae states that Day 1 Certainty decreases validation time by six to eight days. Other lenders are using data aggregators to collect more detailed cash-flow information for use in their credit underwriting models.

Different use cases may involve substantially different patterns of data acquisition by data aggregators and end users. For instance, verification of income for credit underwriting is likely to require only one or two data pulls of limited information (for instance, once at application and once before a mortgage closing), while a service that provides ongoing monitoring of account balances and transactional activity may require daily or even more frequent access to more information.

Sources: 81 Fed. Reg. at 83808-09; Treasury, Fintech Report at 22-23, 160-62; Sarah Kocianski, How Banks Are Driving the Evolution of Personal Financial Management, Forbes (Nov. 2, 2018); TradeIt Blog, Aggregation Wars, Part 1: Near History, blog.trade.it (Jan. 18, 2017); Mark Schwanhausser, Blog, Intuit Is Selling Quicken: Will Banks Seize the Moment?, javelinstrategy.com (Aug. 21, 2015); Konrad; Smith, How Data Aggregation Can Shake up Credit Decisioning; 12 C.F.R. § 1026.43(c)(3); Fannie Mae, Desktop Underwriter (DU) Validation Service: Leveraging the Power of DU to Provide You with Day 1 Certainty (2019); Fannie Mae, DU Validation Service Frequently Asked Questions (July 20, 2019); Jann Swanson, Freddie Mac Announces More "Big Data" Tools, Mortgage News Daily (Oct. 15, 2018).

key data sources to govern data transfers.[94] However, aggregators do not typically contract directly and separately with consumers or small businesses in their own right, and may or may not interact with applicants under their own branding. For example, aggregators' terms are often woven into those of the lender or other client rather than presented separately to consumers. Some stakeholders have also raised concerns that the interfaces that aggregators supply for applicants to identify the accounts from which data will be used and provide account credentials may not make clear that they are operated by a company that is distinct from both the lender and the bank.[95]

Thus, in some cases, the consumer or small business applicant may not be aware of the existence or identity of the aggregator. However, in other cases, some aggregators are creating mechanisms for direct engagement with consumers. For example, at least one aggregator has developed a branded consumer portal that permits individual applicants to review the data that will be shared prior to authorizing the transfer. At least one other aggregator has established mechanisms for

94 See Section 4.2. Particular data sources may also use the same data aggregators to facilitate transfers for which they are the end user; for example, banks are reportedly data aggregators' biggest clients. 81 Fed. Reg. at 83808; Section 4.2.3.

95 Treasury, Fintech Report at 23, 25, 32; Penny Crosman, Is a New Data War about to Erupt?, Am. Banker (Dec. 23, 2019); Mary Wisniewski, 80% of Financial App Users Admit Not Fully Realizing Their Banking Credentials Are Shared: Survey, bankrate.com (Nov. 19, 2019); Octavio Blanco, Consumers Get More Control Over the Banking Data Shared with Financial Apps, Consumer Reports (Nov. 10, 2019).

consumers to submit disputes and inquiries about cash-flow information, similar to what traditional consumer reporting agencies have established pursuant to the Fair Credit Reporting Act.[96] However, most aggregators argue that they should not be treated as consumer reporting agencies under FCRA, as discussed further in Section 6.1.1.2.

The precise nature of the services that data aggregators may provide to any one lender or other client, as well as the terms on which such services are delivered, may vary depending on the particular aggregator, the context in which the client acquires and uses data, and the business relationships between the two. In general terms, the services offered by individual aggregators can be placed on a spectrum that varies in the degree to which the aggregator acts to clean, contextualize, or analyze the data being transmitted:

- **Simple transmission**: The aggregator transmits or otherwise makes available customer information to data users with no meaningful intervention between the data source and the data user.
- **Data cleaning and structuring**: As part of facilitating data access, the aggregator also cleans and structures data pulled from one or more sources as part of transmitting data. For instance, the aggregator may screen the data for incomplete, incorrect, or irrelevant information and modify or delete such items. Structuring data involves converting it to a uniform format that may be set by the aggregator or customized for a particular end user. Relying on aggregators to act on the data in these ways can provide efficiencies for users, since it allows them to rely on aggregators' technological and analytical capabilities instead of developing and supporting such capacity in-house.
- **Data analytics and supplemental services:** The aggregator enriches the data by providing supplemental products and services, such as fraud screening or identification of patterns in recurring and irregular cash flow, that are derived from analytical tools built and maintained by the aggregator. These tools are developed using data that the aggregator has previously collected for other purposes and stored in anonymized form, or perhaps supplemented with purchased data. Thus, it can provide clients with a far richer baseline for analysis than they would easily be able to obtain on their own.

Aggregators may offer different levels of service to different clients or for different use cases. Our understanding is that it is quite rare for aggregators to provide only simple transmission services in practice, in part because of variations in how the underlying data is stored and collected from original sources as discussed in Section 4.2.2. There are some incentives for aggregators to move toward higher-margin, more complex services over time because those services will retain value in a world in which larger data users may develop the capability to acquire data without assistance from aggregators and smaller clients want to minimize expenditures on computer and regulatory compliance infrastructure.[97] Indeed, at least one aggregator has begun selling aggregated, anonymized data and related analytical services to third parties, although the practice has attracted

96 Finicity, Consumer Reporting Agency, finicity.com (visited Feb. 8, 2020) (describing procedures for filing questions or disputes via its consumer portal). Another aggregator states that it maintains a "Fair Credit Reporting Act (FCRA) compliance framework" to manage data in the same way as a traditional credit bureau but does not appear to provide a specific consumer-focused portal. Envestnet/Yodlee, Press Release, Envestnet/Yodlee Enapbles Comprehensive Financial Picture with Risk Insight Suite, yodlee.com (visited Feb. 22, 2020).

97 For a general discussion not specific to the financial services context see McKinsey Global Institute at 46-52 (concluding that data collectors and aggregators are losing value in markets where it has become easier for users to perform many aspects of that function for themselves, while data analytics is generally the most important and most valuable step in emerging information ecosystems).

criticism from some stakeholders and policymakers as discussed further below in Section 6.1.3.[98]

However, as discussed further below in Section 6.1.1.2, the roles that aggregators take on also have potential implications for their compliance obligations. In particular, providing more complex services in the context of credit underwriting may make it more likely that an aggregator would be considered to be a "consumer reporting agency" for purposes of the Fair Credit Reporting Act, but may not have the same implications when supporting personal financial management or payments activities.

4.2.2 Technological processes and their competitive implications

Movement of deposit and prepaid account data for real-time use is a technology-intensive process. These technologies are evolving, with a particular emphasis on improving the overall security and accuracy of the processes used to access, collect, and transfer the data. In the United States, newer methods currently depend on the formation of bilateral contracts between transfer system participants because there currently are no broadly accepted industry standards or generally applicable terms established in regulation. As discussed in this section and in 5.2 below, the technologies used to transfer the data have important competitive implications for the system as a whole.

Screen scraping was aggregators' initial method of data acquisition and remains by far the dominant method of collection today. The process generally involves using proprietary software to copy information displayed on the data source's customer-facing webpages. Where such information is password-protected, as in the financial services context, aggregators have historically accessed it by asking applicants to provide their login usernames and passwords. Those credentials mean that the aggregator interfaces with the website or app as if it were the individual accountholder, such that the company has the technological ability to access any data that can be seen by the accountholder and to conduct transactions in the account.[99]

Screen scraping can facilitate competitive balance between different sizes and types of firms because it allows data sharing to occur without a contractual agreement or other facilitation by the source and can be used to transfer data from computer systems that may otherwise be expensive and time consuming to connect.[100] However, particularly to the extent that it is effectuated through credential sharing, screen scraping raises substantial concerns with regard to data privacy and customer protection.[101] It also can raise security and burden concerns for data sources, particularly now that more than half of the traffic on some banks' online platforms is coming from aggregators. Finally, screen scraping can also be subject to relatively frequent disruptions and potential accuracy

98 Envestnet/Yodlee, Analytics for Credit Risk Modelling: Making Better Lending Decisions, yodlee.com (visited Feb. 8, 2020); Ryan Tracy, Lawmakers Call for Investigation of Fintech Firm Yodlee's Data Selling, Wall St. J. (Jan. 17, 2020); Penny Crosman, JPMorgan Chase Signs Data Sharing Agreement with Envestnet Yodlee, Am. Banker (Dec. 5, 2019); Nathaniel Popper, Banks and Tech Firms Battle Over Something Akin to Gold: Your Data, N.Y. Times (Mar. 23, 2017); Bradley Hope, Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors, Wall St. J. (Aug. 6, 2015).

99 81 Fed. Reg. at 83808-09; Treasury Fintech Report at 25-28, 34-35; Penny Crosman, Why a Clear Answer to the Data-Sharing Debate Remains Elusive, Am. Banker (Feb. 23, 2017); Financial Data Exchange, The ABC's of APIs 4 (2019); Plaid, Financial Data Access Methods: Creating a Balanced Approach 6-7 (2016).

100 Notably, open banking initiatives in other nations, such as the European Union's Revised Payment Service Directive (PSD2), prohibit the conditioning of API access on the creation of a contractual relationship. Directive (EU) 2015/2366 of the European Parliament and of the Council (Nov. 25, 2015). For overviews of international open banking initiatives, see Box 5.2.21.1; Basel Committee on Bank Supervision, Report on Open Banking and Application Programming Interfaces, Bank for International Settlements (2019); Institute of International Finance, Liability and Consumer Protection in Open Banking (2018); Diana Milanesi, A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States, Stanford-Vienna Transatlantic Technology Law Forum Working Paper No. 29 (2017).

101 *See generally* U.S. Government Accountability Office, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight 21-22, 54-57 (2018) (hereinafter GAO, Fintech Report); Treasury, Fintech Report at 25-26, 35-36; Crosman, Clear Answer; Sections 4.2.3, 5.2.

BOX 4.2.2.1 CONCERNS ABOUT CREDENTIAL SHARING AND SCREEN SCRAPING

Credential sharing and screen scraping present a number of disadvantages both for consumer and small business accountholders and data sources. For example:

Risk of unauthorized activity: Reliance on credential sharing potentially makes accountholders more vulnerable to fraudulent account transactions either by employees of the company to which they provide the credentials, hackers, or phishers. As discussed in Box 5.2.2.2.2, the fact that consumers have voluntarily shared the credentials has created some debate about responsibility for unauthorized activity under existing law, and at least one large bank has made public statements that it might not reimburse losses from consumer accounts in situations involving credential sharing.

Scope of data sharing: In addition, once credentials have been shared, consumers generally have little ability to directly monitor the nature, depth, or duration of access to and use of their financial data. As a practical matter, a party that has the applicant's credentials can view any information that is provided on banks' customer platforms. Moreover, simply deleting a particular financial application from an accountholder's phone or computer does not automatically turn off data access. Only changing passwords or execution of an order to delete credentials (for instance through an aggregator's dashboard) will cut off electronic access. Some stakeholders emphasize that aggregators' data collection and storage activities are limited by contract and the adoption of general business practices to minimize data handling, but others assert that some firms collect far more data than is needed to provide a particular product or service.

Bank systems and security risks: For firms that provide transaction accounts, screen scraping can also create unpredictable systems demands and security concerns, given that maintaining the security of an accountholder's specific credentials is critical to efforts to protect sensitive customer data and the integrity of their systems. Some stakeholders have reported that screen scraping activity at times can appear similar to a "denial of service" attack by malicious actors. The volume of screen scraping may also make it more difficult to monitor for unauthorized uses.

Disruption and accuracy concerns: Screen scraping is also subject to relatively frequent disruptions and potential accuracy concerns. For example, accuracy and linkage problems often increase after a bank or other data source redesigns its web pages or changes security protocols.

Sources: GAO, Fintech Report at 21-22, 54-57; Treasury, Fintech Report at 25-26, 35-36; Crosman, Clear Answer; FDX, The ABCs of APIs at 4; Surane, Big Banks' Clampdown.

issues when banks change their systems. Some system participants have questioned whether service disruptions have been deliberate, which banks have denied.[102]

Over time, some data sources and aggregators have evolved their practices to reduce certain frictions. For example, some data sources have programmed their systems to recognize aggregators' internet protocol addresses or created dedicated "direct feeds" that permit expedited website logins and data retrieval for aggregators in order to reduce burdens on both parties. Aggregators have also moved to "screenless data collection," which queries raw text but not images, advertisements, and other forms of data that may also be presented on bank websites. However, while such improvements have helped to reduce systems loads and some other concerns, they still generally depend on the use of login credentials.[103]

102 Jennifer Surane, Big Banks' Clampdown on Data Puts Silicon Valley Apps on Alert, Bloomberg (Mar. 26, 2019); Nathan DiCamillo, In Data Dispute with Capital One, Plaid Stands Alone, Am. Banker (July 17, 2018); Jennifer Surane, Capital One Restricts Third-Party Data Access, Upsets Customers, Bloomberg (June 27, 2018); Amanda Dixon, Fintech Roadblocks: Why Banks Block Budgeting Apps, bankrate.com (Dec. 5, 2017); Popper; Penny Crosman, The Truth Behind the Hubbub Over Screen Scraping, Am. Banker (Nov. 12, 2015); Daniel Huang & Peter Rudegeair, Bank of America Cut Off Finance Sites from Its Data, Wall St. J. (Nov. 9, 2015); Robin Sidel, Big Banks Lock Horns with Personal-Finance Web Portals, Wall St. J. (Nov. 4, 2015). Fintechs and aggregators have sometimes encouraged and facilitated consumer complaints in response to outages. *See, e.g.,* Yuka Hayashi, Venmo Glitch Opens Window on War Between Banks, Fintech Firms, Wall St. J. (Dec. 14, 2019); Payments Source, Capital One Restricts Third-Party Data Access, Upsets Customers, paymentssource.com (June 27, 2018); Crosman, The Truth Behind the Hubbub.

103 81 Fed. Reg. at 83808; Plaid at 6-7. Although some banks are offering multi-factor authentication systems that rely not just on passwords but on codes sent by text or app, they do not always require recognized aggregators to supply the second factor to view limited account information. Where consumers are using weak or recycled passwords, this has led to concerns that hackers may be able to access the limited data to determine which consumers are worth targeting for further attacks. Brian Krebs, The Risk of Weak Online Banking Passwords, krebsonsecurity.com (Aug. 5, 2019).

In the last few years, a number of larger banks have begun pushing to transition to systems that rely on systems that replace credential sharing with specially generated tokens for data access and screen scraping with transmissions via "application programming interfaces" (APIs).[104] Tokenization involves replacing a sensitive data element with a unique, randomly generated set of values that have no other meaning or value; the token can then be used by one or more parties to take action (e.g., access data or route a payments transaction), without ever obtaining the underlying element.[105] Depending on how systems are constructed, data access tokens can be used to provide read-only access to banks' web portals so that aggregators could obtain data but not conduct account transactions. Or they can be used to access data via APIs that are structured to permit access only to certain data fields. Tokens can also be structured to expire after specified periods of time and/or to be used only by specific parties with authentication, both of which make them difficult to use by bad actors in the event of a breach. However, current models generally require a pre-existing relationship between the companies involved in the data transfer to generate a token at the accountholder's request, and there has been some disagreement about which tokenization systems to adopt for data access purposes.[106]

APIs are software intermediaries that allow two websites or applications to exchange information using a common format. Compared to screen scraping, they can be built to provide greater security, accuracy, precision as to the scope of data sharing, and predictability with regard to costs. APIs are often already used by aggregators themselves in transmitting information to downstream users, and in a wide variety of other financial services contexts. In recent years, a number of individual banks have proceeded with building their own APIs for customer-permissioned data sharing. But where some countries mandate open API access for any companies meeting certain regulatory requirements, U.S. banks are generally providing access to such channels only for aggregators or other companies that sign confidential contracts governing the terms of data transfer.[107] As noted above, they are combining the development of APIs with tokenization initiatives, and in some cases both banks and aggregators are creating dashboards that allow customers to monitor and restrict sharing of their data downstream.[108]

These tokenization and API initiatives address many of the disadvantages of screen scraping but have technological, resource, and competitive implications for the broader market. For example, building APIs requires substantial resources, and negotiating the underlying contracts can also

104 *See generally* 81 Fed. Reg. at 83808-09; Treasury, Fintech Report at 26-28; Crosman, Clear Answer; FDX, The ABCs of APIs at 6-12; Plaid at 4-6.

105 Tokenization is similar to encryption except that it does not involve a key that consistently translates a particular piece of information the same way each time that it is applied; because encryption merely disguises rather than replaces the underlying data, it is somewhat more subject to reversal. In addition to generating tokens to permit access for data sharing purposes, tokens are being used in financial services contexts today to protect credit card and debit card numbers and in some cases to protect routing and account numbers that are used for direct deposit and other automated clearinghouse transactions. *See, e.g.,* Clearent, Tokenization vs. Encryption, clearent.com (visited Feb. 11, 2020); Square, Payment Tokenization Explained, square.com (visited Feb. 11, 2020).

106 FDX, The ABCs of APIs at 11-12; Plaid at 4-6. OAuth is a tokenization standard that has been widely adopted by technology companies such as Twitter, Facebook, and Google, but has not been as popular among traditional financial institutions, data aggregators, and fintechs. It facilitates authentication without having to share credentials with intermediaries or apps, but it requires some resource investment and is operationally complex in part because it requires redirecting consumers from a third-party app's website to the financial institution and back again. After initial resistance, adoption now appears to be spreading at least among large financial institutions in connection with data sharing agreements and API implementation initiatives, though OAuth adoption is possible to implement without construction of APIs. Crosman, Clear Answer; Finicity, OAuth Connections Guide (Oct. 16, 2019) (reporting connections involving OAuth with more than 40 percent of the deposit and investment market); Plaid at 4-6.

107 Treasury, Fintech Report at 26-28, 34-35; 81 Fed. Reg. at 83808-09; Penny Crosman, How APIs Are Being Used at Citi, BBVA and Other Leading Banks, Am. Banker (May 26, 2019); Crosman, Clear Answer; Yurcan.

108 Blanco; Suman Bhattacharya, With Plaid, Wells Fargo Gives Customers a New Lever to Control Their Data, bankinnnovation.net (Sept. 23, 2019); Justin Baer, Fidelity Parent Launching New Online Data-Protection Business, Wall St. J. (Apr. 30, 2019); Nathan DiCamillo, Capital One Mends Fences with One Aggregator, Deepens Relationship with Another, Am. Banker (Aug. 10, 2018); Joseph Lorenzo Hall, Blog, The Beginning of the End for Sharing Bank Credentials, Center for Data & Technology (Jan. 25, 2017). For a discussion of the proliferation of data management dashboards more generally, see Joseph Jerome, Financial Dashboards: Enhancing User Control Outside a Traditional 'Privacy Dashboard,' Center for Data & Technology (Sept. 27, 2017).

be resource-intensive.[109] Although tokenizing data access could be pursued separately from API-building, banks are combining the two initiatives to provide more granular control over what data is being shared. As discussed further below, banks that are developing such channels are also frequently requiring aggregators to comply with and to require their clients to comply with various technology, monitoring, compliance, and liability requirements. As a result, there are serious questions about the scalability of the current system of bilateral contracts and custom-built APIs, particularly absent common industry and/or regulatory standards.[110] Smaller banks, which rely heavily on certain vendors to operate their core deposit platforms, face particular challenges in negotiating data sharing agreements and implementing new transfer technologies.

Moreover, even where APIs have been established, technological limitations and other factors can slow full adoption of this transmission method and affect which types of data are prioritized for API transmission. For instance, we understand that relatively modest amounts of data are flowing through APIs currently and that banks are tending to prioritize other use cases than credit underwriting.

And most significantly, the shift toward API-driven data transfers affects which party determines the data fields that will be shared pursuant to the customer's authorization. Whereas screen scraping permits aggregators to acquire any information that is available to accountholders via the banks' web-based platforms, banks and other account providers are defining the scope of data access via the data sharing contracts and APIs. Banks are generally building the APIs to support narrower flows based on particular use cases and other factors. As discussed further below, the APIs and related data sharing agreements have become a major flashpoint in the market, with aggregators and end users asserting that banks are using them to protect their competitive interests in a way that is inconsistent with consumers' data rights under § 1033 of the Dodd-Frank Act, and banks arguing that they are protecting customers' security and privacy and imposing some discipline on the broader data transfer system in the absence of greater regulatory clarity and consistency.[111]

4.2.3 Bank activity within the data transfer system

Banks have become the biggest consumers of aggregated data as the new system has emerged,[112] yet in their capacity as data sources they are also acting as a substantial brake on that system both through their reaction to screen scraping activities and through the contracts that are governing the deployment of API transmissions. While these contracts have been designated as confidential by the parties, they reportedly impose limitations on the scope of data transmissions and usage, obligations on aggregators with regard to data security and policing their downstream clients, and various

109 Some sources have reported costs as high as $500,000 per API. Penny Crosman, JPMorgan Chase Moves to Block Fintechs from Screen Scraping, Am. Banker (Jan. 2, 2020).

110 Treasury, Fintech Report at 27-28. Smaller banks and credit unions tend to use core processors or other platforms to support their transaction account programs. Although these companies could potentially facilitate scalable solutions, community banks have recently expressed substantial frustration with core processors' policies and services. See Section 4.1.2.

111 For example, stakeholders have complained about some banks withholding customer identification information and routing/account numbers, which complicates authentication, fraud detection, and routing of funds for a broad range of use cases including credit. They also report some cases of banks withholding information for certain use cases that may compete with bank products and with regard to pricing and fees that make it easier for other financial services providers to provide alternative products and services to customers. Banks have defended requiring additional safeguards and/or restricting identification information and routing/accounting numbers because of fraud risk and say they should not be required to provide access to proprietary information. Some argue that pricing information if revealed for a large number of customers could reveal proprietary model information in some circumstances. Consumer Financial Protection Bureau, Symposium on Consumer Access to Financial Records (Feb. 26, 2020), available at https://www.consumerfinance.gov/about-us/events/cfpb-symposium-consumer-access-financial-records/; Surane, Big Banks' Clampdown; Penny Crosman, Fidelity Data-Sharing Hub Aims to End Screen Scraping, Am. Banker (June 11, 2019); Mary Wisniewski, Fintechs' Vulnerability Apparent in Capital One Data-Access Flap, Am. Banker (June 29, 2018); Penny Crosman, Banks Aren't Following CFPB Data-Sharing Guidance, Fintechs Say, Am. Banker (Nov. 20, 2017); Penny Crosman, The Battle Over Bank Customer Data May Finally Be Over, Am. Banker (Nov. 6, 2017).

112 81 Fed. Reg. at 83808.

BOX 4.2.3.1 BANK COMPLIANCE AND LIABILITY QUESTIONS

Banks have focused primarily on three compliance issues in connection with data aggregators' collection of customer information on behalf of fintechs:

Information security requirements: The Gramm-Leach-Bliley Act requires all financial institutions to safeguard consumer information. However, as discussed further in Sections 5.2.2 and 6.1.1, non-banks are subject to less specific standards and are not generally examined for compliance with these requirements. Accordingly, banks have expressed concern that not all aggregators and fintechs comply with the same practices that banks have adopted. The FTC proposed amendments in 2019 that would narrow many but not all of these differences.

Electronic Fund Transfer Act liability: EFTA generally limits the extent to which consumers can be held liable for unauthorized electronic fund transfers from their accounts, leaving banks and prepaid issuers to absorb any additional losses and seek recompense from other parties as best they can pursuant to automated clearinghouse or card network rules. In the data aggregation context, however, stakeholders dispute whether and how the liability limitations apply if an unauthorized transaction occurs as a result of a consumer giving login credentials to an aggregator to pull cash-flow data for delivery to a lender or other end user.

Implementing rules generally define unauthorized transfers to be ones that are "initiated by a person other than the consumer without actual authority to initiate the transfer," but they exclude situations where consumers furnish debit cards or other "access devices" to another party. In those cases, banks can treat transactions as authorized until such time as the consumer tells them otherwise. Some banks have argued that they should not have to absorb losses if the consumer's credentials are subject to a data breach at the aggregator or other misuse by the aggregator or its employees. There are also disputes over when and whether aggregators could be liable to consumers as electronic fund transfer service providers.

Third-party servicer obligations: As discussed in Section 4.1.2, federal banking regulators and the CFPB expect supervised firms to monitor their third-party service providers for compliance purposes. Each agency has described the qualifying relationships in slightly different terms:

- Office of the Comptroller of the Currency: "A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise," including "business arrangements in which a bank … may have responsibility for the associated records."
- Federal Reserve Board: "'[S]ervice providers' is broadly defined to include all entities that have entered into a contractual relationship with a financial institution to provide business functions or activities."
- Federal Deposit Insurance Corporation: Service providers "include all entities that have entered into a business relationship with the financial institution."
- Consumer Financial Protection Bureau: A service provider is "any person that provides a material service to a covered person in connection with the offering or provision of a consumer financial product or service."

There is no dispute that aggregators that provide data to banks are acting as their third-party service providers, but aggregators' status is less clear where they are collecting data *from* banks via screen scraping or APIs that are subject to data sharing agreements because the banks are not typically thought of as receiving services from the aggregators in such situations. A 2018 Treasury Department report suggests that this ambiguity may be discouraging aggregators and banks from signing data sharing agreements to move to APIs and other more secure data transmission practices.

Fair Credit Reporting Act: In the context of transfers for credit-related purposes specifically, there are general questions about whether FCRA applies. However, as discussed in Section 6.1.1.2, we are unaware of any stakeholders who are actively advocating that banks be subject to requirements as "furnishers," although there is a fierce dispute over whether aggregators are "consumer reporting agencies."

Sources: 12 U.S.C. §§ 6801, 6809(3), (4); 84 Fed. Reg. 13158 (Apr. 4, 2019); 15 U.S.C. § 1693g; 12 C.F.R. §§ 1005.2(a)(1), (m), 1005.6(b); *id.* Supp. I, cmt. 2(m)-2, 6(b)(3)-2; Office of the Comptroller of the Currency, Bulletin 2001-12 (Feb. 28, 2001); FRB, Supervisory & Regulation Letter 13-19; FDIC, Financial Institution Letter 44-2008; OCC, Bulletin 2017-21; OCC, Bulletin 2013-29; CFPB, Compliance Bulletin and Policy Guidance 2016-02; Treasury, Fintech Report at 35-36.

requirements concerning insurance, indemnification, and consumer disclosures. A recent template contract based on examples of existing agreements that was released in 2019 by The Clearing House, which represents two dozen of the nation's largest banks, reflects all of these items.[113]

Much as with regard to banks' posture as lenders as discussed in Section 4.1.2 above, their actions as data sources appears to be shaped by a number of competitive and regulatory considerations:

Market positioning: Banks are in an unusual position in that they hold more transaction account data than other types of financial services providers. As different use cases have developed, they have been placed in the awkward position of providing one of their critical assets—details of their customers' transaction records—to firms that are providing financial services that frequently overlap with the banks' own offerings to the banks' existing customers. For example, though banks may not be concentrating on non-prime markets for the reasons discussed in Sections 4.1.2 and 5.2, they may be reluctant to risk losing financial advisory or payments business from wealthier customers. At the same time, given their own growing reliance on data aggregators, it is not in banks' interests to shut down the system.

Monitoring obligations: As discussed in Section 4.1.2, banks face much stronger expectations with regard to management of commercial relationships with other companies than do aggregators and fintech lenders that are not subject to CFPB supervision. In particular, some of the prudential agencies' guidance with regard to third-party service providers suggests that even relatively modest contractual or other ongoing relationships may trigger compliance monitoring obligations by banks. For example, some sources have suggested that a data sharing agreement in the context of an API would be sufficient to render data aggregators third party service providers to banks under existing prudential guidance, even if the aggregator is solely acting to collect data for transmission to non-bank end users that are competing with the bank.[114]

Similarly, bank regulators have directed depositories under the Gramm-Leach-Bliley Act to monitor the information security practices of their service providers, while the GLBA regulations that apply to most non-bank companies are much less clear with regard to vendor monitoring obligations.[115] Even absent a formal obligation to treat data aggregators as third-party service providers, banks may be applying these extant processes and procedures to screen potential companies for API access because they are familiar and established tools for assessing outside companies' ability to manage information security and related risks.

Liability risk and customer expectations: More generally, banks have expressed broader concerns that in the event of a breach or misuse of information, regulators or consumers will expect the depository institution that provided the data to remediate affected customers, even in situations in which the problem occurred downstream due to the conduct of another party. These concerns are based in part on the Electronic Fund Transfer Act's provisions that generally require

113 The Clearing House, Template for U.S. Accounts Data Sharing Agreement articles 4, 5, 8, 13, 14, 15 (Nov. 12, 2019); Jennifer Surane, Big Banks Want to Make It Easier to Share Consumer Data with Startups, Bloomberg (Nov. 12, 2019).

114 Treasury, Fintech Report at 36-37, 73-77 (describing debates over the issue and suggesting that it may be inadvertently discouraging the signing of data sharing agreements); *see also* OCC, Bulletin 2017-21 (stating that a third-party relationship includes "any business arrangement between the bank and another entity, by contract or otherwise," including situations in which 'a bank has an ongoing third-party relationship or may have responsibility for the associated records"). Although the federal banking agencies have also issued guidance under GLBA safeguards requirements that banks should engage in monitoring of third-party service providers, they expressly stated during the initial issuance of that guidance that it did not require banks to prevent such access or monitor the use or redisclosure of the customer's information by a third party that was accessing customer data with the consumer's consent, including by provision of the consumer's password. 66 Fed. Reg. 8616, 8620 (Feb. 1, 2001).

115 *See, e.g.,* 12 C.F.R. Pt. 30, app. B.III.D; 16 C.F.R. § 314.4(d); Federal Financial Institutions Examination Council Information Technology Examination Handbook II.C.20 (2016); Federal Financial Institutions Examination Council Outsourcing Technology Services Booklet (2004). The Federal Trade Commission recently proposed language that would more clearly specify ongoing monitoring responsibilities for non-bank financial institutions. See Section 5.2.2.2.

financial institutions that provide consumer accounts to absorb losses for unauthorized electronic transfers beyond certain liability limits, in part on prudential regulators' guidance that banks are accountable for the compliance activities of their third-party service providers, and in part on more generalized fears that regulators or consumers will expect banks to make consumers whole before the commercial parties determine liability among themselves.[116]

Bank concerns are further exacerbated by the fact that aggregators and fintech end users are not generally required to hold capital from which they could compensate customers in the event of loss, are subject to less detailed information security requirements under the Gramm-Leach-Bliley Act, and are not generally monitored for GLBA compliance by federal regulators.[117] Although the risk that hackers would obtain consumers' login credentials is the biggest concern, banks have also focused on the risk that account and routing number data could be used to conduct unauthorized "pull" transactions on consumers' accounts via the automated clearinghouse system. Such information is not critical for underwriting based on cash-flow information, but lenders may use it to direct deposit funds in customers' accounts and in some cases for repayment arrangements.[118]

Although some banks have argued that they are not liable to their customers under EFTA for any unauthorized activity that occurs as the result of sharing account credentials,[119] they are also investing substantial energy into using the data sharing agreements to require aggregators to implement information safeguards, assume liability for breaches and misuse that occurs after data is transferred away from the bank, and impose various downstream requirements on end users. Firms are beginning to negotiate contractual indemnification clauses to address such situations, so that liability can be decided through negotiated settlement, arbitration, or litigation, depending on the individual contracts at issue.[120] But such processes can be cumbersome, and stakeholders from across the spectrum agree that insurance availability is a substantial constraint. Accordingly, some banks are also arguing that it is appropriate for them to withhold data such as account and routing information that could be used to conduct unauthorized transactions, at least until such time as a tokenization system is implemented to protect that information from misuse.[121]

116 15 U.S.C. § 1693g; *see also* box 4.1.2.2. In one survey conducted by a trade association for large banks, when consumers were asked which parties they would hold accountable for the security of their data, 56 percent of customers of fintech firms said that they would hold banks that they directed to share their data accountable, compared with only 48 percent who stated that they would hold the fintechs to which they granted access accountable. The Clearing House, Fintech Apps and Data Privacy: New Insights from Consumer Research (2018) (survey of nationally representative sample of more than 2000 US banking consumers conducted in January 2018). Banks' primary source of concern is the risk that account credentials or routing and account numbers would be used to conduct transactions on consumers' accounts that they did not authorize. However, there are also concerns about other types of expenses in the event of a data breach, such as customer notifications and provision of identity theft monitoring services.

117 12 U.S.C. §§ 6801(b), 6805(b); 12 C.F.R. Pt. 30, app. B.III.D; 16 C.F.R. Pt. 314; 66 Fed. Reg. 8616 (Feb. 1, 2001); FFIEC, Information Technology Examination Handbook II.C.20; FFIEC, Outsourcing Technology Services Booklet; *see also* The Clearing House, Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers (2015) (contrasting security requirements).

118 Such information is also potentially critical for certain payments-related use cases.

119 *See, e.g.*, Liz Weston, Why Banks Want You to Drop Mint, Other 'Aggregators,' Reuters (Nov. 9, 2015) (reporting statements by JPMorgan Chase and Capital One). See Box 4.2.3.1 for more discussion.

120 For example, see TCH, Data Sharing Agreement articles 4.2(b), 14.

121 This position is controversial because account and routing information sufficient to conduct unauthorized transactions is also available on paper checks, and critics argue that it is anti-competitive and inconsistent with § 1033 of the Dodd-Frank Act to condition sharing on implementation of tokenization systems. Tokenization would reduce fraud risks for automated clearinghouse transactions, not just in connection with customer-permissioned data transfers but more generally, but the market has not yet converged on a standardized system. Individual companies may be reluctant to invest heavily in tokenization initiatives while they are waiting for the outcome of a Federal Reserve Board initiative to provide real-time settlement services by 2023, and to date regulatory agencies have not launched broader initiatives focusing specifically on this topic. Although tokenization is increasingly being used in the card network system, some stakeholders are concerned that it could be implemented for ACH transactions in a way that substantially constrains payments innovations. *See generally* Board of Governors of the Federal Reserve System, Press Release, Federal Reserve Announces Plan to Develop a New Round-the-Clock Real-Time Payment and Settlement Service to Support Faster Payments (Aug. 5, 2019).

In the last few years, large banks' public statements in connection with bilateral sharing agreements have shifted from emphasizing the dangers of the data sharing ecosystem to emphasizing opportunities to empower their customers to use financial apps and control their data.[122] But in other contexts they continue to emphasize fraud and security risks, and aggregators and fintechs have reacted with substantial skepticism to suggestions that banks have come to see the new data sharing system in a more positive light. In late 2019, tensions further increased in response to a series of news stories stating that large banks were planning to begin blacklisting high-volume traffic that is not routed through APIs[123] and a dispute between PNC Bank, Plaid, and Venmo that led to an extended disruption of service.[124] The fact that The Clearing House template provided for the possibility of banks charging for data access and withholding data in certain circumstances has also raised concerns among aggregators and fintechs.[125]

4.2.4 Standardization initiatives, acquisitions, and other market developments

Overall, the system for customer-permissioned data transfers has demonstrated both substantial dynamism and substantial uncertainty over the last several years. As competitive tensions have ebbed and flowed, market actors have made periodic attempts to explore opportunities for greater cross-industry cooperation and standardization. While both the bilateral contracting efforts and these broader cross-industry initiatives are attempting to address certain risks and inefficiencies in the current market, it remains to be seen both how effective they will be and what scope of issues they will take on in light of competitive dynamics and other considerations. High-profile acquisitions and other market developments in early 2020 have injected additional uncertainty into the market.

Standardization efforts relating to financial data date back at least to the 1990s. In 2015, two different groups of industry players launched renewed efforts to encourage adoption of a common API

122 *See, e.g.*, Bhattacharya, New Lever; Crosman, JPMorgan Chase Signs Agreement; Penny Crosman, U.S. Bank Embraces Open Banking with Data Sharing Agreements, Am. Banker (Sept. 24, 2019); Penny Crosman, Wells Fargo Strikes Data-Sharing Agreement with Plaid, Am. Banker (Sept. 19, 2019); JPMorgan Chase, Press Release, Plaid Signs Data Agreement with JPMorgan Chase, media.chase.com (Oct. 22, 2018); Nathan DiCamillo, JPMorgan Chase Inks Fourth Data Aggregator Deal, Am. Banker (Oct. 22, 2018); Nathan DiCamillo, Capital One Mends Fences; Penny Crosman, Wells-Finicity Deal Furthers Data Détente, Am. Banker (Apr. 4, 2017).

123 Some large banks have made sporadic statements about the potential to block screen-scraping for more than a year, but several additional news reports in late 2019 and early 2020 attracted additional attention. In February 2020, sources reported that JPMorgan Chase told fintech companies that they will be barred from data access unless they sign data sharing agreements and transition away from screen scraping. The company reportedly already has data sharing agreements covering 95 percent of requests. *See, e.g.*, Pete Schroeder & Anna Irrera, JPMorgan Sets July Deadline for Fintechs to Sign New Data Access Deals: Sources, Reuters (Feb. 13, 2020); Emma Olson, JPMorgan: US Banks to Adopt Standard API, PaymentEye (Jan. 16, 2020); Anna Hrushka, Banks to Tighten Third-Party Data Access in 2020, Experts Say, BankingDive (Jan. 7, 2020); Crosman, JPMorgan Chase Moves to Block; Laura Noonan, JPMorgan to Ban Fintech Apps from Using Customer Passwords, Fin. Times (Jan. 1, 2020); Surane, Big Banks' Clampdown; Nizan Geslevich Packin, Big Banks vs. Silicon Valley Startups: Whose Customer Financial Data Is It Anyway?, Forbes (Apr. 19, 2019); JPMorgan Chase, Plaid Signs Data Agreement.

124 The Venmo-Plaid-PNC clash escalated substantially because PNC not only shut off access to Venmo after a security upgrade, but tweeted to its customers promoting a bank-offered product called Zelle as an alternative option. PNC denies the allegation that the incident is an attempt to promote Zelle, describing the tweet as an off-hand reference by an individual customer service representative at the end of a long troubleshooting exchange with a single customer. Crosman, Data War?; Ron Shevlin, The Real Story Behind The PNC-Venmo Clash, Forbes (Dec. 18, 2019); Hayashi.

125 TCH, Data Sharing Agreement, articles 4.2 (authorizing the withholding of data in various circumstances, including where provision "could cause harm to [a data source's] reputation or contradicts [its] business guidelines"), 10 (providing alternatives where fees will or will not be charged on an ongoing basis, and providing as a standard term that the parties will bear their own expenses unless otherwise agreed to). To the extent that banks are currently seeking to impose charges in connection with data sharing to date, our understanding is that it may be in connection with one-time expenses for API construction rather than ongoing access. As discussed further in Section 5.2.2.1, charges could raise a number of policy questions with regard to competitive effects and consumers' rights to access data under § 1033 of the Dodd-Frank Act. The template has met with mixed reviews from aggregators and fintechs, with praise for provisions curtailing credential sharing and prohibiting the downstream sale of data without customer consent, but some negative reactions to its provisions regarding charges for data access, liability, and data usage restrictions. John Pitts & Sam Taussig, Plaid, Kabbage: Clearing House Model Agreement Creates "Uneven Playing Field," bankinnovation.net (Dec. 6, 2019); Rick Morgan, Clearing House Sets Data-Sharing Framework, But the Devil Is in the Detail, bankinnovation.net (Nov. 25, 2019); Surane, Big Banks Want to Make It Easier.

and common specifications for what data should be transmitted for particular use cases.[126] But while those efforts may have created some movement toward more standardized data specifications, they did not become universal. After large banks' push toward customized bilateral agreements in 2017 provoked an initial wave of backlash,[127] a further cooperative initiative called the Financial Data Exchange (FDX) was announced in late 2018.[128] The group, which consisted at its start mostly of large banks, large investment services providers, and large aggregators, broadened its membership to include a small bank trade association and the largest of the core processors that provide deposit account platforms for small banks. It has also added consumer advocate organizations, which participate in working groups but do not have voting power at the board level.[129]

FDX analogizes its role to the adoption of Bluetooth specifications in wireless technology. To date its primary focus has been the adoption of a standardized API and related data specifications for particular use cases. The organization estimates that approximately 8 million consumers were being served via the FDX API as of early 2020, although members' announcements about data sharing agreements are sometimes unclear as to whether they have moved to full adoption.[130] The group has also begun working with members to convene consumer focus groups to improve consent protocols, compile considerations with regard to customer authentication, and to prepare for a implementation of a certification program that will facilitate greater standardization among members.

However, efforts to define the minimum data elements to be provided for particular use cases are still under discussion, and the organization is still evolving in its approach to policy issues that extend beyond core technology questions. For instance, while it has endorsed data sharing principles

126 In the 1990s, two data specifications called the Open Financial Exchange (OFX, supported by Intuit, Microsoft, and Checkfree) and Interactive Financial Exchange (IFX, created by IBM) competed with each other. OFX appears to have become more dominant over time, but the consortium that had launched it was largely inactive between 2006 and 2015. That year, two new efforts launched. One group led primarily by financial institutions under the auspices of the Financial Services Information Sharing and Analysis Center (FS-ISAC) released a "durable data API" and specification in May 2015 that focused primarily on facilitating personal financial management applications. That same year, the OFX Consortium was re-launched by Intuit, Xero, Enterprise Engineering, Finicity, and Silicon Valley Bank and later grew to include several other large aggregators. It released OFX 2.2 in 2016 to add data fields and introduce the concept of OAuth tokenization. OFX website materials indicate that 7000 financial institutions currently deploy its open standard. Treasury, Fintech Report at 28 n.50; Plaid at 8-9; Open Financial Exchange, About OFX (visited Feb. 8, 2020).

127 *See, e.g.,* Penny Crosman, Data-Sharing Debate Grows Contentious as Fintechs Vent Grievances, Am. Banker (Aug. 15, 2017). By 2017, a group of what would become more than 50 fintech end-user companies and data aggregators called the Consumer Financial Data Rights Group launched a public campaign to push back on some of the bank contracting efforts, arguing that the institutions were unduly restricting the scope of data flows and permissible use cases. In addition to launching a public tweet campaign aimed at consumers, the group met directly with regulators and testified before Congress to urge greater data accessibility. *Id.*; Dixon.

128 Penny Crosman, Big Banks, Aggregators Launch Group to Hash Out Data Sharing Issues, Am. Banker (Oct. 18, 2018). FDX materials state that it began in 2017 as a grassroot effort. Financial Data Exchange, The Global Industry Standard for Consumer Access to Financial Data: Organization Overview 1 (2019). The initiative incorporates industry actors who were involved in both of the 2015 efforts, and as of July 2019 has formal ties to both of the organizations that facilitated the earlier initiatives. Specifically, FS-ISAC assigned its "durable data application" API standard to FDX, which became a wholly owned, independent subsidiary of FS-ISAC in 2018. In July 2019, the OFX consortium joined FDX as an "independent working group" tasked with maintaining and evolving the OFX standard as necessary to support existing implementations and provide a migration path to FDX for OFX users. FDX, Organization Overview at 1, 7.

129 Blanco (reporting that Consumer Reports has joined FDX); Financial Data Exchange, Press Release, Financial Data Exchange Adds 16 Members (Feb. 25, 2019); FDX, Organization Overview at 2, 7-8. The organization does not appear to include the three largest prepaid account issuers, though it does include some institutions with smaller portfolios. Financial Data Exchange, Members, fdx.com (visited Feb. 8, 2020); The Nilson Report, Blog, 50 Largest U.S. Prepaid Card Issuers (July 31, 2019) (listing MetaBank, The Bancorp Bank, Green Dot Bank, Comerica Bank, and JPMorgan Chase as largest based on number of purchase transactions and The Bancorp Bank, MetaBank, Sunrise Banks, U.S. Bank, and Bank of America as largest based on the number of cards issued); FDX, Members.

130 Financial Data Exchange, Press Release, The Financial Data Exchange Reports Strong First-Year Growth; Now Protecting Online Financial Data for Five Million Consumers, including Business Customers, Through 72-Member Network (Nov. 6, 2019). The group released its API specifications to the public in May 2019. Membership in the organization increased from 21 companies to 82 in its first 15 months of operation, but members are not required to adopt the API and some are signing bilateral agreements that contemplate APIs that are "aligned with" FDX standards. *See, e.g.*, Financial Data Exchange, Press Release, Ally, Discover, MassMutual, and TransUnion Among 25 New Members Joining the Financial Data Exchange (Jan. 27, 2020); Envestnet/Yodlee, Envestnet/Yodlee and JPMorgan Chase Sign Data Agreement to Enhance Consumer Data Protections, Bolster Overall Data Connectivity and Reliability, prnewswire.com (Dec. 5, 2019); Wells Fargo, Customers Will Have More Control, Convenience and Transparency when Sharing Financial Data with Plaid-Supported Fintech Apps, businesswire.com (Sept. 19, 2019); Financial Data Exchange, Press Release, Financial Data Exchange Adds 11 New Members, Makes API Publicly Available (May 28, 2019).

that are similar to those previously suggested by the CFPB and private groups to ensure that the new system protects consumer and small business interests,[131] it has not indicated whether it intends to adopt specific standards for members.[132]

Acquisition activity and other market developments in late 2019 and early 2020 have further increased uncertainty and tensions among transfer system participants. For instance, Visa's announcement that it was purchasing data aggregator Plaid for $5.3 billion sparked both hopes that the payments network could help facilitate better relations, technological adoption, and liability resolution in the broader data transfer system and fears that aggregation services would become more expensive and difficult to obtain for fintechs.[133] In addition, Fidelity announced that it was spinning off its Akoya data sharing subsidiary to become an independent company owned jointly by Fidelity and 11 banks that are members of The Clearing House, raising both hopes that the new venture could help facilitate data sharing activities by smaller firms for which bilateral agreements may be impractical and fears that it would be used by participating institutions to exercise greater control over the scope of data flows going forward.[134]

Particularly coming on the heels of moves by some individual banks to shut off screen scraping by one or more aggregators and the release of The Clearing House's template agreement providing for charges for data access,[135] the announcements are prompting substantial debate and speculation about the potential for further acquisitions and shifts in the balance between banks, aggregators, and fintechs in securing reliable data access going forward.

Overall, while recent industry-led efforts suggest a growing recognition by different market actors that individual firms would benefit from the establishment of broad-based norms, there are substantial questions about which groups of stakeholders will exert the most influence over standardization efforts going forward and how particular decisions will be made. The efficiency gains from standardizing certain baseline technology issues appear relatively intuitive, but questions about standardizing the scope of data being transferred and managing liability risk are closely intertwined and implicate much more complicated dynamics. It is also significant to note that smaller institutions and consumer advocates have somewhat limited representation in the process. Thus, the scope and success of these efforts remains to be seen in solving technological, competitive, and compliance concerns as the data transfer system continues to evolve.

131 See note 90 and accompanying text, Box 4.2.1, and Appendix D.

132 FDX, Organization Overview at 5-6 (endorsing customer control, access, transparency, traceability, and security). Materials released in August 2019 state that FDX intends to document best practices with regard to user experience and consent guidelines and otherwise to provide support to members so that they can adopt the core principles. *Id.* at 4, 6.

133 Verhage & Metcalf; Cara Lombardo & AnnaMaria Andriotis, Visa to Pay $5.3 Billion for Fintech Startup, Wall St. J. (Jan. 13, 2020); John Adams, Visa's $5 Billion Plaid Deal Takes a Possible Rival Off the Table, Am. Banker (Jan. 13, 2020).

134 Penny Crosman, Fidelity's Data-Sharing Unit Akoya to Be Jointly Owned with The Clearing House, 11 Banks, Am. Banker (Feb. 20, 2020); PYMNTS, Fidelity Teams with TCH to Launch Personal Data Startup, pymnts.com (Feb. 20, 2020); Justin Baer, Fidelity's Parent Company Is Spinning Out Its Akoya Personal-Data Startup, Wall St. J. (Feb. 20, 2020); Larry Edelman, Fidelity Spins Off Business That Helps Consumers Control Financial Data, Boston Globe (Feb. 20, 2020). TCH also has a seat on the organization's board. The member bank investors are Bank of America, Capital One, Citi, Huntington National Bank, JPMorgan Chase, KeyBank, PNC Bank, TD Bank, Truist, U.S. Bank and Wells Fargo. Fidelity had originally announced Akoya's launch in summer 2019, describing it as being intended to act as a hub between banks, data aggregators, and fintechs. The company has offered a generic data sharing agreement as a baseline to address issues such as liability for breaches, as well as a software platform, dashboards to help both institutions and individual customers monitor data-sharing activities, and services to support tokenization and standardization of data to meet the FDX API formats. However, as of the time of the purchase announcement, the firm had less than 50 employees and the only company that was using its platform was Fidelity. Some sources suggested that other large financial institutions may have been reluctant to use Akoya because they viewed Fidelity as a potential competitor. Crosman, Fidelity Data-Sharing Hub; Baer, Fidelity's Parent Company.

135 See notes 124-126 and accompanying text. A third acquisition involves Intuit's purchase of Credit Karma, which provides access to credit scores, tax filing, and other financial management services to consumers. Nathaniel Popper & Michael J. De la Merced, Dealbook, Intuit to Buy Credit Karma to Create Financial Data Giant, N.Y. Times (Feb. 24, 2020). Intuit acts as a data aggregator but only for companies that it owns, such as Turbo Tax and Mint. See note 86.

BOX 4.2.4.1 REACTION TO RECENT ACQUISITIONS

News of Visa's purchase of Plaid and the spinoff of Fidelity's Akoya subsidiary have injected substantial uncertainty into the market for customer-permissioned data transfers. The Visa transaction is expected to take several months to complete due to regulatory reviews, after which Visa has stated that Plaid will remain a separate company. The acquisition triggered widespread speculation about the potential for additional purchases and acquisitions involving aggregators such as MX and Yodlee, though it was not clear at publication how news of the subsequent Akoya transaction might affect the likelihood of further transactions.

Much of the initial discussion of the Visa-Plaid transaction focused on its implications for payments and money transfer markets both in the U.S. and internationally. Although credit and debit card usage continues to grow, both Visa and MasterCard made other acquisitions in 2019 to improve their positioning with regard to other types of cross-border money transfers. As a growing number of countries adopt regulatory changes designed to promote "open banking" and there is a move toward real-time settlement systems, stakeholders suggested that the move would hedge Visa for potential disruption in its core businesses. Plaid leaders, who had begun to expand the company's footprint internationally, also emphasized the potential for faster international growth from the Visa acquisition.

Beyond the focus on money movement, there was also substantial speculation in the U.S. about how Visa's connection with Plaid could change dynamics in the data aggregation market, for instance whether it would reduce tensions with large banks and/or increase hurdles for fintechs by increasing the cost of data transmission and/or the onboarding requirements for obtaining initial data access. Some stakeholders suggested that Visa could help to address some of the liability and business-to-business challenges in the market, for instance by providing a common tokenization system and/or facilitating dispute resolution mechanisms.

Some commentary also focused on questions about whether Visa and Plaid can combine data sources. Once companies are affiliated, most Gramm-Leach-Bliley Act limitations on data sharing no longer apply. However, Plaid would still be bound by the terms under which it obtained authorization for data access from customers.

With regard to Akoya, parent company Fidelity announced that it was spinning off its data sharing subsidiary into an independent company that would be jointly owned by Fidelity and 11 banks that are members of The Clearing House.

Some news reports indicated that transaction participants hoped that the purchasing banks would become clients of Akoya and that the company would become a network for the entire financial services industry. News of the transaction drew immediate criticism by a trade association representing aggregators and fintechs, which voiced concern that if Akoya was used to consolidate control over customer data it would potentially prevent other third parties from accessing data consistent with consumer and small business authorizations.

Sources: Lombardo & Cimilluca; Crosman, Fidelity's Data-Sharing Unit Akoya; PYMNTS, Fidelity Teams with TCH; Baer, Fidelity's Parent Company; Edelman; Luisa Beltran, Envestnet Hires Goldman to Advise on Options for Yodlee. A Sale Could Be Coming, Barron's (Feb. 5, 2020); Thomas Brown & Tyler Griffin, Visa+Plaid — A Slightly Less Hot Take, Medium (Feb. 3, 2020); Scott Carey, Visa's Acquisition of Plaid Throws Up Data Reuse Concerns, TechWorld (Jan. 21, 2020); Ron Shevlin, What's Visa Going to Do with Plaid?, Forbes (Jan. 20, 2020); Penny Crosman, What the Visa-Plaid Merger Means for Banks, Fintechs, Am. Banker (Jan. 16, 2020); Commerce Ventures, Visa Buys Plaid: What Does It Mean?, Medium (Jan. 16, 2020); Julie Verhage, Visa's Plaid Takeover Signals Wave of Fintech Dealmaking, Bloomberg (Jan. 15, 2020); Verhage & Metcalf; Rey Mashayekhi, With Plaid Acquisition, Visa Makes a Big Play for the 'Plumbing' That Connects the Fintech World, Fortune (Jan. 14, 2020); Ben Thompson, Visa, Plaid, Networks, and Jobs, Stratechery (Jan. 14, 2020); Lombardo & Andriotis; Adams.

5. POLICY ANALYSIS

Potential Benefits and Challenges to Reaching Scale

The use of cash-flow data in credit underwriting is likely to keep growing, but the pace and nature of expansion within the next few years is difficult to predict. The way in which stakeholders and policymakers respond to competitive tensions, coordination challenges, and regulatory uncertainty will help to determine whether and when cash-flow underwriting can reach scale and achieve its potential to foster a more inclusive, efficient, and competitive marketplace.

The credit and data transfer markets detailed in the *Small Business Spotlight* and Section 4 are in a state of substantial flux, but market and policy considerations are beginning to push toward standardization. For instance, the availability of supplemental credit reports and generic scores that incorporate cash-flow information might substantially accelerate adoption by simplifying operational and compliance processes. Secondary market actors have also emphasized a need for more consistent benchmarks. At the same time, it remains to be seen when and how various groups of market actors will respond to these developments in light of remaining research questions, banks' current posture concerning non-prime markets, and the desire to develop proprietary models with unique insights relative to other competitors.

Standardization in the underlying data transfer system also remains a central question for credit and all other use cases in light of challenges in securing reliable access to data and continuing uncertainty about liability, information security standards, and related questions. Industry cooperative efforts suggest a widespread recognition of the disadvantages of continuing to try to manage these issues solely through bilateral contracts, but these self-governance efforts face substantial challenges in light of competitive tensions and coordination challenges among firms, the need to appropriately balance the interests of consumers and small businesses, and gaps in regulatory guidance and standards.

The ways in which credit and data transfer markets expand and evolve over the next few years will also influence the extent to which cash-flow underwriting presents potential risks and tradeoffs for consumers and small businesses with regard to privacy, fairness, accuracy, information security, and transparency. A wide range of stakeholders agree that strengthening informed consent and customers' control over their data would help borrowers realize the potential benefits of cash-flow underwriting and manage potential tradeoffs. Yet they are deeply divided over whether such control mechanisms could substitute for certain traditional prescriptive protections or whether

existing regulatory safeguards also need to be expanded and strengthened to ensure that cash-flow does not evolve in ways that heighten tradeoffs and risks for underserved borrowers.

These issues help to illustrate the potential tradeoffs between standardization, innovation, and individual control as credit and data transfer markets continue to evolve. Greater consistency could be positive for borrowers and firms alike to the extent that it creates greater efficiency and predictability for all market participants, reduces implementation costs and barriers to small firms, encourages investment activity, and reduces privacy tradeoffs and other customer risks. But standardization processes can also have negative outcomes depending on how they occur, for instance if certain industry segments are able to drive them in a way that strongly disfavors competitors, if they enshrine risky or abusive practices, or if the mode of standardization unduly inhibits investments in future beneficial innovations.[136]

Because these policy issues are complicated and interrelated, Sections 5, 6, and 7 approach them from different angles. Section 5 focuses on (1) the scope and nature of potential benefits of using cash-flow data in credit underwriting; and (2) current challenges to cash-flow underwriting reaching scale. Section 6 focuses on (1) potential tradeoffs and risks for consumers and small businesses with regard to cash-flow underwriting as credit markets and the data transfer system expand and evolve; and (2) the potential role that enhanced customer control can play in both realizing the benefits and mitigating the risks of cash-flow underwriting. Section 7 concludes with a discussion of strategic and sequencing considerations for industry, regulators, and Congress, respectively, in addressing critical policy challenges within the next several years.

In considering issues across the three sections, existing laws that apply to traditional credit processes and financial data transfers are often a helpful reference point for analysis, even if they are not applicable to particular circumstances or their interpretation in the cash-flow context is in dispute. Yet the existing regimes may also be in need of modernization and adaptation even in traditional contexts, and more generally have not been built to account for the particular nature of cash-flow data or the processes used to transfer it between companies. We have therefore structured the following analyses to sweep more broadly than existing regulation, with an eye toward fostering a marketplace that:

- Enables choice, competition, and greater access to credit in consumer and small business markets;
- Encourages responsible innovation, including the development of safe and affordable products and services;
- Empowers consumers to take greater control in deciding when, where, and how their financial data is used;
- Aligns incentives for data-acquisitive business models to respect privacy and promotes the security, stability, and reliability of the data transfer system as a whole; and
- Assigns responsibility for safeguarding data and imposes accountability where such data is misused by authorized parties, exposed in a breach, or rendered inaccurate.

These principles may also be useful in structuring the treatment and transfer of customer-permissioned data in other contexts, even where federal laws that focus specifically on credit underwriting are not relevant.

136 For general discussions of standardization within the life cycle of innovation, *see, e.g.,* Knut Blind et al., The Impact of Standards and Regulation on Innovation in Uncertain Markets, 46 Research Policy 249 (2017); Henry King, 5 Ways That Standardization Can Lead to Innovation, Fast Company (Aug. 3, 2011); Michael Cusumano et al., Product, Process, and Service: A New Industry Lifecycle Model (Mar. 8, 2007); Gregory Tassey, Standardization in Technology-Based Markets, 29 Research Policy 587 (2000).

FinRegLab does not view its role to include advocating for specific policy alternatives, but hopes that providing these analyses may facilitate deeper and more efficient engagement by market stakeholders and policymakers going forward. The goal is a balanced set of market norms and regulatory requirements that allows both borrowers and firms to benefit from the data, and likely involves a combination of market-led, regulatory, and legislative initiatives.

5.1 Potential benefits for inclusion, efficiency, and competition

While additional research is needed to determine cash-flow data's value and limitations in modelling credit risk for different products, populations, and economic conditions, our empirical research and interviews with firms that are piloting or broadly incorporating cash-flow data into their credit scoring and underwriting models suggest that the data is indeed beginning to expand access to credit, improve lenders' ability to forecast default risk, and enhance competition and innovation in consumer and small business credit markets. We cannot calculate a numeric estimate of how large these benefits are or could become, but offer several observations with regard to their scope and nature:

Expanding access to credit: While the most obvious use of cash-flow data in underwriting is to evaluate consumers and businesses that lack traditional credit scores, our research suggests that the information adds meaningful predictive power for a substantially broader swath of applicants because it provides somewhat different insights than traditional credit bureau data. For example, cash-flow data may be particularly useful in assessing as many as 80 million consumers who often pay higher prices or are rejected outright by lenders because they have scores in the non-prime range, in addition to the roughly 50 million consumers who cannot be scored by traditional models due to lack of credit history.[137] Cash-flow data may be particularly important in sorting risk more finely within credit score bands that traditional lenders currently will not serve because the overall level of defaults exceeds their particular risk tolerances, even though a majority of borrowers are in fact likely to repay.[138] And even for prime customers, cash-flow data might allow lenders to provide faster processing and more tailored offers for credit products.[139]

Cash-flow data could also be particularly important for increasing credit access among African-American and Hispanic applicants, who are substantially more likely than whites to have low or no credit scores.[140] As noted in Section 2.2, studies suggest that about 10 to 11 percent of African-American and Hispanic households lack bank or prepaid accounts, compared to 27 to 28 percent of individuals who lack traditional credit scores and roughly 32 to 36 percent of households that do not have "mainstream" credit products that are likely to be reported to credit bureaus.[141]

These factors suggest that the inclusion impacts could be substantial, but they do not mean that all "credit invisible" applicants will be approved for loans or that all gaps in credit availability and use will be closed between demographic groups. For example, the use of cash-flow data is less likely to help households that do not have deposit or prepaid accounts because lenders are relying

137 Section 2.1.

138 Sections 2.2, 2.3. With regard to consumers with prime scores, it seems less likely that lenders or borrowers would have strong incentives to operationalize cash-flow data given the relative infrequency of defaults and the fact that prime borrowers are likely to be approved and to receive relatively low prices based solely on traditional credit information sources.

139 Compare Goldstein et al., at 4 (discussing fintechs using faster processing to market to prime consumers).

140 Similarly, in the small business space, to the extent that cash-flow data can make underwriting of smaller loans to younger businesses more cost-effective, it can potentially help substantial numbers of businesses owned by minorities, recent immigrants, and women access credit that would otherwise be unavailable. FinRegLab, Small Business Spotlight at 27-28.

141 CFPB, Credit Invisibles at 6, 17; FDIC, 2017 National Survey at 1, 7, 9-12, 18-19, 34-38, 48-58.

BOX 5.1.1 LONGER-TERM FAIR LENDING AND INCLUSION IMPACTS

While the information available to date suggests that cash-flow data could substantially improve credit access among underserved populations, a number of factors could affect its impact on particular individuals, groups, and markets. Given that underwriting models, regulatory protections, and privacy norms are continuing to evolve, it may be some time before the long-term effects on the market and on particular demographic groups become clear.

For example, differences among different demographic groups in the percentages of households with deposit and prepaid accounts, digital access, and attitudes toward privacy could potentially affect the speed and overall rate at which African-American and Hispanic applicants seek and obtain credit from lenders who use cash-flow data for credit underwriting. As discussed further in Section 6.2.2, given research suggesting that racial and ethnic minorities are more concerned about privacy and other customer protection risks than white borrowers, management of such concerns as the market evolves could have a strong effect on participation rates and inclusion benefits.

Long-term effects will also depend on how individual lenders choose to use the data for particular products and populations, how they construct and refine their particular eligibility and pricing models, and the overall economics of their businesses as discussed further below in Sections 5.1 and 5.2.1. Studies of the initial adoption of credit scoring in small business markets found that access to credit and average prices increased at the same time, most likely because lenders were sufficiently confident to extend loans to applicants they would previously have rejected, but tended to charge them higher prices at least initially because they considered many of the new approvals to be higher risk. Due to data gaps, it is not clear how average prices or prices for individual new borrowers changed over time as they built repayment history.

And while there is little question that providing access to credit for applicants who are currently shut out of the lending system increases net inclusion, the effects of using more predictive models to evaluate applicants who can already access credit will have some degree of individual effects in both directions. Because of the improved ability to predict default risk, some applicants are likely to receive larger loans or better terms, while others may be charged higher prices, receive smaller loans, or be denied altogether. These shifts can help ensure that applicants do not receive credit that they cannot in fact afford to repay, but they make it more difficult to forecast overall effects at a group level.

For these and other reasons, it is mathematically possible that the use of cash-flow data by an individual lender or across the market could increase the raw number of loan approvals across all demographic groups, but that disparities in group approval rates and/or average pricing may not move in lockstep. Such results could also change over time as new borrowers build more repayment history, lenders refine their models, and other market conditions change. Thus, while cash-flow data appears to hold real promise, its full effects will take some time to assess.

Sources: FDIC, 2017 National Survey at 1, 7, 9-12, 18-19, 34-38, 48-58; Terri Friedline & Zibei Chen, Digital Redlining and the Fintech Marketplace: Evidence from U.S. Zip Codes (2019); Andrew Perrin & Erica Turner, Blog, Smartphones Help Blacks, Hispanics Bridge Some—But Not All—Digital Gaps with Whites, Pew Research Center (Aug. 20, 2019); Federal Reserve Bank of Kansas City, Disconnected: Seven Lessons on Fixing the Digital Divide 11-12, 40 (2019); Giulia McHenry et al., Digital and Financial Inclusion: How Internet Adoption Impacts Banking Status, National Telecommunications & Information Administration Working Paper (Aug. 31, 2017); Allen N. Berger et al., Credit Scoring and the Availability, Price, and Risk of Small Business Credit, 37 J. of Money, Credit & Banking 191 (2005); Frame et al., 39 Fin. Rev. at 35-54.

heavily on electronic sources.[142] And while cash-flow data can provide insight into how applicants with particular levels of income and/or assets manage their finances, it cannot erase the fact that there are substantial disparities among demographic groups with regard to those factors in the first place.[143] Thus, it is important to set reasonable expectations, particularly given that impacts at the individual, group, and market levels may vary and evolve over time.

142 As discussed in note 47 and Section 3.1, some lenders are willing to gather cash-flow information from unbanked applicants via physical copies or smart phone snapshots of receipts and other individualized records, and then use automated underwriting models to assess the data. Collecting this information may take additional time and effort, though some companies are providing digitization services to make it easier to combine information from diverse sources. The interactions between lenders and applicants that are needed to collect such information may also have benefits, for instance by engendering a sense of mutual obligation on behalf of consumers. *See, e.g.*, Wang at 15.

143 See Section 2.2 and Box 2.2.2.

Improving risk prediction and lender efficiency: Improving risk prediction and facilitating more efficient underwriting could have substantial benefits for lenders, for instance by lowering their costs of supplying credit over time, as well as improving portfolio performance and market stability. In addition to improving lenders' ability to manage credit risk, the operational benefits are particularly appealing in the small business market, where there has been less automation historically. However, even for consumer markets, electronic cash-flow data could potentially make it more cost-effective for lenders to underwrite applicants that have historically been expensive to evaluate and to meet demand for smaller loans, as well as potentially reducing the price charged for credit to at least certain segments of customers.

Enhancing customer-led competition and innovation: The use of cash-flow data in credit underwriting is helping consumers and small businesses gain access to new products, more convenient origination processes, and new providers. For example, some providers are developing products as an alternative to bank overdraft programs or traditional payday loans.[144] Fintech lenders have also used cash-flow data and other technology to increase the speed and convenience of the application process, which has been particularly important in small business markets where underwriting and loan originations have historically been lengthy and paper-intensive.[145] The use of cash-flow data has also attracted new lenders, including not only general fintechs but some mission-driven providers and, in small business markets, companies whose primary business is e-commerce, payment processing, and accounting software.[146]

The ultimate benefits with regard to pricing and product structures remain to be seen as the market evolves; for instance, stakeholders are still assessing the benefits and risks of particular new product structures as experimentation continues.[147] In addition, fintech lenders tend to have higher cost of funds and customer acquisition expenses than banks and credit unions, and their pricing is continuing to evolve as they increase scale, form new business partnerships, and work to improve access to secondary markets.[148] Thus, future benefits from competition and innovation may depend both on whether traditional lenders begin using cash-flow data more widely and whether nonbanks can improve the economics of their business models, as discussed further in Section 5.2.

5.2 Challenges to reaching scale

Consumers and small businesses cannot realize any benefits from cash-flow underwriting if firms do not adopt it in the first instance. Our market research suggests that whether and when cash-flow underwriting can reach scale will depend largely on the extent to which: (1) banks and investors determine that the data is sufficiently useful to warrant changes to their business processes; and (2) lenders of all types can secure reliable access to the data when it is held by other companies.

144 For discussions of a range of alternative products including ones that rely on cash-flow analyses, see Peter Renton, The Inevitable Movement Towards No Overdraft Fees, Lend Academy (Sept. 23, 2019); Mary Wisniewski, These Challenger Banks Killed the Overdraft Fee. Now, They're Reinventing It, Bankrate (Sept. 12, 2019); Lydia Beyoud, Fintechs Step Into Payday Alternatives Where Banks Fear to Tread, Bloomberg Law (Dec. 18, 2018); Baker, Small-Dollar Credit at 39-88; Suman Bhattacharyya, How Lending Startups Are Trying to Edge Out Payday Lenders, Tearsheet (July 31, 2017).

145 FinRegLab, Small Business Spotlight at 6-9, 19-22.

146 FinRegLab, Small Business Spotlight at 19-22; Section 4.1.1.

147 For example, in small business lending, stakeholders are divided on products that structure repayment requirements as daily or weekly remittances based on sales volume. Defenders assert that structuring repayment terms to vary with sales volumes can be advantageous to small businesses, while critics assert that it can make it difficult for borrowers to predict and manage their finances and can trap them in debt. FinRegLab, Small Business Spotlight at 25; Lipman & Wiersch, Uncertain Terms at 19-20.

148 Perkins at 7-11; Steve Fromhart & Chris Moller, Funding Takes Center Stage for Nonbank Online Lenders, Deloitte Insights (July 9, 2018); Tanaya MacHeel, Why Customer Acquisition Is So Difficult for Financial Startups, Tearsheet (Nov. 7, 2017); QED Investors & Oliver Wyman, The Brave 100: The Battle for Supremacy in Small Business Lending 19, 24, 27 (2015); Chris Myers, For Alternative Lenders To Be Successful, Differentiation Is Key, Forbes (Oct. 15, 2015).

As noted above, the availability of third-party scores and supplemental reports that incorporate cash-flow information and industry self-governance efforts to regularize data transfer technologies could reduce operational challenges to continuing use and further adoption. Nevertheless, it remains to be seen how these initiatives will play out, particularly in light of competitive issues, coordination challenges, and regulatory uncertainty. Greater consistency in business practices and regulatory standards could potentially facilitate expanded use of cash-flow data, but striking an appropriate balance between standardization and flexibility to provide room for additional innovation is a central challenge.

5.2.1 Uncertainty among banks and investors

Banks' and investors' willingness to embrace cash-flow underwriting will depend both on resolving remaining questions about the data's predictiveness and on their assessments of potential rates of return relative to the operational, financial, and compliance challenges involved in making significant changes to their current business practices. These decisions in turn may impact non-bank firms that have already invested substantial resources in cash-flow underwriting, for instance by affecting opportunities for marketplace lenders to secure more stable liquidity via secondary markets and to reduce customer acquisition expenses through new business partnerships.

A gradual increase in the use of cash-flow data in credit underwriting over the next few years may be more likely than a dramatic jump in scale. The ultimate scope of use may depend on banks' appetite for serving different segments in consumer and small business credit markets.

This section analyzes core considerations for banks and investors, including (1) questions about the reliability of cash-flow models; (2) banks' approach to non-prime consumer markets; (3) operational and compliance hurdles to bank implementation; and (4) secondary market considerations.

5.2.1.1 Questions about the reliability of cash-flow models

Questions about the effectiveness of cash-flow data in predicting credit risk across different populations, products, and economic conditions are fundamental to the pace of its adoption. In addition to FinRegLab's 2019 research, information on the UltraFICO pilots across several different financial institutions is expected to be released in early 2020. As discussed in Section 4.1.2, a number of individual banks appear to be using cash-flow data in limited ways with regard to existing customers or in piloting "second look" programs that evaluate consumers who have been rejected based on traditional criteria.

These sources are likely to spur further interest among banks in harnessing their own deposit information for consumer credit underwriting. Given that banks have direct access to the account data of their existing customers, they are particularly well positioned to evaluate remaining research questions through modelling and pilot programs if they are willing to invest the resources to do so. As discussed in Section 3.2, such questions could include what specific variables are most predictive for the kinds of populations and products that were evaluated in FinRegLab's research, as well as the utility of the data for predicting defaults on other types of credit products such as auto loans or mortgages.

BOX 5.2.1.1.1 CASH-FLOW UNDERWRITING IN MORTGAGE LENDING

The possibility of using cash-flow data in mortgage underwriting is attracting substantial interest among mortgage stakeholders, but there are also particular challenges to its potential adoption in that market.

Historically, mortgage lenders relied heavily on debt-to-income (DTI) ratios in manual underwriting. As automated underwriting systems began to allow more sophisticated analyses of multiple variables, the importance of DTI decreased because factors such as loan-to-value ratios and generic credit scores were shown to be more predictive of default risk than DTI once various compensating factors were controlled for. However, DTI has taken on renewed significance since the financial crisis, in part because changes to federal law require lenders to assess whether applicants have the ability to repay a mortgage based on various criteria including either DTI ratios or "residual income" (RI) after paying for major expenses.

Many stakeholders believe that residual income analysis is a better measure than DTI of determining whether borrowers have sufficient income to cover both living expenses and new debt obligations, particularly for low-income families. For example, a family with a DTI of 43% and an income of $20,000 is much differently situated than a family with a DTI of 43% and an income of $200,000. However, because there are relatively few standardized benchmarks for how to determine what level of residual income is sufficient in light of local costs of living and other factors, federal regulations and industry practice currently both focus heavily on DTI analyses.

Use of electronic cash-flow data is therefore appealing because it might offer an opportunity to develop broad-based RI models that are more sensitive and predictive, as well as developing a better sense of thin file applicants' propensity to repay. Research since the financial crisis has further emphasized the impact of income shocks and financial reserves on borrowers' default risk, as discussed in Appendix C.

In early 2020, several members of the House Financial Services Committee requested the Government Accountability Office to conduct a study of the potential use of alternative data in the mortgage market. The Consumer Financial Protection Bureau also transmitted a letter to Congress indicating that it intends to propose an "alternative" to a part of its current rules that sets a 43 percent DTI threshold for certain "qualified mortgages." However, the letter suggests that the alternative metric could be a pricing threshold rather than an alternative approach to DTI or RI. The current DTI threshold has proven unpopular in part because it was accompanied by detailed rules that are designed to promote consistency in how income is treated and the metric is calculated.

Adoption of cash-flow data would also pose particular challenges in mortgage underwriting, in part because the secondary market is so large and so dependent on standardized procedures. As illustrated by its continuing dependence on FICO models that were developed in the 1990s as discussed in Section 2.3, if the entire market is not willing to adopt an innovation at the same time, this creates a strong economic disincentive for innovation because loans originated using different criteria may not be as easy to securitize, for instance by sale to the government sponsored entities Fannie Mae and Freddie Mac. They may also be treated differently with regard to repurchase requirements in the event of default.

Another challenge to broad-based adoption of cash-flow data is how to treat gross versus net income in light of deductions that may be made before income is deposited to the applicant's bank account. The current use of DTI generally avoids this problem by using gross income based on annual tax returns and other sources. Studies of bank account data suggest that it is difficult to forecast gross income based on bank account deposits.

Sources: 78 Fed. Reg. 6408, 6486-6487, 6525-6528 (Jan. 30, 2013); Kate Berry & Hannah Lang, 4 Questions as CFPB Closes in on Revamp of Key Mortgage Rule, Am. Banker (Jan. 21, 2020); Rep. Maxine Waters et al., Letter to the Hon. Gene L. Dodaro (Jan. 16, 2020); Diana Farrell et al., Trading Equity for Liquidity: Bank Data on the Relationship Between Liquidity and Mortgage Default, JPMorgan Chase Institute (2019); Christopher L. Foote et al., Technological Innovation in Mortgage Underwriting and the Growth in Credit, 1985–2015, Federal Reserve Bank of Boston Working Paper 19-11 (2019); Peter Ganong & Pascal Noel, Liquidity vs. Wealth in Household Debt Obligations: Evidence from Housing Policy in the Great Recession, National Bureau of Economic Research Working Paper No. 24964 (August 2018); JPMorgan Chase Institute, Estimating Family Income.

However, it remains to be seen whether banks will launch larger-scale projects until they can determine how models using cash-flow data perform during an economic downturn.[149] Although some fintech lenders report that stress tests of their models based on historical credit report data have returned positive results, it is not clear that the particular products or tests involved use of cash-flow information.[150] The ability to conduct robust retrospective testing depends on being able to access cash-flow information from more than a decade ago, which again underscores that banks are better situated to perform such analyses than other market participants.[151]

General concerns about alternative data's performance in economic downturns are raised frequently in public commentary about marketplace lending, particularly as fintechs' market share continues to grow as discussed in Section 4.1.1. However, it is often difficult to separate out any specific concerns about cash-flow data in particular, apart from more generalized uncertainty about non-traditional information sources and/or concern about other aspects of fintechs' business models.[152] Where sources have focused on aspects of alternative data that are more specific to cash-flow information, the discussions have highlighted both potential benefits and risks. Some sources emphasize that cash-flow data provides insights on income, reserves, and expenses, which have been the general focus of underwriting for decades. Given the data's greater detail and sensitivity, proponents point out that it could position lenders to begin working with borrowers earlier to avoid defaults and more quickly after business conditions start to improve, as discussed further in Section 6.1.2. Other sources have questioned whether greater sensitivity to changes in economic conditions could lead to quicker tightening of credit standards and worsen the severity of downturns overall.[153]

Yet while it may not be able to answer these questions completely until after the next downturn, additional testing and research projects could be useful to better understand performance as economic conditions change. For example, pro forma stress testing, studies of local markets that have

149 The current economic expansion is the longest in recent U.S. history but also the weakest. Fears that it would draw to a close in 2020 moderated in late 2019. Robin Wigglesworth & Keith Fray, The Record-Breaking US Economic Recovery in Charts, Fin. Times (July 4, 2019); Jon Hilsenrath, After Record-Long Expansion, Here's What Could Knock the Economy Off Course, Wall St. J. (June 3, 2019); Heather Long, After a Summer of Panic, Fears of a U.S. Recession Ease a Bit, Wash. Post (Nov. 5, 2019). It is unclear how federal safety and soundness regulators are thinking about risk with regard to economic downturns. The December 2019 statement on alternative data by the four federal banking agencies and the CFPB noted in a footnote that banks should "ensure that use of alternative data comports with safe and sound operations," and referenced the agencies' model risk governance as a relevant source of guidance. But it did not discuss any specific prudential concerns with regard to cash-flow or other alternative data. Interagency Alternative Data Statement at 1 n.2.

150 Nathan DiCamillo, Which Fintechs Are Best Positioned to Handle a Recession?, Am. Banker (June 28, 2019).

151 For a general discussion of stress testing for multiple purposes, see Basel Committee on Banking Supervision, Supervisory and Bank Stress Testing: Range of Practices (2017). Even for banks, access to historical data may be challenging depending on legacy systems. *See, e.g.*, Dave Keever & Chris Sifter, Does Your Bank Have the Stress Testing Data You Need?, bankdirector.com (Sept. 26, 2016). Historical data analyses may also be somewhat complicated because the last downturn was unusual in its length and intensity and because use of cash-flow data in underwriting was not widespread at that time, so that there is little data available concerning the performance of loans that were actually underwritten using the information.

152 *See generally* U.S. Government Accountability Office, Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data 14-16 (2018) (hereinafter GAO, Alternative Data Report); Perkins at 9-12; Treasury, Fintech Report at 136-37; Treasury, Marketplace Lending Report at 8, 23, 33; Robert Armstrong, How Online Platforms Shook Small Business Lending in America, Fin. Times (Jan. 29, 2019). Many of the concerns expressed are driven at least in part by differences in marketplace lenders' capital structures and revenue sources relative to traditional depository institutions. For example, discussions of business or credit cycle risk frequently point out that platform lenders typically do not have diversified business activities relative to banks, rely on relatively expensive and impatient sources of funding, and in some cases rely solely on fee income from new originations rather than repayment of loans over time. All of these features make it harder to survive a downturn in which losses are higher, the cost of capital increases, and demand for loans is lower. GAO, Alternative Data Report at 14-16; Perkins at 9-12; Financial Stability Board, Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention (2017); Wang at 33-35; *see also* Todd Baker, Marketplace Lenders Are a Systemic Risk, Am. Banker (Aug. 15, 2015). Some sources have suggested that improving securitization markets could reduce business cycle risks for platform lenders, while others have suggested that certain types of increased liquidity could actually exacerbate cyclical fluctuations. Treasury, Marketplace Lending Report at 25-26; Wang at 33-35.

153 Marshall Lux & Guillaume Delepine, Revolution in Data: How New Technologies Are Upending Borrowing, Harvard Kennedy School Mossavar-Rahmani Center for Business & Government Associate Working Paper Series No. 107, at 29-30 (February 2019); Armstrong. Some sources have also expressed concern that fintech lenders may exacerbate economic downturns because they are not subject to capital requirements and may be more subject to investor "de-risking." Wang at 33-35; Baker, Marketplace Lenders.

experienced downturns, and analyses of borrowers who have suffered income or expense shocks can be informative if not a full replacement for actual performance data during a nationwide downturn. Pilot programs and concentration limits are also ways to gather performance data within bounded limits, though we understand that concentration limits imposed by covenants on debt facilities are making it difficult for some lenders to expand the size of their trial programs.[154]

At the very least, launching trials now could position lenders to obtain better data as economic conditions change over time because they would have actual loan performance data for specific models and products, rather than modelling general predictiveness based on comparing cash-flow metrics to how consumers or small businesses repaid loan products that were not in fact underwritten using such data. Thus, establishing space for reasonable experimentation could be beneficial to firms and applicants alike.

5.2.1.2 Approach to non-prime consumer markets

A second central question driving banks' level of investment in both pilots and broader expansion of cash-flow underwriting is the potential rate of return relative to the costs of implementation and ongoing operations in particular product markets. This calculus may be particularly complicated for banks in the context of non-prime consumer credit, given that cash-flow data appears to have particular potential in these markets but that banks (particularly large institutions) have retreated from them in various ways since the financial crisis as discussed in Section 4.1.2.

The reasons for the general retreat from non-prime markets are complex and may include both economic and regulatory factors. Non-prime loans can have a lower rate of return than other business lines because they are smaller in size, relatively expensive to originate, and typically have higher default rates; although banks use risk-based pricing to account for some of these factors, they generally are reluctant to go beyond certain pricing ranges.[155] The returns from non-prime lending can also be more volatile cyclically relative to other business lines, and banks historically have often tended to invest more heavily in non-prime lending during early parts of credit cycles before exiting markets when losses begin to increase.[156]

In this particular cycle, large banks seem to have decided on extending wholesale lines of credit to non-bank lenders rather than direct lending activity themselves. Some stakeholders have suggested this may reflect a general preference to avoid volatility, while others have suggested that changes in capital requirements and other regulatory risk-management shifts since the crisis may have tended to discourage larger banks from deviating from traditional credit scoring models and

154 For example, we understand that covenants based on defaults or concentration in particular credit bands may be preventing non-prime credit card issuers and other lenders from testing cash-flow underwriting models more broadly because the covenants do not allow expansion absent recruiting more prime or near-prime customers, which may be impractical for the firms due to resource constraints.

155 *See generally* Oliver Wyman & Ideas42, Reimagining Financial Inclusion 15-21 (2015); U.S. House of Representatives Committee on Financial Services, Subcommittee on Financial Institutions & Consumer Credit, Hearing, An Examination of the Availability of Credit for Consumers (Sept. 22, 2011); Federal Deposit Insurance Corporation, A Template for Success: The FDIC's Small-Dollar Loan Pilot Program, FDIC Quarterly (2010); Bett Mattson-Teig, How to Make Small-Dollar Lending Make Sense, Independent Banker (Feb. 1, 2019); Bethany McLean, Payday Lending: Will Anything Better Replace It?, The Atlantic (May 2016). For a discussion of the drivers of rates of return in small business lending, see QED Investors & Oliver Wyman at 19-21.

156 Baker, Small-Dollar Credit at 36-38.

lending to riskier borrowers more generally.[157] Concerns that particular lending initiatives might be criticized as predatory by regulators or advocates may also be a factor.[158]

Thus, even with the increase in public research about the predictiveness of cash-flow data and progress on operational and compliance questions as discussed further below, it remains to be seen whether banks will prioritize modification of their consumer lending algorithms to incorporate cash-flow data. As noted in Section 2.3, take-up rates on past attempts to create more inclusive credit scoring models have been uneven.

At the same time, there are important implications for banks' long-term business models to the extent that they continue to cede ground to fintech lenders, particularly those who are using transaction account data to underwrite credit. Even if banks do not view non-prime customers as a core constituency, fintech lenders are not limiting themselves to that market, especially as they look to expand product offerings to current and new customer bases. To the extent that banks view transactional data about their customers as a core asset, the best means of preserving that franchise may be to operationalize that information for a broader range of those customers, particularly if electronic cash-flow data allows banks to provide credit in a more cost-effective way than traditional data. Thus, the spread of cash-flow data in underwriting is part of bigger strategic questions about banks' long-term market profiles.

5.2.1.3 Operational and compliance hurdles to bank implementation

A third consideration for banks is the up-front investment in time and effort needed to implement substantial changes in underwriting and compliance processes and to address any related examiner concerns. As discussed in Section 4.1.2, technological and resource constraints can be a substantial limitation, particularly for smaller banks and credit unions that may have a difficult time developing in-house programs and technologies. And depositories of all sizes are held to substantially greater scrutiny than fintech lenders in validating changes to their underwriting models, compliance with consumer laws, and partnering with outside vendors.

On the operational side, the market developments discussed in Section 4 are likely to increase the range of options for banks going forward. For example, a range of small and large banks are already partnering with marketplace lenders to leverage cash-flow data for small business underwriting.[159] Although cash-flow focused partnerships may not be as common in consumer credit markets right now, there are potential advantages to both sides in such arrangements because they

157 The impact of various regulatory requirements is disputed, but some stakeholders have suggested that stress testing requirements on the largest institutions that benchmark to traditional third-party scores could become a barrier to realizing the benefits of cash-flow underwriting. For example, the Comprehensive Capital Analysis and Review program for bank holding companies with more than $100 billion in consolidated assets relies heavily on "commercially available credit bureau scores" in assessing risk scenarios for various types of loans. Board of Governors of the Federal Reserve System, Dodd-Frank Act Stress Test 2019: Supervisory Stress Test Methodology 34, 36-37, 41, 43, 69 (2019). *See generally* Donald Kohn & Nellie Liang, Understanding the Effects of the U.S. Stress Tests, Brookings Institution 22-27 (July 9, 2019); Goldstein et al.; William F. Bassett & Jose M. Berrospide, The Impact of Post Stress Tests Capital on Bank Lending, Finance & Economics Discussion Series Working Paper 2018-087 (November 2018); John Heltman, Is Regulation Really Keeping Banks from Lending?, Am. Banker (Aug. 8, 2017). For an analysis discussion of capital requirements' impact on small business lending by large banks, see Yuliya Demyanyk, Have Stress Tests Impacted Small-Business Lending?, Federal Reserve Bank of Cleveland, Econ. Commentary (Nov. 14, 2019).

158 For instance, federal regulators have at times encouraged banks and credit unions to increase small-dollar lending to underserved populations, but at other times have set program conditions that did not strongly incentivize lending activity or have issued guidance that has discouraged particular product structures and practices. *See, e.g.,* Office of the Comptroller of the Currency, Bulletin 2018-14 (May 23, 2018); Office of the Comptroller of the Currency, News Release 2017-118, Acting Comptroller of the Currency Rescinds Deposit Advance Product Guidance (Oct. 5, 2017); Office of the Comptroller of the Currency, Bulletin 2013-40 (Nov. 26, 2013); Federal Deposit Insurance Corporation, Guidance on Supervisory Concerns and Expectations Regarding Deposit Advance Products (Nov. 21, 2013); FDIC, A Template for Success at 32. *See generally* Lalita Clozel, Banks Want Reassurance on Payday-Type Loans, Wall St. J. (Sept. 6, 2019); Baker, Small-Dollar Credit at 36-38.

159 FinRegLab, Small Business Spotlight at 19-22.

BOX 5.2.1.3.1 INTERAGENCY STATEMENT ON ALTERNATIVE DATA

The December 2019 interagency statement on the use of alternative data in credit underwriting follows on a recommendation by the Government Accountability Office urging federal financial regulators to provide more guidance concerning alternative data given both its potential benefits for inclusion and risks for consumer protection. It was issued by the four prudential regulators and the Consumer Financial Protection Bureau.

The statement specifically cites using cash-flow data to evaluate applicants' income and expenses to determine repayment capacity as a situation in which "use of certain alternative data may present no greater risks than data traditionally used in the credit evaluation process." It also emphasizes that cash-flow data may be particularly beneficial for evaluating consumers who have a variety of income sources over time, and notes several aspects of the data that tend to reduce potential consumer protection concerns. These include the fact that cash-flow information is specific to the borrower, is generally derived from reliable sources, and can generally be explained and disclosed to the borrower in adverse action notices. Finally, the statement notes that the permissioning process for accessing the data can help to enhance transparency and consumer control.

The agencies also specifically highlighted the use of "second look" programs that may consider alternative data only for applicants who would otherwise be denied credit, noting that such programs may improve credit opportunities.

At the same time, the statement emphasizes that cash-flow data, second look programs, and other uses of alternative data must comply with applicable consumer protection laws and be subject to a well-designed compliance management program that is calibrated to the particular level of risk. The statement notes that firms can consult with appropriate agencies when planning the use of alternative data and that the agencies may issue further statements in the future. They provided contact information for feedback on the statement but did not formally request comment.

Sources: Interagency Alternative Data Statement; GAO, Alternative Data Report at 45-46.

allow banks to benefit from the fintechs' modelling experience and technology platforms, while helping marketplace lenders address their high customer acquisition costs and capital limitations. The general trend toward cooperation may further accelerate to the extent that fintech business models are put under pressure in an economic downturn.[160]

The availability of third-party credit scores that incorporate cash-flow data and supplemental credit reports with cash-flow data and attributes will also provide potential routes to implementation in consumer markets. While using distilled attributes and/or scores may not provide quite as much flexibility to lenders as developing proprietary models based on full underlying account data, they have a number of other advantages. For example, such sources are available for both existing and new customers, can help to facilitate comparisons across institutions, and can facilitate compliance with consumer disclosure requirements as discussed further in Section 6.1.1.2.[161]

Finally, the fact that the largest core processor and a small bank trade association have joined the FDX initiative to focus on standardizing APIs and other systems for transferring transaction account data may also help to facilitate new developments to make it easier for small banks to participate in the broader data transfer system. Direct access to non-account holders' cash-flow data would make it easier for smaller institutions to underwrite new applicants using proprietary models.

160 Such partnerships may also be appealing to banks to the extent that they may receive credit under the Community Reinvestment Act, which imposes an obligation on banks and other depositories to meet credit and other financial services needs in low- to moderate-income areas from which they draw deposits. 12 U.S.C. § 2901; Michael Gaughan, Commentary: FinTech and the Liberation of the Community Reinvestment Act Marketplace, Cityscape 187, 193 (2017); Evan Sparks, How to Understand and Partner with Marketplace Lenders, ABA Banking Journal (Feb. 17, 2016); Colin Wilhelm, Citibank, Lending Club to Partner on CRA Loans, Am. Banker (Apr. 14, 2015).

161 See Box 4.1.1.2. For a discussion of reason codes and adverse action notice requirements, see FICO, Introducing the Ultra-FICO Score; Section 6.1.1.2. Transmission of only scores and particular underlying attributes may also reduce privacy concerns as discussed in Section 6.1.1.1.

Uncertainty about compliance issues could also be a factor for banks and credit unions that are considering adoption of cash-flow underwriting, although the outlook on that issue has also improved. To the extent that banks and credit unions have assumed that they may face a high burden of proof in changing their credit models, the December 2019 statement by all four federal banking agencies and the Consumer Financial Protection Bureau on alternative data is encouraging because it specifically notes that cash-flow data may present no greater risks than traditional information sources when it is used to evaluate repayment capacity based on income and expense activity over time.[162] At the same time, the statement also emphasizes that "[m]any factors associated with the use of alternative data, including those discussed for cash flow data, may increase or decrease consumer protection risk" and necessitate a robust compliance program.[163] The statement also does not provide any specific substantive guidance on various compliance or interpretive questions with regard to either cash-flow underwriting or the underlying data flows that are discussed further in sections 5.2.2 and 6.1.[164]

The December 2019 statement by all four federal banking agencies and the Consumer Financial Protection Bureau on alternative data is encouraging because it specifically notes that cash-flow data may present no greater risks than traditional information sources when it is used to evaluate repayment capacity.

5.2.1.4 Secondary market considerations

The ability to sell or securitize loans and attract other forms of investment will help to determine the pace at which lenders who decide to use cash-flow data—bank or non-bank—can serve additional customers.[165] While marketplace lenders have increasingly been selling loans and attracting investments from institutions and secondary market investors,[166] as noted above their cost of funds is more volatile than banks and credit unions and the processes for facilitating these transactions can be cumbersome. Some sources suggest that improving securitization opportunities could improve market stability more generally.[167]

Investors' level of interest in loans underwritten with cash-flow data depends on the same kinds of questions about the data's predictiveness discussed above, plus assessment of the firms' individual appetites for risk and return. Secondary market participants report that they are reluctant to place substantial weight on cash-flow variables used in either consumer or small business lending until they are tested in an economic downturn. This reluctance is compounded by the lack of standardized practices and benchmarks that can be applied across different firms that are using different cash-flow variables and metrics. As discussed in Section 2, for traditionally underwritten loans, third-party credit scores are often used to make comparisons across lenders, monitor portfolio performance, and facilitate securitization and investment transactions because they provide a common benchmark across companies even for lenders that do not rely heavily on the scores in their actual underwriting decisions.

162 Interagency Alternative Data Statement at 2.

163 *Id.*

164 For example, the statement specifically notes that it is focused on the use of alternative data in the credit process, but not the furnishing, compilation, or transfer of such data. *Id.* at 1 n.1. As discussed above in n.146, it also does not discuss any specific prudential concerns with regard to cash-flow or other alternative data. *Id.* at 1 n.2.

165 Indeed, banks sometimes act as investors by purchasing loans from fintechs, though not all such companies use cash-flow data. Perkins at 6-7; Lending Club, Banks and Lending Club, lendingclub.com (visited Feb. 11, 2020) (reporting that 54 banks representing 38 percent of the firm's investor base purchase loans from the platform); Jason Jones, 2017 Will Be a Huge Year for Bank Partnerships, Lend Academy (Nov. 14, 2016) (discussing the structure of various bank/fintech collaborations in consumer and small business lending).

166 Edward L. Truitt Jr. & James Lawler, Marketplace Lending ABS Moves Closer to Mainstream, Maples Group (2019); Allen Taylor, The Rise of Marketplace Lending Securitization, Lending Times (Dec. 19, 2018); Wang at 21-25.

167 Treasury, Marketplace Lending Report at 25-26; but see Wang at 33-35 (suggesting that certain types of increased liquidity for fintech lenders could actually increase cyclical fluctuations).

With cash-flow underwriting, however, there may not yet be enough activity in particular product markets to give investors a basis for a meaningful comparison or a means of developing a common benchmark. Our stakeholder interviews suggest that investors and rating agencies are currently "cross-walking" information on loan portfolios that were originated using electronic cash-flow data back to traditional credit scores.[168] But doing so is somewhat awkward and inefficient for lenders that are primarily focused on underserved borrowers, given that cash-flow data's greatest potential appears to be in assessing applicants who can't be reliably scored or differentiated based solely on traditional information.

This issue serves to highlight some of the challenges of an "each company for itself" approach, and how market pressures tend to encourage standardization over time. While innovators are often fiercely protective of their proprietary information and business advantages, periods of intense market experimentation can make it more difficult to attract investors and foster secondary markets. At the same time, as discussed in Section 2, there can also be risks in coming to rely too heavily on common metrics, as illustrated by experience in mortgage markets where the costs and complications of moving all market actors to updated credit scoring models have caused delay in use of models that are both more predictive and inclusive.

Initiatives to provide third-party cash-flow scores and attributes may have substantial impacts on this issue, though it seems likely that the development of stronger securitization models will likely occur at different times for different product types rather than for use of cash-flow data as a whole. Additional public research may also be useful, for instance by educating secondary market investors, regulators, and other stakeholders about the usefulness of particular cash-flow variables for particular populations, products, and circumstances.

5.2.2 Securing reliable data access

The second issue that will determine whether and when cash-flow underwriting can reach scale across both consumer and small business credit markets is the ability of all types of firms to secure reliable access to the underlying data. While these latter issues are less of a concern for banks if they are seeking only to underwrite existing customers,[169] any lender that wants to compete for new customers must give substantial thought to its ability to secure the scope of data needed to fuel its underwriting models in light of current uncertainties in the underlying system for customer-permissioned data transfers. Even with the growing use of APIs, one fintech and aggregator trade association reports based on data from its members that only about 55 to 60 percent of first-time attempts by consumers and small businesses to provide access to their account data at the nation's largest banks and credit unions are successful today, and that 5 to 15 percent have problems with recurring connections.[170]

As discussed in Section 4.2, competitive, coordination, and compliance issues are complicating the process by which the market is adopting safer and more efficient technologies for data transfers. Resolving these issues would not only facilitate competition and innovation in credit markets, but substantially reduce risk and uncertainty levels for applicants and firms alike. While industry initiatives are underway to resolve some of these challenges, the self-governance efforts face a

168 Fintech lenders who use non-traditional data and/or specialize in serving small businesses, borrowers with marred credit, and other riskier populations may also be required to hold loans on their balance sheets for longer periods of time to season before securitizing them. Wang at 21-23.

169 However, even for banks legacy systems and heavy reliance on core processors can cause some complications. See Section 4.1.2.

170 Financial Data and Technology Association, FDATA North America: Consumers and Small Businesses Lack Critical Access to Their Own Data Fields, fdata.global (Feb. 13, 2020). The report focuses on the largest banks and credit unions that are most likely to have established APIs for at least some data transfers.

number of challenges and some issues likely cannot be solved without policymakers' assistance. Once again, striking an appropriate balance between standardization and flexibility to provide room for additional innovation is a central challenge.

5.2.2.1 Scope of data and transfer technologies

The question that has attracted the most public debate concerns lenders' ability to access consistent data on an on-demand basis, which as described in Section 4 is not as certain as aggregators and end users would like in today's markets. While screen scraping facilitates competition and innovation by allowing lenders and other end users to access data without active facilitation by banks and other data sources, it can have substantial disadvantages with regard to burden on bank systems, frequency of access disruptions, and potential accuracy concerns. Screen scraping also generally relies on sharing of account login credentials, which significantly increases privacy, information security, and liability risks for businesses and customers alike.

Larger banks' efforts to transition to data access tokens, APIs, and dashboards could address many of these drawbacks, but particularly when implemented through confidential bilateral agreements are raising a different set of concerns about scale, consistency, and how competitive dynamics are shaping data flows and contract terms. Discussion of unilaterally cutting off screen scraping and the possibility of charging for data access also raises important policy concerns.[171] While it is not surprising that market actors would seek to share the costs of building APIs, depending on how pricing is structured it could become a way of imposing barriers to competition on particular use cases or parties. There are also questions about whether it is consistent with § 1033 of the Dodd-Frank Act.

Standardization of APIs, data elements, and dashboards could potentially reduce many of these second-generation concerns. But in the absence of congressional action to create a broad national data portability framework similar to what has been adopted in other jurisdictions, the only options to move in this direction are voluntary industry standards or more targeted actions by federal regulators.

Standardization in the traditional credit reporting market has largely been addressed by voluntary industry action rather than by regulation. However, as discussed in Section 2.1, the history of the traditional system also illustrates some of the disadvantages to this approach. For instance, there have been instances of information sources withholding information for competitive reasons, and delays in firms' making investments that are needed to keep up with technological and process improvements over time. Such behavior works to the disadvantage of both consumers and other firms, yet in those instances the private market was unable to resolve the issue until regulators or litigators stepped in to force broader changes.[172]

The evolution of the data transfer system to date as discussed in Section 4.2 also reveals competitive tensions and coordination challenges. The Financial Data Exchange appears to be attracting broader cross-industry representation than previous efforts, but it is difficult to gauge the status of its initiatives to foster the adoption of consistent APIs and data elements. Recent acquisitions activity and other market developments have increased uncertainty and tensions among transfer system participants, raising substantial questions about which groups of stakeholders will exert the

171 Because the APIs do not provide as much information as screen scraping methods, one industry group has estimated that as many as 1.8 billion consumer and small business accounts in the U.S. (including hundreds of millions of credit accounts) could be affected if the data sharing system was required to rely solely on those APIs as currently constructed. Financial Data and Technology Association, Credential-Based Authentication: A Necessary Tool to Enable Consumer and Small Business Data Access for the Foreseeable Future (undated). The number does not represent the number of customers impacted because individuals may hold multiple accounts, but FDATA estimated that such a change would affect tens of millions of U.S. consumers.

172 See Boxes 2.1.1, 2.1.3.

BOX 5.2.2.1.1 OTHER JURISDICTIONS' DATA REGIMES

Other nations and states are beginning to create regimes to promote customer data portability, control, and protections. These include:

UK Open Banking and PSD2: A major component of the United Kingdom's open banking initiative took effect in January 2018 to require the nation's nine largest banks to comply with customers' directions to share standardized data online with firms that have been certified by the Financial Services Authority. The initiative is being expanded to other financial products and services over time. Although the initiative is an outgrowth of European Union (EU) legislation called the Payments Services Directive 2 (PSD2), it is not expected to be reversed as the UK withdraws from the Union.

PSD2 requires member states to implement regimes to require banks to share information upon consumer authorization, but does not mandate development of standardized APIs or provide access to as broad of a range of third-party service providers as in the UK. Banks in both the UK and Europe have struggled to meet deadlines for providing APIs to eliminate screen scraping activities.

GDPR: The EU's General Data Protection Regulation (GDPR) imposes privacy protection requirements on businesses that collect, store, and transfer consumer data from transactions within EU member states. The GDPR framework outlines six legal bases that allow firms to process an individual's personal data, including situations where such processing is necessary to enter into a contract, where there is a legitimate interest to process an individual's data, and where the individual unambiguously consents. The GDPR also defines the conditions for informed consent and provides rights to revoke authorization and compel deletion of data.

In addition, firms that process data must incorporate seven protection and accountability principles outlined in the GDPR framework, which minimizes the amount of data collected and processed and time periods for storage. Data processing must be lawful, fair, and transparent to the data subject and all processing must be done in a way that provides security, integrity and confidentiality for consumers. Firms must also take steps to ensure that information is accurate and up to date.

Other countries: Canada, Mexico, Australia, New Zealand, Singapore, Hong Kong, Japan, and India are also adopting or considering open banking regimes, often in combination with more general data rights and protections. The Canadian government issued a report in January 2020 that recommends implementation of a structured environment for customer-permissioned sharing of financial data to replace credential sharing and screen scraping, but also concluded that such practices should not be barred until the replacement regime is in place. The Advisory Committee on Open Banking is expected to release a second report before the end of the year with more specific recommendations for transition processes and structures.

CCPA: The California Consumer Privacy Act (CCPA) took effect in January 2020, though enforcement will not start until later this year. The CCPA provides consumers with various rights concerning data collected by businesses from their transactions and devices, including the right to information, the ability to opt out of certain data sales, and the right to demand deletion. The law is more protective in some respects than the GDPR, and less in others. Where firms respond to consumers' requests for access to their data in electronic form, the format must be readily transmittable to other companies. The CCPA excludes certain categories of personal information from its privacy protection, including information collected pursuant to the Fair Credit Reporting Act and Gramm-Leach-Bliley Act.

Sources: Ian Hall, Australia Delays Launch of 'Open Banking' Regime, Global Government Forum (Jan. 9, 2020); Department of Finance Canada, Consumer-Directed Finance: The Future of Financial Services (2020); Nick Caley, PSD2 in 2019: A Year of Yet More Delays, FintechFutures (Dec. 30, 2019); Oana Ifrim, Open Banking—A Very Global Business, paypers.com (Dec. 19, 2019); Michael S. Barr et al., Consumer Autonomy and Pathways to Portability in Banking and Financial Services, University of Michigan Center on Finance, Law, & Policy Working Paper No. 1 (Nov. 3, 2019); Sebastian Anthony, What Is Open Banking, and Is It Safe?, bankrate.com (June 3, 2019); Deloitte, How to Flourish in an Uncertain Future: Open Banking and PSD2 (2017); Andrew Rossow, The Birth of GDPR: What Is It And What You Need To Know, Forbes (May 25, 2018); European Union, What Is GDPR, the EU's New Data Protection Law?, GDPR.EU (2018); Skadden, California Consumer Privacy Act: A Compliance Guide 22 (2019); DataGuidance & Future of Privacy Forum, Comparing Privacy Laws: GDPR v. CCPA (2018).

BOX 5.2.2.1.2 SECTION 1033 SCOPE OF COVERAGE

Section 1033 of the Dodd-Frank Act imposes obligations on "covered persons" to make data about consumer financial products and services upon consumers' request in an electronic, usable form. As discussed in Box 4.2.1, the CFPB had not yet issued rules to implement the provision or addressed whether it takes effect in the absence of regulations. There are several limitations on the right of access and interpretive issues regarding the scope of coverage.

For example, the law applies only to providers of "consumer financial products and services" as defined under Title X of the Dodd-Frank Act, which focuses primarily on loans, deposits, and similar retail services rather than products such as securities, retirement accounts, or insurance. While the latter group of financial products may not frequently be factored into credit underwriting, they can be important for purposes of providing personal financial management services to consumers.

And as noted in the main text, there is a debate about whether § 1033 extends to data aggregators who pull data to facilitate loan applications or the provision of other products and services to consumers. The law does not address small business data rights.

In addition, the obligation to provide data also only applies to data that is in the control or possession of the covered person. The statute expressly states that it does not impose a duty to maintain information in the first instance and that information that cannot be retrieved in the ordinary course of business is excluded from coverage. Section 1033 also exempts confidential commercial information (including algorithms for credit and risk scoring), information collected for the prevention and detection of fraud, money laundering, and other potentially unlawful conduct, and other information that is required to be kept confidential under other law.

The statute does not provide standards with regard to what type of request or consent is required to trigger data access or processes for correcting any errors in the data that is obtained. And although the general definition of consumer for purposes of Title X of the Act includes agents, trustees, and representatives acting on behalf of an individual, § 1033 does not address process issues in connection with third-party access, such as how the scope of access is defined or communicated to the covered person, how authorization can be withdrawn, or whether consumers have a right to compel such parties to delete the data.

Sources: 15 U.S.C. §§ 5481(5), (6), (11), (15), 5533.

most influence over industry standardization efforts going forward and how particular decisions will be made.

The other option is for the Consumer Financial Protection Bureau to take action to effectuate and interpret the scope of § 1033 of the Dodd-Frank Act. Although the law may not reach all financial product data that would be relevant for use cases such as personal financial management, the statute expressly states that consumers have a right to "information relating to any transaction, series of transactions, or to the account including costs, charges and usage data" in connection with deposit and prepaid accounts and other consumer financial products and services.[173] While some market actors have argued that the statute does not address access by data aggregators, the Dodd-Frank Act more generally defines "consumer" to include "an individual or an agent, trustee, or representative acting on behalf of an individual."[174]

However, while the statute specifically directs the CFPB to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files,"[175] other language is unclear as to Congress's intent on technical standards. In particular, § 1033 also directs the agency to consult with other federal regulators "to ensure, to the extent appropriate, that the rules … do not require or promote the

173 12 U.S.C. § 5533(a).

174 12 U.S.C. § 5481(4). The U.S. Treasury Department has stated that this language is "best interpreted to cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers." It also noted that the statute may not cover securities, insurance, and retirement accounts but declined to recommend that the statute be amended because it concluded that data access is being provided by those industries. Treasury, Fintech Report at 31-32.

175 12 U.S.C. § 5533(d).

use of any particular technology in order to develop systems for compliance."[176] Thus, the statute's direction as to regulators' role in promoting consistent technology is somewhat unclear.

These considerations may suggest that a hybrid approach could be advantageous. Under such an approach, the CFPB could use a rulemaking process to engage all stakeholders in defining the general scope of data to which § 1033 of the Dodd-Frank Act provides access, the conditions under which agents and representatives can access information on consumers' behalf, procedures for customer authorizations and disclosures, and a staged implementation process to account for the challenges facing smaller financial services providers. Industry in turn could focus on defining technology standards and tools to effectuate specified data transfers efficiently and securely, which would potentially provide more flexibility as market practices and technologies continue to evolve. Such an approach would necessitate regulators' immediate engagement in light of current industry efforts to standardize data elements and APIs. And Congressional action would likely be required to create a completely consistent standardized system for customer-permissioned financial data access across all use cases, given that § 1033 focuses only on access to information concerning consumer financial products and services.

5.2.2.2 Data security, liability, and compliance considerations

An additional set of hurdles to broader implementation of cash-flow underwriting involve concerns about data security, liability for breaches or misuse of data and login credentials, and related compliance questions as discussed in Section 4.2.3. These issues are closely interwoven with the scope of data access because some banks have argued that such access should be restricted until login credentials, personal identification information, and routing/account information can be better protected.

Concerns about security and liability risks are legitimate. Although to date no major breaches of aggregators have come to light, the increasing size of their activities makes them increasingly attractive targets.[177] And while EFTA's liability limitations protect consumers and promote overall confidence in electronic payment mechanisms by ensuring that consumers do not have to wait to be made whole while businesses are sorting out responsibility for mistakes or breaches, a system in which firms are not ultimately accountable for the consequences of their own security and data management practices would create misaligned incentives that could ultimately hurt the interests of consumers, other firms, and the data transfer system as a whole.

Yet managing these issues through bilateral contract negotiations is proving cumbersome for all parties, as evidenced by the fact that the system still has not transitioned away from credential sharing after more than two decades. Large banks' data sharing contracts are now moving substantial elements of the system away from that practice as well as attempting to address a range of other security, usage, and liability concerns about how data is transferred and managed downstream, but they are imperfect tools for managing the system as a whole.

First, the contracts simply do not reach all information transfers in the market, since they are largely confined to the largest institutions. Second, where each bank its own bespoke list of demands, negotiations take substantial time and resources and implementation becomes more complex for aggregators and end users. Third, there is a concern that business incentives and unequal bargaining

176 *Id.* § 5533(e)(3). The Bureau is required to consult with the federal banking agencies and the Federal Trade Commission in promulgating rules. In addition to the language discouraging use of particular technology, the agencies are directed to consult to ensure to the extent appropriate that the rules impose substantively similar requirements on covered persons and take into account situations in which firms do business both in the United States and other countries. *Id.* § 5533(e).

177 See Box 7.3.1 for more discussion.

BOX 5.2.2.2.1 GLBA INFORMATION SECURITY SAFEGUARDS

The Gramm-Leach-Bliley Act reflects a congressional policy that all financial institutions—whether banks or non-banks—have an "affirmative and continuing obligation" to protect the security and confidentiality of their customers' nonpublic personal information. Toward that end, the law directs federal regulators to adopt standards for administrative, technical, and physical safeguards to ensure the security and confidentiality of customer records, protect against anticipated threats and hazards, and protect against unauthorized access or use that could result in substantial harm or inconvenience to any customer. As discussed in Box 5.3.3.1, the law also restricts certain information sharing by financial institutions.

Implementation of GLBA was spread across eight federal agencies. The federal banking regulators and the Federal Trade Commission adopted similar safeguards requirements that require financial institutions to develop comprehensive written information security programs that are appropriate for the size and complexity of the particular institutions. The programs must (1) identify reasonably foreseeable internal and external risks to security, confidentiality, and integrity of customer information; (2) assess the sufficiency of the institution's existing safeguards; (3) design and implement additional protections such as ongoing testing and monitoring; and (4) evaluate and adjust the information security programs on a periodic basis to account for material changes in business operations and the results of testing and monitoring.

The regulators emphasized the need for generalized standards that will not become quickly outdated as technology changes and that can be adapted as appropriate for particular institutions' scale and complexity. Over time, the federal banking agencies have issued additional guidance through examination manuals and other documents to address issues as breach response planning and vendor monitoring. In 2019, the Federal Trade Commission issued a proposal that would adopt substantially more specific standards on these and other topics.

As discussed further in Box 5.3.3.2, the FTC drafted its original regulations more narrowly to define "financial institutions" as only those non-bank firms that were "substantially engaged" in "financial activities" as that term had been defined under the Bank Holding Company Act at the time that GLBA was enacted. The new FTC proposal would expand coverage to activities "incidental to a financial activity" to align more closely with how the federal prudential regulators defined "financial institution."

The safeguards provisions apply to the nonpublic personal information of "customers," meaning consumers who have an ongoing relationship with a financial institution, though financial institutions may apply them on a broader basis as a practical matter. As discussed further in Box 7.3.1, FTC rules require financial institutions to comply with safeguards standards with regard to any customer information they hold, even if they received it from another financial institution and do not themselves have a customer relationship with the particular consumer.

Sources: 12 U.S.C. §§ 6801, 6809(3), (4); 12 C.F.R. §§ 225.28(b), 226.86; 16 C.F.R. §§ 313.1(b), 314.1, 314.2(f)(1), (4)(i), (4)(iv); 84 Fed. Reg. 13158 (Apr. 4, 2019); 67 Fed. Reg. 36484, 36486 (May 23, 2002); 66 Fed. Reg. 8616, 8618 (Feb. 1, 2001).

power will skew both the terms of the contracts and the ways that they are executed in practice. In addition to concerns about large banks' competitive interests, for example, there are also potential concerns about aggregators as the contracts place increasing responsibilities on them to impose requirements and monitor end users with regard to information security, data usage practices, and other activities. It is unclear whether they have either the incentives or clout necessary to monitor end users consistently on all potentially relevant issues, especially since the end users are also the aggregators' customers.

Particularly when combined with the fact that regulatory expectations are unclear, the particular liability concerns connected to specific data elements, and the fact that the individual contracts are confidential, the current market has created substantial uncertainty and distrust among market participants. Although many stakeholders appear to agree at a high level that firms within the broader ecosystem should be responsible for data security harms that happen on their watch, there is substantial tension over which entities will have the ability to determine responsibility in particular instances, which harms will be recognized and how they will be measured, and how to establish reasonable and effective capacity or insurance requirements given the potential for particular aggregators and/or

fintech end users to increase scale quickly.[178] As a practical matter, stakeholders also report that it can be extremely difficult to obtain insurance in connection with a data sharing agreement unless banks are willing to cap aggregators' liability at some specific level because insurers are unwilling to take on open-ended obligations.

Federal regulators' authorities to settle business-to-business liability issues are limited, but a broad range of stakeholders say that clarifying legal requirements and supervisory expectations would help to begin providing greater certainty so that industry can concentrate on solving remaining challenges. The Federal Trade Commission is already engaged in a rulemaking that would increase the specificity and robustness of information security requirements for non-banks under the 1999 Gramm-Leach-Bliley Act, bringing them closer to the standards that apply to banks. For instance, the FTC proposed rule would require data aggregators, non-bank lenders, and other financial institutions to engage in more robust monitoring of their service providers, develop "incident response plans" for dealing with potential data breaches, and encrypt all customer information in transit and at rest.[179] However, the proposal would exempt small companies from certain requirements,[180] and two of the five FTC commissioners dissented from its issuance because they believed that the standards moved too far toward a "one size fits all" approach and were premature given the chance of legislation from Congress.[181]

Beyond this rulemaking, some firms have reported that more frequent updates to safeguards guidance would be useful for both banks and non-banks alike in light of continuing technological and market evolution. Stakeholders say it would also be helpful for the CFPB to clarify and reinforce the application of a second set of GLBA requirements concerning information sharing restrictions in the data aggregation context, as discussed further in Section 6.1.3.

Stakeholders also point to continuing regulatory uncertainty with regard to consumer and institutional liability under the Electronic Fund Transfer Act in situations where a consumer's login credentials are misused to conduct transactions on their accounts and with regard to whether aggregators or fintechs are potentially liable to consumers under EFTA as electronic fund transfer service providers, federal agencies' general expectations concerning banks' oversight of third-party service providers and responsibility to make consumers whole in the event of a downstream data breach, and whether and how the Fair Credit Reporting Act applies to information transfers for credit purposes as discussed further in Section 6.1.1.2.[182] As discussed further in Section 7, another lever for federal agencies to increase consistency in the market would be to increase supervision of non-bank firms for compliance with various federal consumer protection laws.

178 There are also tensions and distrust between banks and other market actors with regard to who controls the customer experience and mechanics of authorizing data access. Aside from concerns that banks would use the tokenization process to shut off or unduly restrict the scope of access, at least some aggregators would prefer to control interactions with all customers on their platforms. Banks, in contrast, would prefer to ensure consistent communications for their customers across all aggregators and fintech end users, and argue that their generation of tokens provides the highest level of security.

179 84 Fed. Reg. 13158, 13166-69, 13175-76 (Apr. 4, 2019) (proposed 16 C.F.R. § 314.4(c), (f)). The FTC's existing rules merely require that financial institutions take "reasonable steps to select and retain" service providers that are capable of maintaining appropriate safeguards, while the new version would specifically require periodic assessments based on the risk presented by particular vendors and the continued adequacy of their safeguards. 16 C.F.R. § 314.4(d).

180 84 Fed. Reg. at 13170-71, 13176 (proposed 16 C.F.R. § 314.6) (proposing to exempt financial institutions that maintain customer information for fewer than 5,000 consumers from certain requirements concerning written risk assessments, incident response plans, and annual written reports and from continuous monitoring or annual penetration testing and biannual vulnerability assessments). As discussed in Box 6.1.3.2, other aspects of the proposal would expand the definition of "financial institution" to more closely match the one adopted by federal banking regulators after GLBA's initial enactment. For example, the proposal would reach companies that act as "finders" by connecting potential buyers and sellers of goods and services for transactions that the buyers and sellers themselves negotiate and consummate. 84 Fed. Reg. at 13162 (discussing 12 C.F.R. § 225.86(d)(1)).

181 *Id.* at 13716-77.

182 See Sections 4.1.2, 4.2.3.

BOX 5.2.2.2.2 MANAGEMENT OF LIABILITY ISSUES IN THE PAYMENTS SYSTEM

Stakeholders sometimes point to the way that liability issues are handled in payment processing systems as a potential model for the system for customer-permissioned data transfers. In particular, they note that the processing systems for credit cards, debit cards, and automated clearinghouse transactions promote consumer confidence by severely limiting liability for fraudulent and unauthorized transactions, while providing business-to-business processes to sort out fault and liability without the need for substantial consumer awareness or involvement.

These systems are the result of several decades of evolution and depend on the interaction between federal consumer financial laws and private network rules. For example, the Electronic Fund Transfer Act limits consumers' liability in the event their debit cards are stolen to a maximum of $50 or $500 if they report the theft within certain timelines, but consumers often have $0 liability for unauthorized debit and credit card transactions due to network rules.

Network rules also provide back-end processes and procedures to govern investigations, business-to-business disputes, fees and penalties for failure to require network requirements, and other topics relating to fraudulent and unauthorized transactions. Although the requirements can be complex and are subject to various criticisms from system participants, they generally operate without substantial involvement from consumers to sort out back-end liability.

Development of the rules has been facilitated by membership organizations (generally called networks or clearinghouses) that set various standards and process requirements in addition to facilitating the underlying transactions. Because a credit card transaction can include as many as a half dozen parties, network rules can help to provide a consistent baseline that somewhat simplifies business-to-business contracting around liability and related topics.

However, while payment systems have evolved to handle the resolution of individual unauthorized transactions, they have struggled to sort out liability in cases of large-scale data breaches. For example, after a 2013 data breach at Target involving 40 million payment cards and 70 million customers' contact information, some banks and credit unions brought a class action lawsuit against the retailer for recovery of expenses relating to having to reissue millions of new credit and debit cards.

Sources: David A. Zetoony & Courtney K. Stout, Credit Card Data Breaches: Protecting Companies from Hidden Surprises, Lexis Practice Advisor Journal (Nov. 8, 2016); N. Eric Weiss & Rena S. Miller, The Target and Other Financial Data Breaches: Frequently Asked Questions, Congressional Research Service 7-10, 14-20 (2015); Salvatore Scanio & Jason W. Glasgow, Payment Card Fraud, Data Breaches, and Emerging Payment Technologies, 21 Fidelity L.J. 59 (2015); Richard J. Sullivan, Controlling Security Risk and Fraud in Payment Systems, Federal Reserve Bank of Kansas City, Economic Perspectives 47 (3rd quarter 2014); Sandeep Dhameja, Clarifying Liability for Twenty-First-Century Payment Fraud, Federal Reserve Bank of Chicago, Economic Perspectives 107 (3rd quarter 2013); Julia S. Cheney et al., The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches, Federal Reserve Bank of Philadelphia Payments Card Center Discussion Paper (Oct. 2012).

However, congressional action would be required to create a completely consistent framework where all parties who receive cash-flow data are subject to consistent substantive requirements, monitoring, and accountability. For example, the fact that no federal agency has general authority to examine non-banks for compliance with GLBA information security requirements is a major gap in the existing regulatory system, although federal prudential regulators can examine non-banks that act as third-party service providers to banks for GLBA safeguards requirements and have already done so for at least one aggregator.[183] Other countries have also created mechanisms to ensure that end users of customer-permissioned banking data are subject to regulatory registration, including proof of privacy and security protections and adequate insurance.[184] Some stakeholders have also suggested that Congress could also play a pivotal role in substantially improving the development of the private insurance market for cybersecurity risk, as discussed further in Section 7.3.

183 See n.292 and Box 7.2.1.

184 *See, e.g.*, Open Banking Implementation Entity, Third Party Providers, openbanking.org.uk (visited Feb. 13, 2020). The Consumer Financial Protection Bureau has some authorities under the Dodd-Frank Act with regard to non-bank actors that are subject to its supervision authority. See note 235.

Many stakeholders also see a substantial need and opportunity for broader industry self-governance initiatives to address ongoing concerns about security, liability, and related matters. They note that much of the infrastructure that supports resolution of liability for unauthorized and erroneous transactions in payments systems is supplied by business-to-business arrangements rather than by regulation, for instance through card network and clearinghouse rules, standardized representations and warranties in contracts, and other business mechanisms. Although there is not an umbrella entity in the data transfer system that plays quite the same role as card networks or clearinghouse associations, various data transfer stakeholders have suggested that increasing efforts to standardize information security standards, traceability mechanisms, and tokenization options could increase efficiency and reduce tensions in the broader system.

Although there has not been as much of a large public group effort to address back-end security and liability concerns as there has been for data transfer technologies, The Clearing House has been piloting a program that would conduct a single due diligence review of aggregators or fintechs for information security purposes that could then be relied upon by multiple banks in making decisions under the third party service provider guidance regarding risk management. Such a system potentially saves both banks and aggregators the time and expense of conducting multiple overlapping reviews.[185]

185 Statement of Natalie S. Talpas, PNC Bank, for the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records (Feb. 26, 2020); Statement of Natalie R. Williams, JPMorgan Chase & Co., for the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records (Feb. 26, 2020).

6. POLICY ANALYSIS

Customer Protection and Customer Control

While the increasing use of cash-flow data in credit underwriting is providing benefits for consumers and small businesses, it also presents privacy tradeoffs and potential concerns about fairness, accuracy, data security, and transparency. The choices that stakeholders and policymakers make as the market expands and evolves will determine whether these issues are mitigated effectively or whether cash-flow underwriting and underlying data transfers begin to evolve in ways that heighten tradeoffs and risks for underserved borrowers.

Customer protection concerns in connection with cash-flow underwriting are not limited to loan origination, but also can arise where lenders pull and review additional cash-flow data during servicing and collections, and to the extent that lenders, aggregators, or other vendors re-use cash-flow data for other commercial purposes. These issues may be somewhat distinct and in some cases more complicated than with regard to using cash-flow data for other use cases, given the amount of historical data that may be useful for credit underwriting, the consequences of credit decisions for both borrowers and lenders, and other factors. Many of these issues are also present with the use of traditional data sources for credit as well, but both the nature of cash-flow information and the processes by which it is transferred between companies can present additional considerations of which applicants may not be aware.

Initial market practices appear to be relatively conservative in some respects, and as discussed above there are some initiatives underway by individual companies and broader self-governance organizations to reduce reliance on credential sharing and screen scraping, address accuracy concerns, and increase applicant transparency. But those efforts also face a number of challenges due to competitive dynamics, coordination challenges, and regulatory uncertainty. And while many of the firms that have pioneered use of cash-flow data in credit underwriting have defined their missions with a relatively strong focus on inclusion, they may have few levers with which to ensure that later adopters conform to similar practices and standards for data use, sharing, and protection.

As the market continues to expand and evolve, uncertainty about the application of existing laws and inconsistency among market actors could potentially affect both the pace of growth and the extent to which cash-flow underwriting produces positive outcomes for consumers and small businesses. At the very least, failing to resolve these issues may make some applicants reluctant

to participate in cash-flow underwriting despite its potential benefits.[186] At the very worst, some stakeholders fear that credit markets could evolve in ways that increase privacy tradeoffs and risks for underserved borrowers, with few practical alternatives in the marketplace or protections against aggressive lender practices.

But stakeholders are deeply divided over whether policymakers should take action on particular issues prior to the manifestation of concrete problems in the market, as well as how best to mitigate particular risks. For example, stakeholders disagree about the extent to which consumers and small businesses could protect their interests if they were able to exercise greater control over their own data. A wide variety of stakeholders support taking steps to increase customer control, but they are deeply divided over whether such mechanisms could substitute for traditional protections or whether stronger prescriptive safeguards are also needed as the volume of data sharing increases rapidly across financial services markets.

Section 6.1 takes an issue-by-issue approach to outline particular customer-protection concerns with regard to the use of cash-flow data during the initial loan application process, in loan monitoring and collections, and in connection with firms' downstream re-use and sharing of the data for other purposes. The discussions include an overview of existing federal laws and guidance on related topics, as well as summarizing stakeholder debates about current and potential risks and mitigation strategies. Section 6.2 focuses on the broader cross-cutting debates about enhancing customer control to realize the benefits and mitigate the risks of cash-flow underwriting, as well as the balance between customer control, customer protection, and other policy goals. Section 6.3 concludes with additional observations about the risk that markets will evolve over time in ways that substantially disadvantage underserved borrowers.

6.1 Emerging risks for consumers and small businesses

As evidenced by the existence of various federal regulations and historical policy debates concerning traditional credit information sources, a number of potential policy issues can arise with regard to how customer information is used both in loan origination and subsequent servicing and collections. These include privacy and fairness concerns about how the data is used to make decisions, the accuracy and completeness of the data, concerns about data security and misuse in connection with underlying information transfers, and the extent to which borrowers understand these various issues and are making informed decisions throughout the course of the credit relationship. In addition, there are potential concerns about privacy, data security, and transparency to the extent that lenders, intermediaries, or vendors are able to re-purpose and share data for their own downstream business activities.

The nature of cash-flow data and the processes by which it is transferred create some differences in the ways in which these issues play out with regard to traditional credit report information. In addition, stakeholders are deeply divided over both the efficacy and the application of existing federal consumer financial laws in protecting consumers and small businesses from harm in connection with cash-flow underwriting and related data transfers. This section provides an overview of the debates about customer protection issues in initial credit decisioning, loan servicing and collections, and firms' downstream re-use and sharing of cash-flow data.

186 As noted in Section 5.1 and discussed further in Section 6.2.2, mitigation of privacy risks could be particularly influential in determining the extent to which African-American and Hispanic applicants are willing to authorize access to their data. Research suggests that racial and ethnic minorities are particularly concerned about data privacy and potential misuse.

6.1.1 Initial credit decisioning

As discussed above, one reason that cash-flow data is so useful for underwriting is its rich detail about how consumers and small businesses manage their finances on an ongoing basis. But this very same quality increases its potential privacy and fairness risks. Particularly where the data must be transferred between multiple companies to facilitate the underwriting process, accuracy and information security can be additional concerns. A final issue is whether consumers and small businesses have sufficient information to weigh the benefits, risks, and tradeoffs of both cash-flow underwriting and the related data transfers.

6.1.1.1 Privacy and fairness concerns

As discussed above, lenders and model developers appear to be focusing on financial variables that reveal overall patterns in income, expenses, and reserves and in how applicants manage their finances on an ongoing basis. But as the market evolves there could be stronger interest in using transaction details that are less directly tied to core financial metrics to predict credit risk. For example, cash-flow data reveals substantial information about the businesses and locations that customers patronize and the individual expenditures that they make. In this respect it is as at least as sensitive as traditional consumer report information, which tends to focus on a limited number of trade lines.[187]

> A checking account … [m]ay well record a citizen's activities, opinions, and beliefs as fully as transcripts of his telephone conversations …. In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum.
>
> California Bankers Association v. Shultz, 416 U.S. 21, 85, 90 (1974) (Douglas, J., dissenting).

A 2008 Federal Trade Commission case against credit card issuer CompuCredit provides a helpful illustration of issues that could arise. That company used a "behavioral" scoring model to reduce consumers' credit lines if they used their cards for certain types of transactions, including cash advances, marital or personal counseling, tire retreading and car repairs, pawn shops, direct marketing merchants, and certain types of entertainment (bars, nightclubs, pool/billiards, and massage parlors).[188] While the case focused on concerns about misleading marketing, the list of transaction types raises broader questions about what information is appropriate for lenders to use in underwriting decisions and what consumers and small businesses need to make informed decisions in applying for credit and using their accounts over time.

These issues are already present in the credit card market, where several large lenders apparently pulled back from relying using behavioral models based on transactional details to make decisions about reducing credit lines and other account terms after substantial controversy in the

187 Indeed, some stakeholders argue that cash-flow data is actually more sensitive. For example, although consumer advocates generally support applying Fair Credit Reporting Act protections to cash-flow data that is used in credit underwriting, they have argued that it should never be used for employment, insurance, housing, government licensing, or other purposes that are generally defined as "permissible" under FCRA and that it should not be used in credit contexts in ways that consumers do not expect or understand, regardless of consent. Lauren Saunders, National Consumer Law Center, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology at 12-13 (Nov. 21, 2019). For more discussion of consent and scope of usage limitations, see Section 6.2.

188 See Federal Trade Commission, Complaint for Permanent Injunction and Other Equitable Relief, FTC v. CompuCredit Corp., No. 1:08-cv-1976-BBM-RGV (N.D. Ga. June 10, 2008); Federal Trade Commission, Big Data at 22. The case materials do not address whether consideration of marital or personal counselling might have violated the FCRA provisions concerning medical data or whether any disparate impact analysis was performed, but news reports about the case were one of the reasons that Congress directed the Federal Reserve Board to conduct a study on behavioral scoring models. See n.187.

late 2000s, though such models are used today at least for marketing purposes.[189] The use of cash-flow data in credit underwriting potentially expands the universe of lenders who have access to detailed transactional information during the initial underwriting process.

Existing laws: Existing laws bar the use of certain data in credit underwriting due to privacy and/or fairness concerns. For example, the Equal Credit Opportunity Act and Fair Housing Act generally prohibit the use of race, sex, the receipt of public assistance, and other protected characteristics in underwriting models.[190] The Fair Credit Reporting Act also generally prohibits lenders from obtaining or using medical information in credit decisions.[191] Other state and federal laws prohibit the provision of certain types of information to or by consumer reporting agencies, although they do not prohibit lenders from using such information if it is derived from other sources.[192]

In addition, the disparate impact doctrine under fair lending laws restricts use of underwriting criteria or other practices that have a disproportionately adverse effect on racial minorities and other protected classes, unless they meet a legitimate business need that cannot reasonably be achieved by less impactful means.[193] In practice, this requires a careful analysis of each individual firm's credit approval and pricing algorithms to assess the extent to which particular variables are proxies for race or other protected class status, the variables' respective contributions to the accuracy of default predictions, and whether alternative variables achieve similar levels of predictiveness while producing less negative impacts on protected classes.[194]

More broadly, federal law also prohibits unfair, deceptive, and abusive acts and practices in connection with the provision of consumer financial products and services.[195] However, while federal agencies have pursued some deception and unfairness cases involving data practices as discussed further in Section 6.1.1.3, we are unaware of any cases in which such prohibitions have been applied to use of particular underwriting criteria other than deception allegations similar to those raised in

189 *See, e.g.,* Barry Paperno, Q&A: How Cardholder Behavior Can Impact Your Credit, creditcards.com (Nov. 9, 2017) (describing behavioral models based on transactional data as "widely" used). A 2010 Federal Reserve Board study that included a survey of 98 percent of the market found that credit card issuers rely heavily on transaction and geographic information in fraud detection and prevention systems, but that only a handful were using the data to make negative decisions about existing credit lines. Several of those lenders appeared to have stopped using the data for underwriting decisions by the time the survey was conducted perhaps in response to public debate over the practice, although some stakeholders questioned that finding in light of ambiguities in the question wording. Criteria considered included use of cards to obtain cash advances, excessive gambling activity, and spending as divided into general expense categories and/or within broad geographic units. One lender considered the performance and spending patterns of other cardholders with similar credit-related characteristics who shopped at the same merchants where the given cardholder had made purchases. Board of Governors of the Federal Reserve System, Report to the Congress on Reductions of Consumer Credit Limits Based on Certain Information as to Experience or Transactions of the Consumer 2-3, 13-19 (2010) (hereinafter FRB, Transactional Data Report); Joshua M. Frank, Analysis of Federal Reserve Research on Behavioral Scoring, Center for Responsible Lending Research Comment (2010); *see also* Mikella Hurley & Julius Adebayo, Credit Scoring in the Era of Big Data, 18 Yale J.L. & Tech. 148, 150-51 (2016); Cullerton at 813, 819. Disclosure requirements concerning behavioral scores that are based on the lender's own data rather than outside sources are less robust than for scores based on third-party data. Paperno; Section 6.1.1.2.

190 15 U.S.C. § 1691(a); 42 U.S.C. § 3605; 12 C.F.R. § 1002.6(a), (b); 24 C.F.R. § 100.120. ECOA does permit age and the receipt of public income to be considered under very limited circumstances. 12 C.F.R. § 1002.6(b)(2).

191 15 U.S.C. §§ 1681a(d)(3), (i), 1681b(g), 1681c(a)(6); 12 C.F.R §§ 1022.30-.32.

192 For example, FCRA prohibits consumer reporting agencies from providing certain adverse payments information after seven years and bankruptcy information after ten years for use in evaluating loans that do not exceed certain size thresholds, but it does not restrict lenders from relying on such information if it is obtained through other means. 15 U.S.C. § 1681c. As discussed in Section 2, a few state laws also prohibit the furnishing of certain utility payments information to consumer reporting agencies. See supra n.32.

193 12 C.F.R. § 1002.6(a); *id.* Supp. I, cmt. 6(a)-2; 59 Fed. Reg. 18267 (Apr. 15, 2014); OCC, Bulletin 97-24, app. at 11. *See also* Boxes 2.2.1, 3.2.1.

194 See Boxes 3.2.1 and 3.2.2.

195 12 U.S.C. § 5531; 15 U.S.C. § 45.

BOX 6.1.1.1.1 UDAAP DEFINITIONS

Federal law has prohibited unfair and deceptive acts and practices since 1938 under the Federal Trade Commission Act, which has been applied to both consumers and small business owners and in both financial and non-financial settings.

Deceptive acts have generally been defined to include material representations, omissions, or practices that mislead or are likely to mislead a consumer that is acting reasonably under the circumstances.

Unfairness is generally defined under federal law to include activities that (1) cause or are likely to cause substantial injury (usually monetary) to consumers; (2) cannot be reasonably avoided by consumers; and (3) are not outweighed by countervailing benefits to consumers or to competition. Unfairness enforcement cases have generally focused on situations where firms unreasonably create or take advantage of an obstacle to the free exercise of consumer decisionmaking.

In 2010, the Dodd-Frank Act also addressed abusiveness in the context of consumer financial products and services. The statute generally defines abusiveness to include activities that either (1) materially interfere with the ability of consumers to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of consumers' lack of understanding about a consumer financial product or service, inability to protect their interests in selecting or using the product, or reasonable reliance on the covered person to act in the interests of the consumer.

Sources: 12 U.S.C. § 5531; 15 U.S.C. § 45; Federal Trade Commission, FTC Policy Statement on Deception (Oct. 14, 1983); Consumer Financial Protection Bureau, Statement of Policy Regarding Prohibition on Abusive Acts or Practices (Jan. 24, 2020); Federal Trade Commission, Policy Statement on Unfairness (Dec. 17, 1980); Evans at 3.

the CompuCredit case. Given the required elements, application of these authorities tends to be very fact-specific.[196]

Stakeholder debates: Stakeholders vary widely as to their level of concern about the fact that transaction-level details are being shared (if not widely used) today, about the risk that evolution in cash-flow underwriting over time will substantially increase privacy and fairness risks over current levels, and about their preferred methods of risk reduction.

For some, the priority is preserving as much latitude as possible for lenders and model developers to find new ways of improving default risk prediction, since improved predictiveness is generally beneficial to both firms and borrowers by reducing the risk that applicants are approved for loans that they cannot in fact repay. Given that existing laws already prohibit use of the categories described above and that research on consumer attitudes about privacy is quite mixed as discussed further in Section 6.2, such stakeholders argue that applicants and firms can manage any remaining concerns through individual choices in the market, for instance where applicants choose lenders who do not use cash-flow data (or use it in particular ways) if they are concerned about such practices. These stakeholders may support improving disclosures to ensure informed consent as discussed further below, but many of them argue that prescriptive restrictions either through industry standards or by policymakers would be premature absent concrete problematic practices manifesting in the market.

Other stakeholders express concern that the potential adoption of models that rely on transaction details could violate existing laws, conflict with customers' general privacy expectations, or otherwise worsen the challenges facing already financially vulnerable applicants based on factors

196 *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d. 236 (3d Cir. 2015) (upholding the FTC's authority to bring unfairness cases based on data security practices). For a general discussion of unfairness considerations in the context of fintech and underwriting, see Evans at 3-9. Although they do not directly prohibit the use of particular underwriting criteria, our conversations with stakeholders suggest that transparency-related considerations may play a role in lenders' decisions to use particular variables. In addition to concerns that there might be conflicts or omissions in marketing materials similar to the CompuCredit case, for example, as discussed in Section 6.1.1.2, lenders are required to disclose their principal reasons for taking "adverse actions" on credit applications. Some stakeholders have indicated that they would be less likely to adopt criteria that might present reputational risk because they are not understandable to borrowers or might seem unfair or unreasonable even if they are legally permissible.

BOX 6.1.1.1.2 FUTURE OF THE DISPARATE IMPACT DOCTRINE

As discussed in Boxes 2.2.1 and 3.2.1, lending discrimination cases are brought on two bases: Disparate treatment cases focus on decisions made on the basis of protected characteristics, while disparate impact cases focus on situations in which a facially neutral practice has a disproportionately negative effect on members of a protected class, unless the practice meets a legitimate business need that cannot reasonably be achieved by less impactful means

Use of automated underwriting models is generally recognized as reducing disparate treatment risk because the models reduce subjectivity and are generally prohibited from using race or other protected characteristics as variables. However, many stakeholders view the disparate impact doctrine as increasingly important in helping to detect situations in which facially neutral data and algorithms are unrepresentative, reflect historical bias, or contain other flaws that systematically disadvantage racial and ethnic minorities, women, or other groups. Some sources argue that similar fairness analyses should be applied in other, non-financial fields in which automated decisionmaking is becoming more common, though some stakeholders in financial services argue that the disparate impact doctrine creates substantial uncertainty and burden in part because there are not clear thresholds and definitions for such concepts as "legitimate business need."

The Supreme Court confirmed in 2015 that the disparate impact doctrine is enforceable under the Fair Housing Act, but it has not yet ruled on the Equal Credit Opportunity Act. Federal regulations, agency guidance, and lower court decisions have recognized the disparate impact doctrine under both laws for several decades, but both the Department of Housing and Urban Development and the Consumer Financial Protection Bureau have announced plans to reexamine the doctrine in light of the Supreme Court's decision.

In 2019, HUD proposed a rule that would create safe harbors for the use of automated underwriting models if a lender shows that they were the responsibility of a "recognized" third party rather than the lender, or if they were validated by a neutral third party as not using inputs that are substitutes for protected characteristics and as empirically derived, statistically sound, and predictive of credit risk. The proposal would also increase the showing required at the first stage of a case for plaintiffs to be able to pursue claims that a particular practice has a disproportionate effect on a protected class.

The Consumer Financial Protection Bureau announced in 2018 that it was reexamining ECOA requirements in light of the Supreme Court decision and other developments, and in 2019 that it intended to hold a symposium on the topic at a future date.

The Government Accountability Office reported that many fintech lenders that it interviewed in 2018 had performed fair lending testing or analyses in conjunction with developing new underwriting models, but did not provide details on the nature or scope of their analyses. As discussed in Section 4.1.2, the Consumer Financial Protection Bureau has not yet taken the administrative steps necessary to begin regularly examining "larger participants" in markets for general personal loans for compliance with fair lending and other federal financial laws.

Sources: 12 C.F.R. § 1002.6(a); *id.* Supp. I, cmt. 6(a)-2; 59 Fed. Reg. 18267 (Apr. 15, 2014); *Texas Dep't of Housing & Community Affairs v. Inclusive Communities Project, Inc.*, 135 S. Ct. 2507 (2015); 84 Fed. Reg. at 42859-60; Consumer Financial Protection Bureau, Press Release, Consumer Financial Protection Bureau Announces Symposia Series (April 18, 2019); Consumer Financial Protection Bureau, Statement on Enactment of S.J. Res. 57; Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev. 1085, 1100-05 (2018); Mark MacCarthy, Fairness in Algorithmic Decision-Making, Brookings Institute (Dec. 6, 2019); GAO, Alternative Data Report at 35.

that are not entirely within their control.[197] Such stakeholders point out that certain federal agencies have announced plans to reexamine the disparate impact doctrine and that non-bank lenders and model developers are not currently subject to equal levels of supervision for their compliance with existing laws as discussed further in Section 7. And as discussed in Section 6.2 with regard to improving consumer consent, they advocate for giving customers optionality about the level of detail they can share with lenders, for instance by choosing whether to include merchant identities. But more broadly some also question whether it is fair or practical to expect credit applicants to

197 Even if such impacts do not raise fair lending concerns or constitute an unfair practice as that term has been defined by federal law, stakeholders argue that they can raise broader policy concerns about negative impacts on low-income populations. To take an illustration from the CompuCredit case, for instance, charging higher prices or denying credit to applicants based on the fact that they have had to pay for previous car repairs could become a self-fulfilling prophecy to the extent that the applicant cannot travel to work or operate their businesses, or must pay such high prices that they are more likely to default.

manage all of the risks for themselves, particularly as the use of cash-flow data becomes more pervasive both for credit purposes and various other use cases.

Mitigation options: With regard to compliance with existing legal requirements, increasing supervision of non-bank lenders and model developers could be a helpful step as discussed further in Section 7.2. The practical challenges and broader debates over the likely impact of strengthening disclosures and authorization processes are discussed further in Section 6.2.

Beyond these items, additional research and analysis as to what specific cash-flow variables are most useful for predicting default risk would help to inform policy judgments about how best to manage potential privacy and fairness concerns in its potential use. It is difficult to begin to define the minimum data elements that are needed for cash-flow based underwriting because the market is still in the process of evaluating different variables, models, and approaches. And even when there is greater consensus around useful attributes, the credit use case presents challenging questions about how to balance the quest for innovation in improving model predictiveness for diverse populations with protecting consumer privacy, fairness, and transparency interests.

As industry members and policymakers develop a better understanding of the usefulness of particular data, there are a number of potential tools that could be used to manage privacy and fairness concerns. One way is to focus on voluntary or prescriptive restrictions at the lender level to prevent particularly sensitive information from being used particular ways. In the credit card context in the 2000s, for example, some lenders used merchant category codes or other similar rolled-up data rather than individual transaction details to assess expense patterns in their underwriting analyses.[198] Another mitigation method is to use voluntary or prescriptive methods to filter the initial flow of data to ensure that particularly sensitive features are not available to lenders in the first instance. Transmissions of distillations of cash-flow information in the form of credit scores and/or attributes rather than raw details is one way to move in this direction. Provisions to restrict the transmission and use of medical data under FCRA and its implementing regulations take both approaches by both requiring consumer reporting agencies to perform certain filtering activities and imposing direct lender restrictions.[199]

Implementing these measures also requires careful attention to which parties decide that particular data should be restricted and effectuate the data limitations, which raises many of the same issues discussed in Section 5.2.2.1. If decisions about data scope are determined by individual market actors, there is a concern that either banks or end users might be influenced by business considerations in purporting to balance borrowers' interests in privacy and fairness. There are also potential accuracy, privacy/security, and regulatory issues raised by whether filtering functions are performed by banks, aggregators, other vendors, or lenders themselves.[200]

198 FRB, Transactional Data Report at 19.

199 FCRA contains multiple restrictions on the use and sharing of medical information. First, the statute provides a regime by which consumer reporting agencies are required to scrub certain details out of listings concerning medical debts to the extent that the medical provider has identified itself to the CRA so that lenders have less information about the nature of the underlying service. 15 U.S.C. §§ 1681b(g)(1), 1681c(a)(6). Second, the statute generally prohibits creditors from obtaining or using medical information that has not been scrubbed by a consumer reporting agency as described above. Recognizing that information relating to medical expenses may be volunteered by applicants or mixed into other data sources, the Federal Trade Commission issued rules that allow lenders to use unsolicited information relating to medical expenses so long as the lender does not take the consumer's heath, condition, history, or other details into account in the credit process, the information is used in ways that are no less favorable than comparable non-medical information, and certain other conditions are met. 15 U.S.C. § 1681(g)(2); 12 C.F.R. § 1022.30.

200 Banks are most familiar with their own data and could minimize information flows overall, though such an approach would impose costs. Aggregators acting on behalf of lenders are the other alternative, though they are somewhat less familiar with the data and there is some privacy/security risk to the extent that the aggregators receive fulsome information even if end users do not. Performing such activities could also potentially affect the question of whether aggregators qualify as consumer reporting agencies under the FCRA, which may make some firms reluctant to take on the responsibility. See Box 6.1.1.2.1.

Thus, although more research is needed to inform policy analyses, these considerations demonstrate why determining whether and how to restrict use could prove to be one of the most challenging policy questions posed by cash-flow underwriting. Self governance options to define the scope of data to be transferred could provide a more consistent baseline, but it is unclear whether those initiatives will be able to overcome competition and coordination challenges and weigh consumer and small business interests as discussed in Section 5.2.2. The scope of federal agencies' authorities to act on privacy and fairness concerns may also depend on the particular facts and circumstances.[201] The possibility of data legislation is discussed in greater depth in Section 7.3.

6.1.1.2 Accuracy concerns

Accuracy of underwriting data is a potential concern for applicants and lenders alike, since data errors and omissions can lead to mistakes in both eligibility and pricing decisions. Stakeholders generally agree that cash-flow data as it is maintained by banks and prepaid issuers tends to have fewer accuracy problems that traditional credit reports, though comparative statistics are difficult to obtain.[202] And where the data must be transferred between companies, errors can be introduced in the collection and processing of the information, particularly where screen scraping is involved.[203]

Congress has judged accuracy in credit underwriting to be enough of a systemic and consumer protection concern in the traditional credit reporting system to impose substantial protections via the Fair Credit Reporting Act. However, application of the FCRA to cash-flow underwriting is fiercely disputed by stakeholders. And laws that apply generally to transaction account records are not specifically built to address situations in which the records are later used for other purposes.

In the absence of regulatory clarity, at least one aggregator has adopted back-end investigation procedures similar to those used by traditional consumer reporting agencies, while at least one other has developed a front-end portal by which customers can review data for accuracy before it is transmitted to lenders in the first instance. But many consumers and small businesses do not have formal tools with which to seek corrections in the current market.

Existing laws: FCRA accuracy protections are designed primarily to govern three-way data flows involving "consumer reports"[204] that are compiled by intermediaries called "consumer reporting

201 For instance, both the application of the disparate treatment doctrine and application of authorities to prevent unfair, deceptive, and abusive acts and practices tends to depend on detailed factual analyses of particular models or other business conduct.

202 Accuracy rates are likely higher because the data reflects the ongoing clearing of individual transactions by financial institutions and is relatively likely to come to the consumer's attention through periodic statements, financial apps, or bank websites and automated teller machines. Consumer reporting agencies play a different and less active role in compiling data from other sources for their credit files, and consumers must generally seek out access to their information. A 2012 study found that one in five consumer reports contained errors; accuracy rates may have increased since then but current statistics are not available. See Box 2.1.1.

203 See Section 4.2.2. Because the consumer or small business is affirmatively consenting to and facilitating data access through the provision of login credentials or other means, there is likely less risk that an aggregator would pull or merge data for someone other than the applicant than in a traditional consumer report. See Box 2.1.1. However, in addition to screen scraping problems, there could be challenges in properly structuring and categorizing information. In the personal financial management market, for instance, sources suggest that as much as 10 to 20 percent of transactions cannot be categorized by general type or are mis-categorized due to ambiguities and inconsistencies in merchant names and other data. *See, e.g.,* GDS Link, The Evolution of Bank Transaction Data 5 (2019); Baker Shogry, Blog, Making Sense of Messy Bank Data, Plaid (updated Nov. 21, 2018); Pramod Singh, Blog, Enriched Data for Better Banking Decisions, Envestnet/Yodlee (Oct. 5, 2018).

204 15 U.S.C. § 1681a(d). A consumer report is generally defined as the communication of information by a consumer reporting agency bearing on a consumer's credit worthiness, capacity, character, general reputation, personal characteristics, or mode of living which is collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for personal credit, insurance, employment, or various other purposes identified by the FCRA. *Id.* The definition is interrelated with the definition of consumer reporting agency since each term refers to the other. See n.203.

agencies" as defined by the statute.[205] For example, CRAs must adopt "reasonable procedures to assure maximum possible accuracy," both in structuring their own operations and in monitoring data obtained from external sources.[206] Firms that furnish data to CRAs are also required to implement front-end processes to promote accuracy,[207] and both furnishers and CRAs are required to investigate and resolve consumer disputes about the accuracy of specific information.[208] To facilitate corrections, consumers are entitled to access their credit reports in various circumstances and to receive disclosures where lenders rely on external data in taking an "adverse action" on an application or account.[209]

Where a lender takes adverse action based on information from a party that is not a consumer reporting agencies (such as application references), FCRA still requires an adverse action notice but the content is less detailed and there is no right to data access. [210] FCRA also does not impose accuracy or investigation requirements on the original data source in such cases, or on lenders who rely on "transaction or experience information" from their own prior dealings with an applicant.[211] The Equal Credit Opportunity Act separately requires lenders to provide adverse action notices concerning the principal reason(s) for the action to both consumers and small businesses, but it is not specifically focused on error correction.[212]

With regard to data as it is held at banks and prepaid issuers, the Electronic Fund Transfer Act requires such financial institutions to investigate various types of errors so long as consumers report them within 60 days after transmission of the first periodic statement reflecting the alleged mistake.[213] The law and regulations do not explicitly address financial institutions' duty to correct records after that date, though they may have to do so as a practical matter to comply with EFTA provisions that limit consumers' liability with regard to unauthorized electronic fund transfers.[214]

Stakeholder debates: We are not aware of any stakeholders that are actively pressing to treat banks and prepaid issuers as furnishers under the Fair Credit Reporting Act where cash-flow data is collected by an aggregator for use in credit underwriting. As a number of sources have noted, furnishing is a voluntary activity under the statute that entails accepting a number of compliance obligations. Subjecting banks and prepaid issuers to those requirements when they facilitate one-off transfers of account data at the request of individual customers could create a substantial chill on

205 15 U.S.C. § 1681a(f). A consumer reporting agency is generally defined as an entity that regularly engages in assembling or evaluating information on consumers for the purpose of furnishing consumer reports to third parties. *Id.*

206 *Id.* § 1681e(b).

207 *Id.* § 1681s-2(e); 12 C.F.R. §§ 1022.40-42.

208 15 U.S.C. §§ 1861e, 1861i, 1861s-2(a)(3), (8), (b); 12 C.F.R. § 1022.43.

209 15 U.S.C. §§ 1861g, 1861h, 1861m(a); 12 C.F.R. §§ 1022.70-.75, 1022.130, 1022.136-38.

210 15 U.S.C. § 1681m(b).

211 *Id.* § 1681a(d)(2).

212 12 U.S.C. § 1691(d); 12 C.F.R. § 1002.9. As discussed in note 39, ECOA's Shoebox Rule permits applicants to provide supplemental credit history data in certain circumstances, but does not specify any processes for how the information should be treated. The provision has been little used in practice. 12 C.F.R. § 1002.6(b)(6); *id.* supp. I cmt. 6(b)(6)-1.

213 15 U.S.C. § 1693f; 12 C.F.R. §§ 1005.11, 1005.18(e). Errors are defined to include such items as unauthorized electronic fund transfers (EFTs), incorrect EFTs to or from the consumer's account, the omission of an EFT from a periodic statement, and computational and bookkeeping errors made by the financial institution relating to an EFT. 12 C.F.R. § 1005.11(a).

214 15 U.S.C. § 1693g; 12 C.F.R. §§ 1005.6, 1005.18(e). Unauthorized electronic fund transfers are generally defined to mean transfers from a consumer's account initiated by another person without actual authority and from which the consumer receives no benefit, though in situations in which the consumer provides their access device to another party, the financial institution may treat the transfers as valid until and unless the consumer notifies it that transfers by the person are no longer authorized. 12 C.F.R. § 1005.2(m).

BOX 6.1.1.2.1 FCRA COVERAGE DEBATES

Most FCRA protections apply to "consumer reports" from "consumer reporting agencies." Consumer reports are defined broadly to include communications "of any information by a consumer reporting agency bearing on a consumer's credit worthiness, ... character, general reputation, personal characteristics, or mode of living which is ... collected in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility" for credit, insurance, employment, or other authorized purposes under the statute.

Consumer reporting agencies are defined in turn as organizations that "regularly engage[] in whole or in part in the practices of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."

Informal guidance by staff from the Federal Trade Commission has distinguished entities that perform only mechanical tasks in connection with transmitting consumer information from those that are performing more sophisticated assembly and evaluation activities. For example, the guidance suggests that companies that transmit records without knowing their content or retaining any information are not consumer reporting agencies. Other strands of guidance suggests that mortgage brokers and companies that act as intermediaries or agents on behalf of consumers who have initiated a transaction do not become consumer reporting agencies because they forward information to lenders at the consumer's direction, and that agents and employees of a firm do not become consumer reporting agencies when sharing information that is a consumer report with their principal/employer in connection with the purpose for which the reports were obtained.

Some stakeholders invoke this guidance to argue that aggregators are not subject to the FCRA, in addition to making policy arguments that FCRA requirements are inapposite because of the consumer permissioning process and unduly burdensome given the nature of the data and transmission processes. In contrast, one aggregator specifically states that it complies with FCRA requirements for consumer reporting agencies when performing credit-related activities.

Some stakeholders have argued that data aggregators are covered by the FCRA, noting that the definitions of consumer report and consumer reporting agency are both quite broad and do not refer to either the absence or presence of consumer permission as affecting the scope of coverage. They have also noted that if the FCRA does not apply, state laws that have been preempted in the traditional credit reporting system may be applicable to the new ecosystem.

Sources: 15 U.S.C. § 1681a(f); 15 U.S.C. § 1681a(d)(1); 12 C.F.R. §1022.41(c); FTC, Staff FCRA Summary at § 603(f)-3.B, 4.E, 4.H (2011); Finicity, Consumer Reporting Agency; National Consumer Law Center, Data Gatherers Evading the FCRA May Find Themselves Still in Hot Water (2019).

BOX 6.1.1.2.2 OTHER FCRA RIGHTS AND REQUIREMENTS

Apart from the accuracy related provisions, the FCRA imposes other requirements on both consumer reporting agencies and users of consumer reports, as well as providing consumers with various rights. For example:

Consumer reporting agencies: CRAs are subject to the most extensive FCRA requirements because they function as the hub in the broader consumer reporting system. For example, they must follow certain restrictions with regard to reporting certain types of adverse information, medical-related data, and information in situations involving identity theft and credit freezes. They also must perform due diligence and take other steps to ensure that users of consumer reports use the information only for permissible purposes under the statute. Finally, they must provide various disclosures and information to all of the other actors in the broader reporting system.

Consumer report users: Users must certify the permissible purpose for which they are obtaining a consumer report and that it will be used for no other purposes. They must provide certain disclosures to consumers after taking an adverse action on a credit application or account, or after extending credit on terms that are materially less favorable than those available to a substantial proportion of customers. Financial institutions and creditors are also subject to certain additional requirements in connection with "red flags" that may indicate identity theft has occurred.

Consumers: Consumers do not have a general right to control furnishing and reporting of their information under FCRA, but they do have a right to various disclosures, to permit companies to obtain their credit reports in circumstances that would not otherwise be permissible under the statute, and to restrict data flows in certain employment and credit freeze situations. Consumers also have the right to obtain copies of their reports and to dispute the accuracy and completeness of particular information.

Sources: 15 U.S.C. §§ 1681-1681x; 12 C.F.R. pt. 1022.

the broader data transfer system.[215] Thus, particularly given outstanding questions on error rates and the fact that consumers have some ability to pursue corrections under EFTA and general customer service channels, stakeholders generally do not appear to view engineering accuracy protections for cash-flow data as it sits with banks and prepaid issuers as a high priority.[216]

However, application of FCRA to aggregators and lenders is more hotly contested in cases where cash-flow data is transferred between companies for credit underwriting purposes.[217] These debates hinge in part on how much significance different stakeholders attribute to the fact that customers must generally provide affirmative consent for their cash-flow data to be transferred to lenders for use in the underwriting process,[218] as well as disagreements over whether aggregators meet the definition of consumer reporting agencies.

In the accuracy context specifically, stakeholders also debate the potential burdens of and necessity for FCRA protections. For example, some stakeholders argue that aggregators already have sufficient business incentives to ensure that they do not introduce errors into information that they receive from banks or other financial institutions,[219] and assert that additional requirements would add unwarranted costs and complications. For example, there is a question whether some aggregators might be forced to collect more personally identifiable information about consumers than they do today in order to verify identities for purposes of managing any accuracy disputes. Some stakeholders also argue that providing applicants with an opportunity to review data that is collected by aggregators before it is transmitted to lenders or other end users would provide a better mechanism for identifying any issues than waiting for FCRA dispute resolution procedures to kick in after lenders take an adverse action.

Yet while the opportunity to resolve errors prior to an initial credit decision could have advantages for all participants in the credit process, other stakeholders argue there is still a need for formal dispute resolution requirements. For example, they note that general business incentives to maintain accuracy have not been sufficient to avoid responsiveness concerns with other business-to-business

215 *See, e.g.,* Kwamina Thomas Williford & Brian J. Goodrich, Why Data Sources Aren't Furnishers under Credit Report Regs, hklaw.com (Sept. 25, 2019). In addition to the policy arguments against applying FCRA furnishing requirements, stakeholders point to the fact that implementing regulations specifically state that consumers themselves are not furnishers when they provide information to a consumer reporting agency. They also note that there are other circumstances involving public records and employment and education verifications where data sources are not treated as furnishers, even though the intermediaries that collect information from them are treated as consumer reporting agencies. 12 C.F.R. § 1022.41(c)(3); Federal Trade Commission, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations 8-10 (2011) (hereinafter FTC, Staff FCRA Summary).

216 To the extent that errors in cash-flow data as it sits with banks and prepaid issuers are later deemed to be a problem in the underwriting context, EFTA likely would not provide a clean mechanism for ensuring corrections as it is currently structured. As noted above, the statute and regulation do not expressly provide error resolution rights in situations in which the errors are not reported within 60 days of the initial statement. The regulatory regime is also primarily focused on making consumers whole financially rather than correcting records for their own sake. For instance, there is no provision for flagging disputed items while an investigation is underway because the law does not assume that the underlying records would be used for other purposes.

217 Stakeholders do not appear to be pressing to apply FCRA protections to situations in which cash-flow data is transferred for other use cases involving payment products or personal financial management services. Though the statute contains language that encompasses situations in which the user of a consumer report has "a legitimate business need for the information … in connection with a transaction that is initiated by a consumer," the law is primarily focused on situations involving use of the information for eligibility determinations for such items as consumer credit, insurance, employment, government licenses and benefits, and other types of accounts. 15 U.S.C. § 1681b(a)(3)(F).

218 *Id.* § 1861b(b)(2)(A) (allowing consumer reports to be accessed for most permissible purposes without consumer permission, other than certain employment related uses); Box 2.1.1. As discussed in Section 6.1, some stakeholders view the need for affirmative consent to access cash-flow data as an opportunity to empower consumers and small businesses to take greater control over their financial lives and as a potential substitute for traditional prescriptive protections. Others argue traditional safeguards are more needed than ever as data sharing increases exponentially.

219 Such stakeholders argue that aggregators are not similarly situated to traditional consumer reporting agencies, which generally have ongoing contractual and operational relationships with their furnishers because those companies are also generally purchasers of the CRAs' credit reports. Particularly where data is gathered via screen scraping, the aggregator may have no relationship with the furnisher and thus little insight or leverage in attempting to detect or investigate accuracy issues in the original data, rather than reviewing their own technical processes. See Section 4.2.2.

vendors that do not have direct customer relationships with consumers.[220] They also point out that the FCRA imposes accuracy requirements on consumer reporting agencies even in situations in which the data source is not treated as a furnisher, such as in situations involving use of public records.

Mitigation options: Additional research into the frequency, nature, and source of data inaccuracies in the context of cash-flow underwriting would be helpful in evaluating and prioritizing particular mitigation options.

Our engagement with stakeholders to date suggests that transitioning the broader system from screen scraping to APIs could materially affect risk levels in cash-flow underwriting and the assessment of further mitigation options. However, the success of industry initiatives to accelerate and standardize this process remains to be seen in light of the scale and competition issues discussed in Section 5.2.2, we understand that credit use cases may not currently be prioritized for API transmission even where such mechanisms have been implemented.[221]

Lenders could also address potential concerns about accuracy by choosing aggregators that can offer applicants an opportunity to review their data and/or that follow FCRA requirements for consumer reporting agencies when transmitting cash-flow information for credit-related purposes.[222] Section 1033 could potentially also become a mechanism for consumers to request access to their data from an aggregator or lender in order to review it for accuracy, although the statute does not expressly address correction rights or general accuracy procedures.[223]

Yet even if these other methods of managing accuracy risks are adopted, resolving the outstanding legal questions with regard to application of the FCRA to cash-flow data in credit underwriting is important to providing greater certainty to firms and borrowers in structuring their own decisions going forward.[224] To the extent that some stakeholders argue that FCRA accuracy requirements are unduly burdensome for consumer-permissioned data flows, such concerns could be potentially be mitigated by providing tailored regulatory standards and guidance or by a decision to interpret the statute not to apply to particular parties in the first instance. For example, to the extent that aggregators might be subjected to FCRA requirements for consumer reporting agencies, federal regulators could establish specific standards for what constitutes "reasonable procedures" for assuring accuracy in particular contexts, given the differences between screen scraping and APIs. FCRA provides the Consumer Financial Protection Bureau with relatively broad authority to prescribe such regulations "as may be necessary or appropriate to administer and carry out the purposes and objectives of this subchapter, and to prevent evasions thereof or to facilitate compliance therewith."[225] However, some industry stakeholders warn that in the absence of specific standards, application of existing FCRA

220 Aggregators that are building their brands as consumer-centric start-ups do appear to have strong business incentives to avoid introducing errors to the information they transmit, and some appear to be working affirmatively to build reputations and relationships directly with consumers. Their ability to develop systems for the explicit purpose of data transmission, rather than crafting transmission capabilities onto a patchwork of systems of different vintages and built for different purposes, undoubtedly also serves broader accuracy interests. At the same time, critics note that loan applicants do not generally direct revenue to aggregators or get to choose another intermediary if there are problems. This kind of three-party structure has led to consumer responsiveness concerns in a variety of other contexts, such as loan servicing and traditional consumer reporting. *See, e.g.,* 78 Fed. Reg. 67848, 67849 (Nov. 12, 2013); 78 Fed. Reg. 10696, 10699-10701, 10843-10844 (Feb. 14, 2013); U.S. House of Representatives Committee on Financial Services, Hearing, Credit Reports: Consumers' Ability to Dispute and Change Inaccurate Information 210 (June 19, 2007) (testimony of ChiChi Wu, National Consumer Law Center).

221 See Sections 4.2.2, 4.2.3, and 4.2.4.

222 For example, initiatives by traditional consumer reporting and scoring incumbents to incorporate cash-flow data are providing lenders with "reason codes" for purposes of adverse action notices and mechanisms for consumers to file disputes about accuracy concerns.

223 12 U.S.C. § 5533; Box 4.2.1.

224 There appears to be no dispute among stakeholders that ECOA's adverse action disclosure and Shoebox Rule requirements apply to both consumers and small businesses where lenders use cash-flow data in their underwriting processes. Adverse action disclosure requirements are somewhat more flexible as applied to commercial applicants, for instance by allowing oral notices in certain circumstances. 12 C.F.R. § 1002.9(a)(3).

225 15 U.S.C. § 1681s(e)(1).

BOX 6.1.1.2.3 ADVERSE ACTION ISSUES

ECOA's adverse action notice provisions generally require lenders to disclose the specific and principal reason(s) for rejecting an application to both consumers and small businesses. Where lenders relied on information from a "consumer report" in taking an adverse action or engaging in risk-based pricing for consumer credit, FCRA requires additional disclosures including the key factors that adversely affected any third-party credit score used in the decision. However, where information comes from other sources, FCRA notices are not as detailed, which may make them less useful to applicants in detecting underlying data errors. ECOA regulations provide model language that can be used to satisfy the disclosure requirements under both statutes; they also provide sample reasons that can be used to satisfy the ECOA disclosure requirements, but do not list sample key factors for FCRA purposes.

The December 2019 interagency statement on alternative data expresses confidence that the use of cash-flow information "can generally be explained and disclosed to the borrower" as may be required under ECOA and FCRA, but federal regulators have not issued any specific interpretive or compliance guidance. For example, it is unclear whether information collected by a data aggregator constitutes a "consumer report," which would trigger FCRA requirements for lenders to provide the more detailed FCRA adverse action notices. Information from a bank's own account records would not trigger FCRA adverse action requirements at all.

The Consumer Financial Protection Bureau also has not updated the list of sample reason codes under ECOA to include items specific to cash-flow underwriting. However, UltraFICO is expected to provide lenders with key factors that adversely affect individual applicants' scores based on both cash-flow and traditional credit data.

Another question concerns the content of disclosures by lenders that use traditional credit data to make an initial assessment and only consider cash-flow or other alternative data for applicants that would otherwise be rejected. We understand that some lenders may be focusing their notices on the first-stage determinations based on traditional credit data, rather than the use of cash-flow data in the second stage. Such an approach is less likely to alert applicants of any accuracy issues in connection with their cash-flow data and/or to educate them about changes in how they manage their transaction accounts that could boost their chances in later applications.

Beyond these specific interpretive issues, there are broader debates about the utility of adverse action notice requirements as they are currently structured. Implementing regulations and guidance under ECOA generally discourage provision of more than four principal reasons for an adverse action, and provide lenders with some latitude in determining which factors to highlight in the context of complex multivariate underwriting models. They also do not require lenders to explain how or why a particular variable adversely affected the applicant. Accordingly, some stakeholders have suggested that additional guidance or disclosure testing under the Consumer Financial Protection Bureau's trial disclosure program could make the notices more useful to applicants.

Sources: 12 U.S.C. § 1691(d); 12 C.F.R. § 1002.9. 15 U.S.C. § 1681m(a), (b); Interagency Alternative Data Statement at 2; FICO, UltraFICO Score; Solon Barocas et al., The Hidden Assumptions Behind Counterfactual Explanations and Principal Reasons (December 2019); Selbst & Barocas at 1100-05; Winnie F. Taylor, Meeting the Equal Credit Opportunity Act's Specificity Requirement: Judgmental and Statistical Scoring Systems, 29 Buff. L. Rev. 73, 82 (1980).

requirements could severely disrupt data sharing. And a number of stakeholders also argue that it would be important if FCRA is applied to ensure that cash-flow information is held separately from traditional credit files maintained by nationwide consumer reporting agencies to ensure that it is only used for the specific purposes that consumers have authorized.[226]

226 Stakeholders' concern is that mixing cash-flow data into a general file would permit it to be used by employers, landlords, and other firms even though the consumer originally intended to authorize its use only for limited purposes in connection with a specific credit application. This is one of many issues that raises some stakeholders' concerns about the long-term evolution of cash-flow underwriting toward a system in which it becomes increasingly difficult for consumers and small businesses to limit access to and use of their data as a practical matter. See Section 6.3. To date, most of the cash-flow related initiatives that are being undertaken by consumer reporting and scoring incumbents emphasize that cash-flow information is maintained separately from traditional credit files; Experian Boost is the one exception, but company blog materials indicate that the limited utility data that is derived from bank account sources for purposes of that program will be dropped from consumers' traditional credit files if they withdraw authorization to continue updating the information. See Box 4.1.1.2. Consumer reporting agencies already maintain separate databases for certain other purposes, for example with regard to marketing data or other direct-to-consumer products that are subject to Gramm-Leach-Bliley Act but not the Fair Credit Reporting Act. *See, e.g.*, U.S. Government Accountability Office, Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data 27 (2006).

Clarifying the content of adverse action notices in the cash-flow context under both FCRA and ECOA would also be helpful to firms and consumers alike, since such disclosures are an ongoing compliance obligation for lenders, an important means of surfacing potential data inaccuracies for correction, and a vehicle for educating credit applicants about the underwriting process more generally so that they can improve their chances of approval over time.

However, if FCRA is determined to be not well suited for managing accuracy concerns in the cash-flow underwriting context, creating a more tailored regime might require Congressional action.[227] Similarly, filling structural gaps in the current statute would also require amendment, for instance if policymakers decided that it was important to provide comparable notification and dispute rights in situations in which cash-flow data or other credit underwriting information comes from a lender's internal records or from another party that is not considered to be a consumer reporting agency under the statute.[228] The possibility of comprehensive legislation is discussed in greater depth in Section 7.

6.1.1.3 Data security and misuse concerns

As discussed in section 5.2.2.2, where cash-flow data is transferred between companies to facilitate credit underwriting processes, additional concerns about privacy and data security are raised because the risk of potential breaches and misuse increases as the data is spread across more firms.

These concerns are heightened by the fact non-bank actors are not subject to as detailed information security requirements or related compliance monitoring as banks under the Gramm-Leach-Bliley Act. Although the Federal Trade Commission is currently engaged in a rulemaking that may bring substantive information security requirements for non-banks more in line with those that apply to banks, monitoring of non-bank entities for GLBA compliance remains a substantial concern. Although both the Consumer Financial Protection Bureau and the Federal Trade Commission have taken some information-security related actions based on their authority to address unfair, deceptive, and/or abusive acts and practices, only Congress can provide a consistent ongoing monitoring regime.

Where login credentials are used to effectuate data transfers, the privacy and security concerns are further heightened as discussed in Section 4.2.2. For instance, there is no practical way to limit the scope of data access within the range of information that is available via banks' websites, and any party that gains access to the credential typically gains the practicable ability to conduct transactions on the applicant's account.[229] The lack of guidance on application of the Electronic Fund Transfer Act and third-party service provider guidance creates further uncertainty for consumers as to whether they would have to absorb any subsequent losses.[230]

Aside from the risk of breaches and misuse by hackers, there are also potential privacy and security concerns raised where parties who are authorized to have the data in the first instance for credit-related purposes seek to re-use (and potentially share) that data for their own general commercial purposes. These issues are discussed in more depth in Section 6.1.3.

227 Some stakeholders have suggested that § 1033 of the Dodd-Frank Act could provide an alternative basis for accuracy protections although the law does not expressly address the topic. Because the Dodd-Frank Act defines "consumer" generally to include agents or representatives acting on the consumer's behalf, the Bureau could presumably define the conditions under which a firm can act as an agent or a representative. 12 U.S.C. §§ 5481(4), 5533.

228 For example, if the market started to evolve so that lenders began regularly pulling cash-flow data directly from banks or prepaid accounts, most FCRA protections would not apply because there would be no intermediary involved in the data flow. Similarly, lenders are not subject to FCRA requirements when they use their own "experience" information about the consumer to make credit decisions.

229 See Section 4.2.2.

230 See Section 4.2.3.

6.1.1.4 Related transparency issues

Finally, concerns about transparency regarding the scope of data use and sharing and about informed consent are interwoven with many of the issues outlined above. While consumers and small businesses must authorize lenders who do not already provide them with transaction accounts to access their cash-flow data for underwriting purposes, it is unclear whether applicants are making informed decisions about the various risks and tradeoffs in the current market or are alert to the practical and potential regulatory differences between cash-flow data and traditional credit reports. As discussed in Section 4, current communications content and practices vary widely across firms, and there are no federal standards for application-stage disclosures regarding what data is used in credit underwriting or related data transfers.

Enhanced educational materials and disclosures could also help consumers and small businesses take better advantage of the potential benefits of cash-flow data in credit underwriting, for example by helping them determine whether they fit the profile of people who are likely to be helped by the use of such data and how to manage their transaction accounts in a way that increases the chances that their applications will be approved over time.

Existing law: Current federal consumer financial laws do not generally require disclosure of either underwriting methodologies and inputs prior to the underwriting process. Although the Consumer Financial Protection Bureau has authority under § 1032 of the Dodd-Frank Act to require disclosures about "the costs, benefits, and risks" associated with particular consumer financial products and services both initially and over the term of service, it has not exercised that authority in connection with cash-flow underwriting or the underlying transfers of information between companies.[231]

As highlighted in the CompuCredit case, however, federal law does prohibit deceptive statements or omissions where firms choose to make voluntary statements in marketing or other materials about their criteria, processes, or products.[232] For instance, the Federal Trade Commission alleged in those case filings that it was deceptive for the card issuer to tout the fact that its cards could be used for cash advances and to list particular credit limits without explaining that cash advances and particular expenditures would actually lead to a reduction below the stated limits.[233]

Stakeholder debates: In light of the various potential customer protection concerns described above, stakeholders generally agree that education materials about cash-flow underwriting and effective application-stage disclosures are important to empowering consumers and small businesses to make informed decisions about the potential risks and benefits of cash-flow underwriting and related data transfers.

However, as discussed in more detail in Section 6.2, there are a number of challenges involved in providing meaningful disclosures for all relevant topics, particularly when consumers are submitting an application via smart phones. Providing the information and mechanisms needed for applicants to understand and exercise meaningful control over the transfer and use of their data is extremely challenging in light of the technical issues, fluid regulatory environment, and evolving customer expectations. In addition, stakeholders are divided about whether such consent processes can substitute for traditional regulatory protections with regard to privacy, fairness, accuracy, and data security.

Mitigation options: Options for improving pre-application disclosures either through voluntary firm adoption or regulatory action are discussed in more detail in Section 6.2.

231 12 U.S.C. § 5532(a).

232 See Section 6.1.1.1.

233 FTC, Complaint for Permanent Injunction and Other Equitable Relief, ¶¶ 75, 89-91, FTC v. CompuCredit Corp.

6.1.2 Loan monitoring and servicing

Privacy, fairness, and other customer protection concerns can also arise where lenders collect and review supplemental cash-flow data after an initial loan approval. In some cases, such reviews can be highly beneficial to borrowers, for instance by facilitating additional loan extensions, ongoing access to credit cards and lines of credit, and early assistance for struggling borrowers. But depending on the frequency and purpose of the reviews, there is also a risk that they could unduly intrude on borrowers' privacy or be used to take advantage of delinquent borrowers during a collections process.

Current industry practices on this issue vary widely depending on such factors as product type, individual lender policies, and borrower behavior. For example, some products that are designed as alternatives to checking overdraft services involve ongoing account monitoring to determine when consumers may need advances,[234] while additional reviews in connection with installment loans may occur only upon consumer delinquency. More continuous monitoring may also be more common in small business lending than consumer lending, given the importance of understanding how businesses' revenues may be changing over time and other factors.[235] The frequency of data pulls is often discussed in lenders' terms and conditions, but as discussed in section 6.2, there is growing evidence that applicants rarely read those documents in the course of the credit application process.

To the extent that subsequent pulls and reviews of cash-flow data are used to make decisions about additional loan extensions or adjustments in credit terms, the issues are similar to those discussed above with regard to the initial credit decisioning process. However, there also broader questions about whether it is appropriate for lenders to condition the extension of credit on the ability to collect and monitor cash-flow information over time, even in situations in which the nature of the product does not require updates and the lender is not contemplating taking some specific action with regard to the loan. A second, related question focuses on how lenders use cash-flow data to determine whether borrowers are in financial distress and if so how they then treat such borrowers.

Existing laws: The Fair Credit Reporting Act permits lenders to access consumer reports for purposes of "review or collection of an account" without obtaining consumer permission.[236] Informal guidance by Federal Trade Commission staff has interpreted this provision to permit lenders to obtain reports "solely to consider taking a specific action with regard to the account," such as adjusting terms of the account, deciding whether to participate in a bankruptcy debt management plan, or formulating a collections strategy.[237] The agency has rejected arguments that the FCRA permits pulling reports on closed-end accounts that are being paid on time where no account modification is at issue.[238]

234 Similarly, credit card issuers typically perform fraud, credit risk, and account profitability management decisions on an ongoing basis after origination, both because the accounts can be used at the discretion of the consumer and because the consumer's financial circumstances, general economic conditions, and other factors can shift at any time. FRB, Transactional Data Report at 15-16.

235 *See, e.g.,* Chris Nichols, What Commercial Loans Matter for Banks, Center State Correspondent Division (Aug. 11, 2019); Organization for Economic Co-Operation and Development, New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments 16 (2015). However, even in small business markets, electronic cash-flow data may facilitate continuous monitoring, as compared to monthly or quarterly reporting. *See, e.g.,* Armstrong; Peter Carroll & Ben Hoffman, Financing Small Businesses: How "New-Form Lending" Will Reshape Banks' Small Business Strategies 4-5, 7 (2013).

236 15 U.S.C. § 1681b(3)(A).

237 FTC, Staff FCRA Summary at § 604(a)(3)(A)-3. The staff interpretations on this issue have been controversial among some stakeholders. More generally, staff interpretations by the FTC have not always been accorded consistent deference by the courts. Rulewriting and interpretive authority transferred to the CFPB in 2010 under the Dodd-Frank Act, but the Bureau has not yet addressed its position on many of the interpretive issues that had been addressed through FTC informal guidance. *Id.* at 1-2, 6-7.

238 *Id.* at 13-14 (discussing 1999 interpretive letter).

However, because the statute provides a further exception for obtaining reports with the written permission of the consumer,[239] it is not clear whether this limitation has much practicable effect even with regard to traditional credit reports because lenders may be obtaining consumer authorizations to ongoing monitoring via application forms or other contract materials. And as noted above, federal regulators also have not yet opined on whether cash-flow data obtained via a data aggregator for use in credit underwriting is a "consumer report" in the first instance.[240]

Stakeholder debates: Debates about the fairness of conditioning credit on ongoing access to cash-flow data and about its use in connection with distressed borrowers underscore that cash-flow underwriting may not just involve a one-time review of limited account information to facilitate increased access to credit, but an ongoing relationship in which data collection and review may occur multiple times and in situations in which the lender's and borrower's interests may be in more tension with each other.[241] In the context of potential borrower distress, access to cash-flow data could have both benefits and risks: The relative sensitivity of the data could help to minimize losses for both borrowers and lenders, but lenders could also use it to prioritize their interests at the expense of borrowers' through excessive data pulls, cutting off access to credit preemptively, or using such information as the timing of deposits to engage in highly aggressive collection practices.

Many stakeholders take positions on post-origination monitoring that are similar to their views on the potential privacy and fairness risks in initial underwriting. For instance, some stakeholders tend to emphasize the potential benefits of monitoring, noting that some lenders may not be comfortable extending credit to riskier or more opaque borrowers in the absence of such information and that it creates the potential for faster intervention in the event of distress. Such stakeholders also argue that customer choice can be relied upon to manage concerns to the extent that some consumers or small businesses are uncomfortable with the conditions or risks in ongoing monitoring.

In contrast, critics tend to emphasize the potential risks of ongoing monitoring and aggressive collections practices as further illustrating how cash-flow underwriting could work to the substantial disadvantage of more vulnerable borrowers. They also argue that customer choice is not sufficient to manage concerns, both because applicants may not focus on lenders' monitoring or collections practices during the origination process and may be practically constrained in shopping for alternatives.

However, the idea of conditioning credit on continuing access to cash-flow information raises potential tensions with some stakeholders' embrace of a robust customer control regime to govern data sharing more generally. As discussed further in Section 6.2, in discussing the broader data sharing system that is emerging in U.S. markets, some stakeholders have argued that meaningful customer control cannot be effectuated unless consumers and small businesses have a right to revoke previous consents and terminate data access. Some also argue for non-discrimination protections to prevent customers from being subject to different treatment after exercising such rights. Thus, to the extent that lenders might reserve a contractual right to terminate credit upon a withdrawal of cash-flow access, this creates substantial tension with some stakeholders' concepts of a robust consumer control regime.

239 15 U.S.C. § 1681b(a)(2).

240 See Box 6.1.1.2.1.

241 For instance, where a borrower becomes delinquent, the lender's focus is on repayment of the particular credit product in isolation, while the borrower may be focused on managing a general deterioration across all of their finances.

Mitigation options: Additional quantitative and market research would be helpful to assess the potential benefits and risks of using cash-flow data in loan servicing and collections processes, as well as best practices and risk mitigation options.

In terms of the most obvious risk management tools, clarifying application of the FCRA to cash-flow information would at most establish a mild general norm with regard to pulling cash-flow data for purposes of subsequent account monitoring, given the additional provision permitting access to consumer reports upon authorization by the consumer. As discussed further in Section 6.1.3, federal regulators have provided little substantive guidance on how the authorization process should operate under that part of the statute.

Although some stakeholders argue that any concerns on these issues can be managed through robust disclosures and authorization processes as discussed further in Section 6.2, past history with other servicing and collections practices issues suggests that credit applicants tend not to focus substantial attention on such issues at the time that they are choosing between lenders. Indeed, federal regulators have sometimes found it appropriate to impose direct restrictions on servicing and collections practices under unfairness and other legal authority because they concluded that it is impracticable to expect consumers to protect themselves from aggressive practices in the initial process of selecting a lender or other financial services provider.[242]

With regard to establishing affirmative standards for conditioning credit on the availability of post-origination monitoring or otherwise restricting lenders' ability to engage in such monitoring, we are unaware of any other regulatory regimes that have addressed the issue in detail. For example, the California Consumer Privacy Act contains a general protection against discrimination on the basis of consumers' exercise of data rights, but it is subject to an exception that is still in the process of being implemented and is not specific to the lending context.[243]

On the question of how cash-flow data might be used in collections practices, various general restrictions apply to lenders and third-party debt collectors under the Electronic Fund Transfer Act concerning collecting preauthorized payments from consumers' accounts[244] and the Fair Debt Collection Practices Act concerning various activities by third-party debt collectors.[245] However, consumer advocates have raised concerns in other contexts about both the level of substantive protections provided and enforcement.[246] The Consumer Financial Protection Bureau is in the process of the first-ever rulemaking to flesh out FDCPA statutory requirements, though to our knowledge access to or use of cash-flow information has not been raised to date in that process.[247] Some stakeholders have suggested that one mechanism for protecting consumers in light of the particular sensitivity of cash-flow information would be to require debt collectors to obtain a new and separate authorization to access consumers' cash-flow data, rather than assuming

242 *See, e.g.,* 78 Fed. Reg. at 67849; 49 Fed. Reg. 7740, 7744 (Mar. 1, 1984).

243 Cal. Civ. Code § 1798.125 (generally prohibiting businesses from denying goods or services to consumers, charging different prices, providing a different quality of goods or services, or suggesting that consumers will receive different prices or quality for exercising rights under the statute, but permitting the offering of "financial incentives" if the price incentive is "directly related to the value provided to the consumer by the consumer's data"). The Attorney General of California, who has proposed rules for implementation, has noted that the provision has created "a significant amount of confusion and misunderstanding." California Department of Justice, Notice of Proposed Rulemaking, Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations 36-37 (Oct. 11, 2019).

244 15 U.S.C. §§ 1693e, 1693k; 12 C.F.R. §§ 1005.10. For discussion of EFTA requirements and compliance issues in the context of preauthorized transfers and lending more generally, *see, e.g.,* Consumer Financial Protection Bureau, Compliance Bulletin 2015-06 (Nov. 23, 2015); Hunton & Williams, Client Alert: Where Are We Now: A Look at the EFTA's Prohibition of Compulsory Payments of Loans by Electronic Fund Transfers (2017). For a discussion of problematic presentment practices in the payday lending market, see 82 Fed. Reg. 54472, 54720-30 (Nov. 17, 2017).

245 15 U.S.C. §§ 1692-1692p. For discussion of FDCPA requirements and compliance issues more generally, *see, e.g.,* 84 Fed. Reg. 23274 (May. 21, 2019); 78 Fed. Reg. 67848 (Nov. 12, 2013).

246 See notes 244-245.

247 84 Fed. Reg. 23274 (May. 21, 2019).

that consumer authorization for lenders to obtain the information would transfer downstream to later parties.

6.1.3 Downstream re-use of cash-flow data

A final set of customer protection concerns focuses on the circumstances under which lenders or other firms can re-use cash-flow data that was obtained for credit purposes to support their own downstream business activities, such as refining underwriting models, developing new products or services, providing analytical services to other clients, or marketing other products or services to the customer.

Particularly because of the richness of cash-flow information, the broader the latitude to re-use and transfer customer data for other purposes, the larger the incentives for firms to collect and retain more data than they may strictly need for immediate purposes. And to the extent that the downstream re-use involves transfers to additional companies, they may further exacerbate potential privacy and security risks for consumers and small businesses. These re-use concerns can potentially arise not only with lenders, but with aggregators and other vendors that have facilitated initial data transfers and processing.

Existing federal financial laws restrict the re-use and downstream data sharing for certain types of financial data in some circumstances, particularly in connection with third-party marketing to consumers. However, they provide fairly wide latitude for other activities, including re-use and transfer of data that has been anonymized by stripping out certain identifying information. These provisions have been critical to innovation in the U.S. financial services market because they provide an avenue for lenders, model developers, and other financial services providers to access data to refine underwriting models and develop new products and services more generally.

However, re-use activities are attracting increasing concern from some stakeholders, particularly where they involve sharing between multiple companies. Critics have raised concern that the scope of data use and sharing may not conform to customer expectations and may make it difficult for customers to monitor their privacy and security risks over time as data is passed downstream to additional parties. Some sources are also raising increasing concerns about the risk of reidentification of anonymized data as digital information and analytical tools spread much more widely across more firms.[248] These concerns are not unique to the cash-flow underwriting context, although they are attracting significant attention there due to activities by one aggregator that have drawn criticism by privacy researchers and calls for investigations by members of Congress.[249]

Existing laws: The Fair Credit Reporting Act and Gramm-Leach-Bliley Act impose certain restrictions on the re-use and/or sharing of data within their respective purviews. Specifically, FCRA

248 *See, e.g.,* Luc Rocher et al., Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models, 10 Nature Communications 3069 (2019); David Sanchez et al., How to Avoid Reidentification with Proper Anonymization (2018); Yves-Alexandre de Montjoye et al., Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata, 347 Science 536 (2015); Arvind Narayanan et al., A Precautionary Approach to Big Data Privacy (2015); Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010); Alessandro Alcquisti & Ralph Gross, Predicting Social Security Numbers from Public Data (July 7, 2009); Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University Data Privacy Working Paper 3 (2000).

249 In January 2020 three members of Congress asked the Federal Trade Commission to investigate the practice, raising concerns about whether the aggregator's partners were clear enough in disclosing the fact that data could be resold and about risks that the data could be "reidentified" as belonging to specific individuals. Sen. Ron Wyden et al., Letter to Joseph J. Simons (Jan. 17, 2020); Tracy; Lydia Beyoud, Democrats Call for FTC Probe of Financial Data Giant Yodlee, Bloomberg Law (Jan. 17, 2020); Emily Bernbaum, Lawmakers Call for FTC Probe into Top Financial Data Aggregator, The Hill (Jan. 17, 2020). A few weeks after the announcement, news reports based on leaked documents raised questions about the particular anonymization techniques used to manage the data. Joseph Cox, Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans, Vice (Feb. 19, 2020). For a detailed description of Yodlee's aggregation business servicing large banks' personal financial management services and data sales practices as of 2015, see Hope.

BOX 6.1.3.1 GLBA PRIVACY REQUIREMENTS

The Gramm-Leach-Bliley Act generally prohibits "financial institutions" from sharing consumers' nonpublic personal information with non-affiliated companies unless the institutions first provide notice and an opportunity to opt out. Various exceptions to the statute permit certain types of sharing without notice and/or opt out, for instance when the financial institution uses a vendor to provide financial services to the consumer, hires a marketer to cross-sell financial products to existing customers, and for various other business functions. The restrictions also do not apply to data that has been anonymized.

Sharing is also permitted with the consent or at the direction of the consumer and to people acting in a fiduciary or representative capacity on behalf of the consumer or holding a legal or beneficial interest relating to the consumer. There is relatively little interpretive guidance on consumer authorizations for sharing under the statute as discussed in Box 6.2.1.1.

See Box 6.1.3.2 for discussion of the definition of a "financial institution" and other coverage issues. Where a vendor or other non-affiliated party receives consumer/customer information from a financial institution, it generally is also subject to GLBA restrictions on re-use for other purposes and on further sharing of the information with other third parties, although the details vary depending on the circumstances as discussed in Box 7.3.1. Such firms are not required to provide a privacy notice to the consumer/customer because they do not have a direct relationship. The Federal Trade Commission's original rulemaking notices specifically emphasized that firms that provide account aggregation services directly to consumers would be treated as "financial institutions," and that firms that process consumer data as service providers to other financial institutions are subject to the regulation's limitations on re-use of customer data.

Unlike the GLBA information security requirements discussed in Box 5.2.2.2.1, which apply only to customers who have an ongoing relationship with a financial institution, the information sharing provisions apply to consumers who apply unsuccessfully for credit or engage in other one-time transactions.

In addition to the initial notice required in connection with the opportunity to opt out of certain information sharing, financial institutions must generally provide annual privacy notice updates to their customers even if they do not engage in the type of information sharing that triggers a right to opt out. The initial and annual notices are required to explain the institutions' information sharing and information security practices. Federal regulators issued a model form for these privacy notices in 2009, and the Consumer Financial Protection Bureau assumed rulewriting authority over the privacy provisions in 2011.

Sources: 15 U.S.C. §§ 6801-6803, 6809; 12 C.F.R pt. 1016; 74 Fed. Reg. 62890 (Dec. 1, 2009) 65 Fed. Reg. 35162, 35171-72 (June 1, 2000); 65 Fed. Reg. 33646, 33654-56 & n.29, 33658, 33667-68 (May 24, 2000).

restricts users of "consumer reports" from obtaining or repurposing such information for general marketing, curiosity, or other purposes not designated as permissible under the statute.[250] GLBA does not generally restrict the internal use of customer information by "financial institutions," but it does prohibit them from transferring nonpublic personal information to non-affiliated companies for certain purposes unless consumers have first received notice and an opportunity to opt out.[251]

Because of these provisions, consumers may have a general expectation that their credit-related information will not be reused or shared for purposes that are unrelated to the provision of the particular loan or account. However, the extent of practical limitations may be more limited than many consumers realize. For example, both FCRA and GLBA restrictions have been interpreted not to apply to data that has been de-identified.[252] Thus, traditional consumer reporting agencies may currently license anonymized data to lenders for model development, and such data can also be transferred by

250 15 U.S.C. § 1681b; FTC, Staff FCRA Summary at § 604(a)-6.

251 15 U.S.C. §§ 6802-6803; 12 C.F.R. §§ 1016.10-.15.

252 12 C.F.R. § 1016.3(q)(2)(ii)(B); FTC, Staff FCRA Summary at 11, § 603(d)(1)-5.

financial institutions under GLBA without the need for notice and opt out.[253] Both statutes also allow activity that would not otherwise be permissible with consumer consent.[254] Accordingly, consumers who do not read opt-out notices under GLBA or lenders' terms and conditions documents carefully may find that they have authorized more re-use and sharing than they would otherwise expect.[255]

As discussed in Section 6.1.1.1, federal law also generally prohibits unfair, deceptive, and abusive acts and practices.[256] Federal agencies have pursued some deception and unfairness cases involving data practices, including situations in which companies' actual collection and usage practices were alleged to be inconsistent with their representations to customers. However, while federal agencies have urged companies to collect only information that is reasonably needed to provide services to customers and to use such data only in ways that customers reasonably expect, these concepts are generally treated as best practices rather than legal requirements.[257]

Stakeholder debates: Stakeholders are deeply divided over the general application of the FCRA to cash-flow data that is transferred for credit purposes as discussed in Section 6.1.1.2. There is less debate over whether GLBA restrictions apply, though even on that topic it is not clear that there is a common understanding of how specific requirements operate in the context of consumer permissioned data transfers and there are deep divides about the adequacy of its protections.[258]

At one end of the spectrum, some stakeholders prioritize protecting the re-use of data (particularly in anonymized form) in order to fuel further innovation in financial services markets and argue that customers can manage any individual privacy concerns through the consent processes. Though some of these stakeholders advocate for improving consumer control mechanisms as discussed further in Section 6.2, they generally argue against other regulatory prescriptions on data re-usage. They emphasize that to the extent that there are concerns about the potential re-identification of anonymized data, they are not unique to customer-permissioned data transfers and argue that they should be dealt with on a broader sectoral basis.

In contrast, some stakeholders argue that sales of anonymized data should not be permitted in the customer-permissioned context even if they are allowed in other settings because they believe it is particularly difficult to explain the benefits and risks to consumers, that sales could change incentives with regard to data collection practices in the customer-permissioned market, and that they could shift pricing within the industry.[259]

Other stakeholders view GLBA protections as fundamentally inadequate in both the context of customer-permissioned transfers and with regard to financial data more generally. While they

253 Even if the data is not anonymized, GLBA permits transfers to non-affiliated companies for marketing and other general purposes if the consumer is provided notice and opportunity to opt out of the sharing. 15 U.S.C. § 6802(a). News reports of such transfers attracted substantial attention in the years preceding GLBA, although statistics were difficult to obtain. One evaluation of more than 6000 financial institution privacy notices from 2016 found that more than 85 percent indicated that institutions did not engage in this kind of information sharing, but that it is more common among large banks and credit card companies. Lorrie Cranor, A Large Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices, ACM Transactions on the Web 13-14, 16-17 (2016); Electronic Privacy Information Center, The Gramm-Leach-Bliley Act (visited Feb. 8, 2020); Peter P. Swire, The Surprising Virtues of the New Financial Privacy Law, 86 Minn. L. Rev. 1263 (2002).

254 15 U.S.C. §§ 1681b(a)(2), 6802(e)(2); 12 C.F.R. § 1016.15(a)(1); FTC Staff FCRA Summary at § 604(a)(2)-1 & -2.

255 To the extent that FCRA or GLBA do not apply in the first instance, California residents are provided more robust protections with regard to data use and sharing by the California Consumer Privacy Act. See Cal. Civ. Code § 1798.145(d), (e); Box 5.2.2.1.1.

256 12 U.S.C. § 5531; 15 U.S.C. § 45.

257 *See, e.g.,* Federal Trade Commission, Complaint for Civil Penalties, Permanent Injunction, and Other Relief, U.S. v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019); Federal Trade Commission, Complaint for Civil Penalties, Permanent Injunction, and Other Relief, U.S. v. RockYou, Inc., No. 3:12-cv-01487-SI (N.D. Cal. Mar. 26, 2012). *See generally FTC v. Wyndham Worldwide Corp.*, 799 F.3d. 236 (3d Cir. 2015) (upholding the FTC's authority to bring unfairness cases based on data security practices); Federal Trade Commission, Start with Security: A Guide for Business: Lessons Learned from FTC Cases (2015).

258 15 U.S.C. §§ 6801-6803, 6809; 12 C.F.R pt. 1016.

259 See Section 6.2 for further discussion of general challenges concerning informed consent.

BOX 6.1.3.2 GLBA COVERAGE ISSUES

As discussed in Boxes 5.2.2.2.1 and 5.3.3.1, GLBA was generally designed to impose consistent information sharing and security requirements on both bank and nonbank "financial institutions." However, coverage rules are somewhat complex due to both legislative language and regulatory implementation. Federal regulators have not issued specific guidance to address how the various parts of the law apply in the context of the modern system for customer-permissioned transfers of financial data or to fintechs more generally, although their original rulemaking notices provide helpful discussions and some aggregators and fintechs have acknowledged that they are subject to the law's safeguards requirements.

The law applies generally to nonpublic personal information, which is defined to mean personally identifiable financial information that is provided by a consumer to a financial institution, that results from any transaction with the consumer or service provided for the consumer, or that is otherwise obtained by the financial institution. However, it excludes information that is publicly available from other sources. Federal regulators have interpreted the term to apply broadly even to information that is not inherently financial in nature (such as lists of bank customers), but not to cover aggregate or blind data that does not contain personal identifiers.

GLBA generally defines "financial institution" to mean any company whose business is to engage in "financial activities" as described in the Bank Holding Company Act. BHCA regulations define the covered activities to include items such as extending credit, maintaining information relating to the credit history of consumers and providing it to creditors to underwrite or monitor loans, providing various types of financial advisory services, certain payments-related activities, and certain processing and transmission of financial data.

However, the Federal Trade Commission applied its regulations only to non-bank entities that "substantially engage in financial activities" as that term had been defined when GLBA was enacted, while the federal banking agencies applied their requirements to "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities." The FTC did not explain the precise differences between the two definitions, but included examples excluding retailers whose only means of extending credit are occasional lay away or deferred payment plans or grocery stores that allow customers to cash a check or write a check for over the purchase amount to obtain some cash in return.

A 2019 FTC proposal would extend coverage to non-banks that are substantially engaged in activities that are financial in nature or incidental to such financial activities, as defined by BHCA regulations as they are amended over time. For example, the proposal would reach companies that act as "finders" by connecting potential buyers and sellers of goods and services for transactions that the buyers and sellers themselves negotiate and consummate. The Consumer Financial Protection Bureau has not yet indicated whether it will conform the definition of non-bank financial institution for purposes of the GLBA privacy rules that transferred to its jurisdiction in 2011.

An additional source of potential confusion is the way in which particular requirements apply to particular companies that receive customer information from financial institutions. For instance, if a company is a financial institution, FTC rules specify that it must follow information safeguards requirements to protect customer information even if that company itself does not have a direct relationship with the consumer in question. On the information sharing side, the statute subjects companies that receive customer or consumer information from a financial institution to restrictions on re-use and further sharing of the information, regardless of whether they themselves are financial institutions. However, the scope of the restrictions vary depending on the circumstances as discussed in Box 7.3.1.

Sources: 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k)(4); 12 C.F.R. § 225.28(b)(1), (2)(iv), (6), (10), (12) (13), (14); 12 C.F.R. § 1016.3(l)(1), .3(l)(3)(i), .3(l)(3)(iv), .3(q)(2)(i), .3(q)(2)(ii)(B); 16 C.F.R. § 313.1(b); 84 Fed. Reg. 13158, 13166-69, 13175-76 (Apr. 4, 2019); 83 Fed. Reg. 40945, 40948 (Aug. 17, 2018); 67 Fed. Reg. 36484, 36486 (May 23, 2002); 66 Fed. Reg. 8616, 8618 (Feb. 1, 2001); 65 Fed. Reg. 35162, 35171-72 (June 1, 2000); 65 Fed. Reg. 33646, 33654-56 & n.29, 33658, 33667-68 (May 24, 2000).

advocate for shifting GLBA from an opt-out to an opt-in regime and other tightening measures, many also believe it is impracticable to expect consumers and small businesses to manage all of their privacy and security risks through a permissioning process as discussed in Section 6.2. Many of these stakeholders thus also argue for the adoption of broader standards that would require companies to collect, transfer, and retain only data that is reasonably needed to provide particular products and services to customers, to use it only in ways that customers would reasonably expect, and to provide additional safeguards with regard to de-identified information.

BOX 6.1.3.3 DIFFERENTIAL PRIVACY AND OTHER PRIVACY ENHANCING TECHNIQUES

In addition to stripping personal identifiers from data sets, researchers are developing other techniques that allow them to reduce the sharing of raw data and the chance that machine learning and other analytical models can later be used to reverse engineer the data for individuals whose information was used to build the algorithms. Some of these techniques include:

K-anonymity and similar techniques: These techniques modify or remove values for certain "quasi-identifier" fields that could be used to help re-identify individuals in broader data sets even after the directly identifiable information such as name or Social Security number is stripped out. For example, with k-anonymity, specific number values might be replaced with ranges that are constructed so that every combination of potentially identity-revealing characteristics occurs in at least k different rows within the data set. These modifications are typically made before data is shared or used to develop a model.

Differential privacy: Differential privacy is built on the concept that if it is difficult to determine whether any one individual's data is contained in a particular data set, it should be difficult to determine anything else about them either. The techniques involve adding a small amount of "mathematical noise" to the raw data, the computations, or the published outputs in ways that make it difficult for an outside party to determine from the results or from a model trained on the data whether a particular individual's information is included in the underlying data set. Researchers use a mathematical definition of privacy and a "privacy budget" to manage various tradeoffs between accuracy and privacy risk, for instance in deciding how much noise to add and how many inquiries can be run against the data set before aggregate results would allow an outside party to begin filtering the noise back out of the results.

Federated learning and secret multi-party computation: While standard machine learning models rely on a centralized data set to train a model, federated learning and secret multi-party computation involve different ways of running models on "local" data sets and then cumulating the results to develop a global model. Some techniques can be performed even at the level of an individual smart phone or other device, though such an approach requires substantial processing power and is dependent on device connectivity.

Homomorphic encryption: These techniques are used when data analysis needs to be performed by a third party. They involve encrypting the underlying data, providing the encrypted results for further processing by the third party's model (which can also be encrypted, for instance in a cloud environment), and returning the outputs to the original data source (which has a non-public encryption key to decode the actual results). This has advantages to both the data source and the model developer in terms of protecting customer privacy and intellectual property, and can be constructed to maintain full accuracy. However, these systems are relatively slow and to date can only be used with certain types of mathematical functions.

Some techniques can be combined with each other, for instance by using federated learning on individual devices and then differential privacy to add "noise" to the aggregated results. Each of these techniques is still in the process of being developed and enhanced to minimize potential disadvantages, and some are not yet widely used in financial services.

Sources: Sanchez et al.; Narayanan et al.; Jack Mardack, Layman's Guide to Machine Learning and Customer Data Privacy, Actian (Jan. 16, 2020); Kyle Wiggers, AI Has a Privacy Problem, But These Techniques Could Fix It, Venture Beat (Dec. 21, 2019); World Economic Forum & Deloitte, The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value (2019); Anton Dimitrov, The World Needs Privacy-Preserving Computations, Medium (Jan. 15, 2019); Harvard University Privacy Tools Project, Differential Privacy, Harvard University (visited Feb. 8, 2020); Google, How Google Anonymizes Data, Google.com (visited Feb. 8, 2020); Apple, Differential Privacy, Apple.com (visited Feb. 8, 2020); Google AI, Federated Learning: Building better products with on-device data and privacy by default, Google.com (visited Feb. 8, 2020); Brendan McMahan & Daniel Ramage, Blog, Federated Learning: Collaborative Machine Learning without Centralized Training Data, Google AI (April 6, 2017).

Mitigation options: Industry could potentially reduce general concerns about data re-use by improving disclosures, individual adoption of minimization and reasonable use standards and corresponding contractual restrictions on their business partners, and/or by implementing broader self-governance standards. As discussed in Section 5.2.2, some of these efforts are underway though they face challenges due to competitive and coordination issues.

With regard to the use and sharing of de-identified data, more widespread adoption of more sophisticated anonymization techniques could reduce reidentification risks somewhat, and privacy

enhancing technologies can also be helpful.[260] However, those measures can have tradeoffs with regard to data utility depending on the circumstances and may still not entirely eliminate potential risks as data compilations, machine learning techniques, and computer capacity continue to grow. Accordingly, some jurisdictions are also beginning to strengthen protections by adopting more specific definitions of what constitutes sufficiently anonymized data to warrant exemption from certain data protections, as well as imposing other types of safeguards with regard to its retention, use, and transfer.[261] In the research context, some stakeholders are also beginning to ask whether consent protocols need to be changed in light of reidentification risks.[262]

Federal regulators could help to address concerns about reuse and reidentification by providing additional guidance under GLBA and the FCRA, for instance by publishing specific information to explain whether and how the statutes apply to consumer-permissioned transfers of transaction account data and fleshing out the conditions under which the statutes' exceptions for customer-authorized use/transfers and for anonymized or de-identified data are triggered. Such guidance could dovetail well with stakeholders' calls for strengthening disclosures and permissioning processes more generally as discussed further in Section 6.2. A few sources have also asserted that data minimization requirements could be imposed under GLBA or unfairness authorities.[263]

However, congressional action would be needed to adopt certain additional safeguards. For example, converting GLBA's underlying framework from opt-out to opt-in, making its coverage more consistent, adopting broad data minimization requirements, and providing protections to small businesses would likely all require statutory amendments. Similarly, while federal regulators can address what constitutes sufficiently anonymized data to fall outside the scope of the FCRA and GLBA, imposing affirmative requirements with regard to handling of such data to manage residual privacy risks might require congressional action. These issues are discussed further in Section 7.

6.2 Enhancing customer control to leverage benefits and mitigate risks

As stakeholders debate the various policy issues discussed above about cash-flow underwriting, questions arise repeatedly about the extent to which particular concerns can be managed by enhancing customers' control over their data. The fact that credit applicants must generally authorize access to their transaction account records is one of the biggest distinctions between cash-flow information and traditional credit reports, and many stakeholders view enhanced customer control as (1) a key to effectuating the potential benefits described in Sections 5.1 and 5.2; (2) a means of managing various tradeoffs and risks discussed in Section 6.1; and/or (3) an opportunity to empower consumers and small businesses to benefit from their own data and to take greater control over their financial lives more generally.

260 For example, in addition to removing direct identifiers, anonymization techniques can include "data coarsening" of "quasi-identifiers" such as birth date or zip code. Differential privacy algorithms add small, quantified errors ("noise") to analytical outputs for release, rather that releasing either the original input data or unaltered outputs. *See, e.g.,* Sanchez; Narayanan et al.; Singapore Personal Data Commission, Guide to Basic Data Anonymization Techniques (2018); Opinion 05/2014 on Anonymisation Techniques (EU), Technical Report, Article 29 Data Protection Working Party (Apr. 10, 2014).

261 *See, e.g.,* Cal. Civ. Code §§ 1798.140(a), (h), (o), (r), 1798.145(a)(5); Council of European Union, Regulation (EU) 2016/679 (2016); Opinion 05/2014 on Anonymisation Techniques (EU). Some countries have considered criminalizing re-identification of data. *See, e.g.,* Kurt Wimmer & Gabe Maldoff, India Proposes Updated Personal Data Protection Bill, Inside Privacy, Covington (Dec. 12, 2019).

262 *See, e.g.,* Nature, Editorial, Time to Discuss Consent in Digital-Data Studies, nature.com (July 21, 2019); European Commission, Ethics and Data Protection 7-8 (2018).

263 *See, e.g.,* Electronic Privacy Information Center, Comments to the Federal Trade Commission on Standards for Safeguarding Customer Information at 10-11 (Aug. 1, 2019) (urging adoption under GLBA authorities); Woodrow Hartzog & Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 Geo. Washington L. Rev. 2230 (2015) (discussing data minimization in the context of unfairness authority).

Indeed, it is striking how many different stakeholders and policymakers have emphasized the importance of consumer control in the course of debates about cash-flow underwriting and the use of customer-permissioned data more generally.[264] Yet despite this broad-based support at a high level, fostering informed consent and providing other control mechanisms presents a number of communications, business process, and technological challenges, as well as potential policy issues. Although various market actors are working to develop prototypes and other implementation solutions, the practical and coordination challenges for market-wide adoption are substantial. No one market actor acting alone may be able to provide the kind of robust control regime that many stakeholders envision.

Stakeholders are also deeply divided about the role that control should play in the broader marketplace. Some argue that customer control mechanisms can manage privacy tradeoffs and certain other risks without the need for prescriptive restrictions that would increase compliance burdens or restrict flexibility for further innovation. Other stakeholders point to evidence that consumers and small businesses are already feeling overwhelmed by data privacy and security issues, and advocate for adopting additional safeguards to simplify customer choices as the volume of data sharing increases. And others have questioned whether customer data rights might need to be calibrated in particular circumstances to account for other policy concerns, for instance to ensure that lenders do not get a distorted picture of applicants' finances, to facilitate lenders' ability to work with borrowers who may be experiencing financial difficulties, or to make it easier for lenders to build predictive models for all populations.

This section provides an overview of the various challenges and debates about how to develop a robust control regime to help actualize the benefits of cash-flow underwriting and to manage its risks and tradeoffs. Section 6.2.1 provides a brief overview of potential mechanisms for enhancing customer control and some of the practical challenges to effectuating those elements in a meaningful way in the context of cash-flow underwriting. Section 6.2.2 looks at the research on how customers approach data control issues in the current market and the implications for stakeholder debates about balancing customer control, customer protection, and other policy interests. Section 6.2.3 discusses potential options going forward.

6.2.1 Elements of a robust control system

Although existing federal financial laws do not provide detailed guidance on how to construct a robust opt-in system for data use and sharing, other jurisdictions are in the process of building out more comprehensive regimes to provide consumers with multiple rights that are designed to provide them with robust control over businesses' handling of their personal information. As noted above and discussed in Appendix D, both the CFPB and various private organizations have also issued principles for customer-driven data sharing that emphasize the importance of consumer

264 *See, e.g.,* CFPB, Data Sharing Principles at 3 (emphasizing that "[c]onsumers can enhance their financial lives when they control information regarding their accounts or use of financial services"); JPMorgan Chase, Press Release, JPMorgan Chase, Envestnet Yodlee Sign Agreement to Increase Customers' Control of Their Data, businesswire.com (Dec. 5, 2019) (touting a data sharing agreement and new dashboard as giving customers "more visibility and control" in using financial apps); Saunders, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology at 12-13 (arguing that consent mechanisms should be provided at the level of individual data elements, should be time-limited and self-expiring, and should provide multiple simple options for ending data sharing);); Financial Data Exchange, Organization Overview at 6 (stating as a first principle that "[c]onsumers should be able to permission their financial data for services or applications"); John Pitts, Letter to Chairman Mike Crapo and Ranking Member Sherrod Brown, Senate Committee on Banking, Housing and Urban Affairs at 3 (Mar. 15, 2019) (arguing that customer control should be a "defining characteristic" of any effort to fix the sharing of consumer financial data).

BOX 6.2.1.1 GUIDANCE ON AFFIRMATIVE OPT-IN FOR DATA SHARING UNDER FEDERAL CONSUMER FINANCIAL LAWS

The Federal Credit Reporting Act requires consumer permission before employers can obtain consumer reports for employment purposes and allows users to obtain and use consumer reports for otherwise impermissible purposes pursuant to the consumer's written instructions or permission. Somewhat similarly, the Gramm-Leach-Bliley Act contains an exception that allows sharing nonpublic personal information with non-affiliated third parties with the consent or at the direction of the consumer. Aside from these circumstances, neither the FCRA nor the Gramm-Leach-Bliley Act generally rely on opt-in requirements for data use or sharing, and there is only limited regulatory guidance on the operation of these permission-based provisions.

With regard to the FCRA employment provisions, the statutory language and informal FTC staff guidance focus primarily on the contents of pre-authorization disclosures, for instance by mandating that clear and conspicuous language in a standalone document without extraneous material. The statute does not prohibit employers from conditioning employment on consent, and the staff guidance states generally that a disclosure and consent remain effective throughout the duration of employment.

Although widely used, there is also relatively little guidance concerning the FCRA provision that allows uses of a credit report "[i]n accordance with the written instructions of the consumer to whom it relates." Informal guidance from FTC staff indicates that a statement that "I authorize you to procure a consumer report on me" is a sufficiently clear authorization under this provision, while a statement that "I understand that where appropriate, credit reports may be obtained" is not sufficient because it could be construed as a notification of a possible future action rather than as an affirmative grant of permission. However, other than addressing certain mechanical issues concerning electronic authorization, the guidance does not otherwise suggest standards for the authorization process, defining the scope of the permitted use, revoking a previous authorization, or other topics.

Similarly, GLBA privacy regulations allow information sharing with non-affiliated companies "[w]ith the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction," but do not provide additional guidance on the statutory provision. During its rulemaking process, the Federal Trade Commission stated that any information sharing pursuant to the exception should not exceed the purposes for which consent was given and that consents would not be sufficiently clearly made if they were effectuated via "a line buried in a document or a negative option not clearly explained to the consumer." The preamble to the final rule emphasized that financial institutions should "take steps to ensure that the limits of consent are well understood by both the financial institution and the consumer," but did not mandate specific procedures or language.

Sources: 15 U.S.C. § 1681b(a)(2), (b)(2); *id.* § 6802(e)(2); 12 C.F.R. § 1016.15(a)(1); 65 Fed. Reg. 11174, 11184 (Mar. 1, 2000); 65 Fed. Reg. 33646, 33671 (May 24, 2000); FTC, Staff FCRA Summary at § 604(a)(2), 604(b)(1), 604(b)(2).

decisionmaking and autonomy, not just in providing initial informed consent but throughout the course of their dealings with financial services providers.[265]

In considering how these general rights and principles could translate to the cash-flow underwriting context specifically, several distinct elements stand out as potentially important:

- Clear and effective communications prior to and during the application process about the use of data, related information transfers where relevant, and the privacy and information security practices of firms that participate in the transfer and processing of cash-flow data;
- Efficient processes for memorializing the applicants' authorizations for data access and use, as well as for communicating them to downstream parties;

265 *See, e.g.,* CFPB, Data Sharing Principles; American Law Institute; American Bankers Association, Statement for the Record; Financial Data Exchange, Organization Overview at 6; World Economic Forum, White Paper; Center for Financial Services Innovation; Center for Financial Services Innovation, CFSI's Consumer Data Sharing Principles. The broader discussion of respecting privacy and empowering consumers to exercise control may raise questions about whether banks themselves should consider providing specific information and/or seeking affirmative consent before using existing customers' cash-flow data for credit underwriting. At the same time, some stakeholders have indicated that some consumers and small businesses may be frustrated if their banks do not routinely take their history as longstanding customers into account when considering applications for additional credit.

- Mechanisms for applicants to review their data, for instance to confirm the scope of the transmission and identify and address potential accuracy concerns; and
- Downstream processes and tools to enable borrowers to manage their data over the course of their credit relationships, such as mechanisms to monitor ongoing use and sharing; the potential ability to modify or revoke access and compel deletion; and dispute resolution channels.

Various market actors are working to develop prototypes and other implementation solutions for many of these features. For instance, the Financial Data Exchange has begun working with individual members to convene consumer focus groups to improve consent protocols, and a growing number of banks and aggregators provide dashboards that allow consumers and small businesses to monitor the authorizations they have previously granted and to modify them over time. Initiatives to provide third-party credit scores that encompass cash-flow data are also providing dispute resolution processes similar to those provided in the traditional credit reporting system to address potential accuracy concerns.

Yet market-wide adoption of the elements listed above would require overcoming a range of communications, business process, and technological challenges, as well as resolving potential policy considerations:

Communications and disclosures. Informed consent cannot occur without first providing clear, effective communications to educate applicants about the relevant tradeoffs, but such disclosures can be challenging to design and deliver for a number of reasons. First, to consider all of the potential risk/benefit tradeoffs discussed in Section 6.1 above, applicants would potentially need several distinct types of information, including:

- what data will be collected and relied upon in the underwriting process;
- the frequency and nature of any subsequent data pulls and monitoring practices;
- information regarding the risks and logistics of the data-sharing process where relevant, potentially including the identity of the aggregator or other vendors used to transfer and process the data;[266] and
- the relevant firms' policies regarding data management, re-use, and sharing for other purposes.

Beyond these practical details, consumers and small businesses may also want broader information to help evaluate the potential privacy tradeoffs of authorizing use of their data, such as a sense of the degree to which sharing the data will increase their chances of obtaining credit or better terms—or, conversely, the likelihood of negative impacts if particular information is withheld. However, it might be particularly difficult to convey this broader tradeoff information in a way that would be meaningful to a diverse range of credit applicants, and firms may also view such information as proprietary.[267]

266 On the latter topic, requiring that lenders disclose the aggregator's identity could be useful to the extent that it would enable consumers to connect publicly available news information to the security of their own data in the event that the aggregator is subject to a breach or to regulator action for lax practices. The case for such a requirement becomes stronger to the extent that aggregators retain and use consumer data after transmission. This benefit would have to be weighed against operational costs and complexity, however, as data sharing becomes more common and lenders establish multiple aggregation relationships or switch aggregation relationships periodically.

267 Such information might be particularly important where lenders are making affirmative marketing claims about their underwriting processes. More broadly, such information could be useful to applicants in deciding whether the tradeoffs in providing access to their cash-flow data (or withholding particular data) are warranted. However, it could be extremely difficult to convey such information that would be clear, meaningful, and accurate to a diverse range of credit applicants.

BOX 6.2.1.2 DISCLOSURE COMMUNICATIONS CHALLENGES

Although disclosure is used frequently as a customer protection tool, research over the last several decades demonstrates that it can be challenging to execute effectively. Both firms and regulators have come to rely more heavily on consumer testing to improve individual communications, but new challenges are emerging as the overall volume of disclosures and the range of delivery channels continue to increase. Relevant considerations include:

Plainer language, shorter disclosures: Disclosures that are short and that use plain language are generally more likely to be read by consumers and more effective in conveying content, but federal regulators have also found situations in which shorter was not better. For example, alternative wording may be needed where consumers' common understanding of particular terms does not match the way that the terms are used in specific laws or varies based on geography, firms' past usage of similar wording, or the consumers' familiarity with a particular topic.

Design and delivery channels: Testing suggests that design elements such as typographic distinctions, tables and charts, and shading can also increase the likelihood that consumers will read disclosures and in some cases can be more effective in conveying information than undifferentiated prose. But the effect of particular design elements may differ when they are viewed on paper, full computer screens, or mobile devices, and some design tools (such as the use of color) may not be practicable in all situations. A particular concern with online disclosures is whether and how consumers skim for key information, particularly where it takes multiple scrolls or clicks to access all content.

Choice architecture: Research suggests that a substantial number of consumers may make different choices depending on how a particular decision is presented to them, for instance whether it is structured as an "opt in" or an "opt out." Although federal agencies have historically tended to strive to present information in neutral ways that do not steer consumers in particular directions, this research suggests that that goal is difficult to accomplish.

Variations in personal and environmental factors: The ways in which consumers interact with particular disclosures depends not just on their content and design, but on consumers' own personal situations (e.g., their past experiences, their overall finances and preferences, whether they intend to engage in comparison shopping). As a result, standardizing disclosures can have many benefits but may also have tradeoffs for different groups of consumers. In additions, differences in the environment in which individual consumers are receiving and reviewing the information (e.g., whether firms present additional information at the same time, whether there are environmental distractions, and whether there are pressures to move ahead with a particular decision or transaction) can affect attention and comprehension in ways that are difficult to replicate in testing environments.

Cumulative effects: As the number of disclosure topics and consumer choices increase, it becomes more challenging to balance between consolidation versus separation and to measure cumulative impacts. For instance, even with regard to a single financial product or service, consolidating disclosures and choices in a single series or document may make it easier for consumers to concentrate on a sequence of key decisions and information, or it can make it more difficult for consumers to identify and concentrate on the particular issues that they are most concerned about.

These and other factors substantially complicate the process of designing and testing individual disclosures because there are so many potentially relevant considerations to take into account. They have also generated an increasing debate among stakeholders about the general risk of "information overload," the appropriateness of structuring information and choices to achieve particular policy outcomes, and the overall effectiveness of disclosure as a means of customer protection.

Sources: Peter Gordon Roetzel, Information Overload in the Information Age, 12 Bus. Research 479 (2019); Petra Persson, Attention Manipulation and Information Overload, Behavioural Public Policy 78-106 (May 2018); Heidi Johnson & Jesse Leary, Policy Watch: Research Priorities on Disclosure at the Consumer Financial Protection Bureau, 36 J. Pub. Policy & Marketing 184, 187–89 (2017); Omri Ben-Shahar & Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure (2014); Elizabeth Rosenthal, News Analysis, I Disclose ... Nothing, N.Y. Times (Jan. 21, 2012); Jeanne M. Hogarth & Ellen A. Merry, Designing Disclosures to Inform Consumer Financial Decisionmaking: Lessons Learned from Consumer Testing, Fed. Res. Bulletin (August 2011); Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions about Health, Welfare, and Happiness (2008).

Delivering this much content at the same time that applicants are attempting to shop for providers, evaluate prices and other basic product features, and complete the application process can be challenging both for lenders to execute and for applicants to absorb. These challenges are heightened where the application process is occurring via a smart phone screen. Such disclosures also have business process implications, particularly for online lenders who primarily receive digital applications and who compete in part on the ability to originate loans through faster and more streamlined processes. Many of these firms are reluctant to add "clicks" to origination processes because of concern that it will increase the number of abandoned applications. Yet particularly if the permissioning process is intended to substitute for back-end protections, slowing the process down may become increasingly important to ensure that applicants have a chance to absorb the information and exercise their rights.

Authorization and data review processes. As described in Section 4, authorizing data access through credential sharing and screen scraping is generally a take-or-leave-it process, since credit applicants cannot negotiate the scope of access defined in lenders' terms and conditions and do not have a practicable ability to restrict what aggregators can collect from their banks' websites. Depending on the configuration of the interface and the extent to which applicants read disclosures, applicants may not understand that they are providing their credentials to the aggregator or lender, let alone the scope of data access they have authorized.[268] Where tokenization and APIs have been implemented, credit applicants can restrict access to particular accounts or types of information, but it is unclear exactly what level of choice is being provided to consumers and small businesses.

Ensuring that applicants are clear about the parties with which they are dealing, the fact that they are providing credentials to a firm other than their bank, and the scope of the authorization that they have agreed to are fundamental to the concept of informed consent, and raise many of the same communications challenges discussed above.

A second issue concerns the practicality and policy ramifications of providing consumers and small businesses with much more granular control over what data is conveyed—for instance, the ability to withhold merchant identities and deposit sources, to select only certain transaction types to be transmitted, or even to edit at the individual transaction level. As a practical matter, that level of control may require additional technology and coordination mechanisms. As noted in Section 6.1.1.2, at least one aggregator has developed a dashboard that allows applicants to review their data before it is transferred to lenders or other end users, including checks for accuracy. But such features are not widespread in the marketplace today, and implementing individualized authorizations may require more extensive coordination between credit applicants and firms.

Such a system would also have potential ramifications for both firms and applicants. While the ability to tailor authorizations could allow consumers and small businesses to make more fine-grained decisions with regard to privacy and other considerations, it might also have a significant impact on the likelihood of success for their applications. As noted above, it may be difficult to position applicants to make informed decisions about the tradeoffs involved in excluding particular data elements. As discussed further in section 6.2.2, some stakeholders have also suggested that such a system would raise prudential concerns if applicants could edit their data selectively to create a misleading picture to lenders.

And while a wide variety of stakeholders have expressed enthusiasm for providing applicants with a chance to review their data before transmission, it is unclear in practice whether consumers and

268 Surveys by an organization representing the nation's largest banks found that only about 20 to 25 percent of fintech app users understand that apps or third parties may access information until the credentials are revoked. The Clearing House, Consumer Survey: Financial Apps and Data Privacy 3, 6 (2019); The Clearing House, Fintech Apps and Data Privacy: New Insights from Consumer Research 11 (2018).

small businesses would consistently detect material errors or omissions. Particularly given that they may not know what information is important to lenders in the first instance, it may be difficult to review several months' or years' worth of account transactions for accuracy, especially if applicants have time or device constraints or do not have immediate access to past records for comparison.[269]

Downstream elements. Positioning consumers and small businesses to exercise meaningful control over their data after the initial application process implicates a number of additional downstream processes. Other data sharing regimes and principles include such items as tools for monitoring subsequent use and transfer of the data, the ability to obtain copies of data as it is held by various companies for review and correction, processes for revoking or modifying consent to data access and compelling deletion, the availability of dispute resolution mechanisms, and potential prohibitions on discrimination or retaliation by firms where customers have exercise various control rights.

As discussed in Sections 5.2.2 and 6.1, laws such as FCRA and § 1033 of the Dodd-Frank Act provide some of these elements in connection with certain consumer financial products and services, but there are a number of outstanding questions and disputes about their current application to data shared for cash-flow underwriting. The policy considerations implicated by these elements may also be different in the credit context than for other data sharing use cases. For example, as noted in Section 6.1.2, the question about whether and when it is appropriate for lenders to condition an extension of credit based on some level of ongoing access to cash-flow credit for risk monitoring purposes raises complicated questions about prudential risk management, financial inclusion, and customer privacy that may not be likely to arise with payments or personal financial management use cases. And widescale data deletion might affect lenders' ability to use data for credit modelling.[270]

Providing appropriate and effective mechanisms for downstream control also depends on the availability of technological tools and inter-company communications. For example, it is substantially easier for banks to provide dashboards for consumer data monitoring and control once APIs have been implemented. And creating dashboards may be technically challenging for smaller institutions. Communications between different players in the system may also be important both to provide transparency and to execute customer instructions. For example, a bank or aggregator would not be able to provide transparency as to all parties that may have a particular customer's data without additional information from downstream recipients as to whether they in turn have provided the data to vendors, investors, or other additional parties.[271] And deletion instructions may need to be conveyed to downstream parties. Thus, a single firm acting alone—whether a data source, aggregator, or lender—likely cannot provide all of these features without cooperation from other companies. And to the extent that controls are structured in a way that depends on consumers or small businesses communicating directly with companies that hold their data but may not

269 In contrast, it may be easier for individual applicants to focus the scope of their data review after they have received an adverse action notice that alerts them to the principal reason(s) for the action, the data source, and other background information. However, as discussed in Section 6.1.1.2, such systems also have some disadvantages in that applicants only get an opportunity to pursue corrections after having already been subject to an adverse action or risk-based pricing.

270 Data deletion rights would also need to account for federal consumer financial laws that require the retention of documents for compliance and litigation purposes. For example, lenders are generally required under Truth in Lending Act to retain evidence of compliance with specific requirements for two years after the date that disclosures are made or the action is required to be taken, though regulators may require longer retention periods if necessary to carry out enforcement responsibilities. 12 C.F.R. § 1026.25(a).

271 In Europe, for example, companies report receiving fraudulent and spam requests for data access. In California, some consumers who attempted to exercise their new rights to access their data at particular companies have complained that they are being required to share large amounts of sensitive identifying information with additional vendors in order to complete the verification process. Alistair Barr, Fully Charged Newsletter, Come on a Trip to the New Privacy Circle of Hell, BloombergTechnology (Jan. 9, 2020); Catherine Stupp, Companies Scramble to Respond to Spam GDPR Requests, Wall St. J. Pro (Nov. 25, 2019).

otherwise have direct relationships with them, verification of identity can raise both practical and policy issues.[272]

There are also some tensions as between at least some banks and aggregators as to the best locus of communication with the consumer or small business. Banks argue they are the most logical location because customers always know to start with their existing banking relationship. Aggregators argue that they can provide a more consistent customer experience because of their scale across many banks and many fintechs and their ability to provide information about data collection that is occurring via screen scraping. In addition to questions about providing consumers and small businesses with effective and consistent mechanisms, the resolution of this question has important implications for the participants' ability to maintain and strengthen customer relationships over time.

In light of these various challenges, stakeholders are generally supportive of strengthening informed consent and other control mechanisms at a high level but have varying views with regard to the details of particular features, prioritization among different elements, and the overall likelihood of success in creating robust data control rights. As discussed in the next section, these differences are just one component of the broader debate over how customer control and customer protection should balance with each other in cash-flow underwriting and the broader system for customer-permissioned data flows.

6.2.2 Likelihood that customers will exercise meaningful control

Assuming that the practical challenges to creating robust control mechanisms can be overcome, stakeholders also disagree sharply in their predictions as to how consumers and small businesses would react to the provision of such features. This question is central to gauging both the potential efficacy of control mechanisms as a means of customer protection and the likelihood that customer control could create tensions with other policy goals, such as facilitating innovation or managing prudential risk. The debates center in large part on the so-called "privacy paradox" between customers' expressed preferences and actual practices in managing their personal data.

At one level, surveys and focus groups reflect high levels of concern about data privacy, security, and related issues among consumers and small business owners.[273] Privacy sensitivities appear to be even higher among racial and ethnic minorities and low-income respondents than the general population, while trust in government institutions and business organizations is lower.[274] Levels

272 In Europe, for example, companies report receiving fraudulent and span requests for data access. In California, some consumers who attempted to exercise their new rights to access their data at particular companies have complained that they are being required to share large amounts of sensitive identifying information with additional vendors in order to complete the verification process. Alistair Barr, Fully Charged Newsletter, Come on a Trip to the New Privacy Circle of Hell, BloombergTechnology (Jan. 9, 2020); Catherine Stupp, Companies Scramble to Respond to Spam GDPR Requests, Wall St. J. Pro (Nov. 25, 2019).

273 *See, e.g.,* Brooke Auxier et al., Americans and Privacy: Concerned, Confused, and Feeling Lack of Control over Their Personal Information, Pew Research Center (2019); Sam Sabin, Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year, Morning Consult (2019); SAS, Data Privacy: Are You Concerned? Insights from a Survey of US Consumers (2018); Lee Rainie & Maeve Duggan, Privacy and Information Sharing, Pew Research Center (2016). Research on small business owner attitudes about the privacy and security of their data as it is housed by financial institutions or other third parties is more limited, but suggests that entrepreneurs also are concerned about data protection issues. Lipman & Wiersch, Uncertain Terms at 23, 27; Barbara J. Lipman & Ann Marie Wiersch, Browsing to Borrow: 'Mom & Pop' Small Business Perspectives on Online Lenders, Board of Governors of the Federal Reserve System 12, 16-17 (2018); Barbara J. Lipman & Ann Marie Wiersch, Alternative Lending Through the Eyes of 'Mom & Pop' Small Business Owners: Findings from Online Focus Groups, Federal Reserve Bank of Cleveland 17 (2015).

274 Auxier et al. at 19 (reporting that African-American survey respondents were at least twice as likely as Hispanics or whites to have had someone use their name to attempt to take out credit and three times as likely to have someone take over their social media or email account in the past year); Mary Madden, Privacy, Security and Digital Inequality, Data & Society Research Institute 2-10 (2017) (reporting differentials in attitudes about privacy and information security risk based in a 2015 nationally representative survey of 3,000 adults); Mary Madden et al., Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans, 95 Wash. U.L. Rev. 53 (2017).

of concern about protecting financial and health data are particularly high relative to other types of information.[275]

Yet other studies that focus on consumers' actual behavior with regard to managing and protecting their own data reveal a much more complicated set of dynamics. Relatively small fractions of consumers read on-line privacy notices or take advantage of various types of privacy-enhancing tools and strategies, even in the financial services market.[276] And while some studies in the international context find that low-income consumers are willing to pay more and wait additional time for loans that come with heightened privacy protections,[277] other research suggests that many consumers are also quite willing to provide data in return for pricing discounts, more convenient processes, or other benefits.[278] Indeed, lab experiments have found that even participants who profess a high degree of concern about privacy often act in cavalier ways, for instance by providing their own personal data or the data of others for extremely modest renumeration.[279] Other research suggests that despite the fact that consumers say they generally want transparency and seek more information, they in fact are more likely to disclose information on less professional websites than on those that treat privacy and security issues in a more serious and detailed way.[280]

Stakeholders are deeply divided over the interpretation of this evidence as it applies to customer protection concerns. While many stakeholders agree that the steady drumbeat of large data breaches may be increasing feelings of helplessness among consumers and small businesses,[281] some stakeholders argue that the behavioral studies show that customers are quite willing to trade data

275 Accenture, 2019 Global Financial Services Consumer Study 10, 13, 16, 19 (2019); HIPAA Journal, Patient Privacy and Security Are Greatest Healthcare Concerns for Consumers, hipaajournal.com (Jul. 10, 2018); National Telecommunications and Information Administration, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (2016).

276 For general sources not specific to financial services, *see, e.g.,* Darrell M. West, TechTank, Brookings Survey Finds Three-Quarters of Online Users Rarely Read Business Terms of Service, Brookings Institution (May 21, 2019); Alfred Ng, Blog, Microsoft Wants a US Privacy Law That Puts the Burden on Tech Companies, CNET (May 20, 2019); Jonathan A. Obar & Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, Information, Communication & Society 1-20 (June 2018); Caroline Cakebread, You're Not Alone, No One Reads Terms of Service Agreements, Business Insider (Nov. 15, 2017); Aaron Smith, FactTank, Half of Online Americans Don't Know What a Privacy Policy Is, Pew Research Center (Dec. 4, 2014).

277 Marian Fernandez Vidal & David Medine, Focus Note, Is Data Privacy Good for Business?, Consultative Group to Assist the Poor (2019) (reporting results of experiments in India and Kenya).

278 For examples involving credit specifically, *see, e.g.,* Mekebeb Tesfaye, Financial Service Consumers Are Willing to Share Their Personal Data for Benefits and Discounts, Business Insider (Mar. 18, 2019) (reporting results of an international Accenture survey reporting that 81 percent of survey respondents were willing to share additional data with banks for faster and easier loan approvals); Experian, The State of Alternative Credit Data at 14 (reporting that 70 percent of US consumers surveyed in a 2018 study indicated that they were willing to share additional financial information to a lender if it increases their chance of approval or improves the price of a loan).

279 Accenture at 32; Susan Athey et al., The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, National Bureau of Economic Research Working Paper No. 23488 (June 2017); Rainie & Duggan; Leslie John, We Say We Want Privacy Online, But Our Actions Say Otherwise, Harvard Business Review (Oct. 16, 2015); Joseph Turow et al., The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, University of Pennsylvania (2015); Sarah Spiekermann et al., E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior, EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce 38-47 (2001).

280 *See, e.g.,* Leslie K. John et al., Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information, J. of Consumer Research (February 2011).

281 According to one report, only 6.5 percent of all breaches that were reported in 2019 were suffered by financial services firms, but those breaches involved 61.7 percent of all leaked records. Bitglass, The Financial Matrix: Bitglass' 2019 Financial Breach Report 4 (2019) (using data from the Identity Theft Resource Center and Ponemon Institute); Identity Theft Resource Center, 2018 End-of-Year Data Breach Report (2019). Indeed, several large breaches over the last several years have involved financial firms—including the 2019 Capital One breach (100 million U.S. consumers), the 2017 Equifax breach (143 million U.S. consumers), and the 2014 JPMorgan Chase breach (76 million households and 7 million small businesses)—and several others have involved theft of credit and/or debit card data from merchants or processors. Matthew Goldberg, 10 of the Biggest Data Breaches over the Last Decade, Bankrate.com (Dec. 17, 2019). For studies and surveys reflecting impacts of recent breaches on consumer and small business attitudes about managing privacy risks, *see, e.g.,* Auxier et al.; Lipman & Wiersch, Browsing to Borrow at 12, 16-17; Ping Identity, 2018 Consumer Survey: Attitudes and Behavior in a Post-Breach Era (2018); PwC, Consumer Intelligence Series: Protect.me (2017).

BOX 6.2.2.1 CUSTOMER BEHAVIOR PATTERNS CONCERNING FINANCIAL DATA

Although surveys indicate that consumers are particularly concerned about the privacy and integrity of their financial data, the data that is available is mixed as to their actual behavior and level of awareness about particular data issues.

For example, annual surveys indicate that the proportion of consumers that check their credit scores rose from approximately 43 percent in 2012 to a peak of 57 percent in 2018 before dropping slightly the following year. The percentage of consumers who checked their full credit report has also been increasing, from 29 percent in 2014 to 36 percent in 2018. Yet survey responses suggest that consumers' level of knowledge about credit scoring has actually been declining over the same period, even though their confidence in their knowledge has increased. For example, the number of respondents who stated that it was important to check credit reports declined from 82 percent in 2012 to 67 percent in 2019.

Recent statistics on the number of consumers who read privacy notices that are required under the Gramm-Leach-Bliley Act or who exercise their right to opt out of certain types of information sharing between companies under GLBA are not available. Opt out rates were reported as between 1 and 10 percent during initial implementation. Reports regarding opt outs for certain affiliate marketing under FCRA are generally similar, though some individual companies have reported numbers as high as 30 percent.

A 2019 survey by The Clearing House on consumers' use of financial applications indicate that 79 percent of respondents reported that they had not read all of the terms and conditions for the financial apps that were asked about. About 80 percent of respondents were not fully aware that financial apps had access to their bank account, and about 20 percent understood that the apps' access to their data would continue until they revoked their credentials.

Sources: VantageScore, Press Release, Annual Survey Reveals that Consumer Knowledge about Credit Scores Has Steadily Declined Over the Past Eight Years (June 10, 2019); Consumer Federation of America, Press Release, Survey Shows an Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores (June 18, 2018); Senate Committee on Banking, Housing, and Urban Affairs, Hearing, The Fair Credit Reporting Act and Issues Presented by Reauthorization of the Expiring Preemption Provisions 338 (2008) (written responses of Martin Wong); Senate Committee on Banking, Housing, and Urban Affairs, Hearing, Financial Privacy and Consumer Protection, 9, 60 (2002) (testimony of Fred H. Cate and John C. Dugan); W.A. Lee, Opt-Out Notices Give No One a Thrill, Am. Banker (July 10, 2001); The Clearing House, Consumer Survey at 3, 5-6.

access for product benefits and that robust customer control mechanisms would be sufficient to allow the minority of applicants who feel differently to protect their data.[282]

Other stakeholders view the results at least in part as the product of poor choice architecture, overly legalistic disclosure documents, and general information overload within existing consent regimes, suggesting that better design would reveal consumer preferences that are more consistent with survey data and empower more active data management.[283] And some argue that the evidence demonstrates the limitations of relying on customer control as a protection regime, given the practical

282 Some sources also note that disclosures can have market impacts in certain circumstances even if large numbers of consumers do not read or use the information. For example, such effects may occur where competitors, regulators, or advocates pay attention to disclosures even if many individual consumers do not, where firms are particularly focused on the "informed minority" of consumers who are most likely to act based on the disclosures, or because intermediaries use the disclosures to assist consumers in decisionmaking. However, the extent to which these circumstances occur in practice is fiercely debated in the broader literature on consumer disclosure, Ben-Shahar & Schneider; Yannis Bakos et al., Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts, 43 J. Legal Studies 1 (2014); Thomas A. Durkin, Credit Card Disclosures, Solicitations, and Privacy Notices: Survey Results of Consumer Knowledge and Behavior, Federal Reserve Bulletin (2006), and critics argue in any event that there is little evidence of these kinds of dynamics to date with regard to data sharing, privacy, and related topics.

283 Fernandez Vidal & Medine at 7 (noting that experiment results changed when consumers were not given or did not perceive themselves to have a choice that offered higher privacy protections); Dan Svirksky, Why Are Privacy Preferences Inconsistent?, John M. Olin Center for Law, Economics, and Business, Fellows' Discussion Paper Series No. 81 (June 2018) (finding experiment results were sensitive to choice architecture); John et al. (reporting experiment results suggesting that privacy decisions are sensitive to environmental cues). One study in 2008 calculated that U.S. residents encounter an average of 1462 privacy policies per year, representing costs in time of approximately 244 hours and $3534 per internet user. Aleecia M. McDonald & Lorrie Faith Cranor, The Costs of Reading Privacy Policies, I/S: A Journal of Law & Policy for the Information Society, vol. 4, issue 3 (2008).

challenges that consumers and small businesses face with regard to making complex tradeoffs as data sharing fuels a growing range of financial products and services.[284]

The debates about how consumers and small businesses would respond to a more robust suite of data rights also have important implications for the interaction between customer autonomy and control with other policy objectives. For example, the extent to which applicants would actually edit their data or request deletions would affect the degree of concern that lenders could get a distorted picture of individual applicants' finances or have less representative data available overall for credit modelling.[285]

6.2.3 Options going forward

These considerations demonstrate why developing effective ways to strengthen customer control and deciding what role control should play in the broader marketplace are some of the most complex and far-reaching policy questions raised by cash-flow underwriting and customer-permissioned data flows more generally. Enhancing customers' ability to control their own data is both intuitively appealing and practically necessary to respect personal autonomy and choice, empower consumers and small businesses to realize greater benefits from their own data, and increase inclusion, competition, and innovation across the broader marketplace. Yet the research and examples cited above suggest that customer control also has substantial limitations as a tool for managing customer protection risks, and depending on implementation details could present tradeoffs for achieving other policy objectives and/or cut against the desire by both customers and firms for simple and efficient procedures.

Thus, although stakeholders' rhetoric about the transformational potential of customer control can become quite sweeping at times, it is not a simple solution to many of the policy issues outlined above. Some protection issues are not suited to management through individual customer choice in the first instance because assessment of the particular risks requires access to types of information and evaluation techniques that individual customers do not have.[286] And even for other issues, the more risks that consumers and small businesses are required to manage and the more options they are required to evaluate, the harder it becomes to achieve informed consent and to avoid potentially negative outcomes. Particularly to the extent that a large number of risk mitigation decisions are bundled into a single take-it-or-leave-it authorization at the time of credit application, increasing customer control could potentially decrease rather than enhance customer protection.

These considerations suggest that while industry efforts to foster informed consent and more meaningful control mechanisms over the life of the credit relationship are encouraging, supplementary action by policymakers is likely to be needed to calibrate the broader relationships between data rights and data protections, to balance customer interests in autonomy and control with other policy considerations in the credit context, and to overcome obstacles to coordination and consistency in the marketplace. Even some stakeholders who argue for using customer control

284 David Medine & Gayatri Murthy, Focus Note, Making Data Work for the Poor: New Approaches to Data Protection and Privacy, Consultative Group to Assist the Poor (2020); Lauren Saunders, Fintech and Consumer Protection: A Snapshot, National Consumer Law Center 6-7 (2019).

285 An additional consideration with regard to concerns about potentially incomplete cash-flow data is the extent to which lenders are able to crosscheck other data sources, seek additional information where needed, and/or adjust risk forecasts where available information is not sufficiently complete to be reliable. Lenders already have to make these kinds of decisions today when underwriting borrowers who have thin traditional credit files or determining whether to verify supplemental sources of income in the mortgage context. And given that some types of data sources report negative but not positive information, traditional credit reports are more likely to be missing positive payments history than negative history. See Box 2.1.1, notes 43 and 46 (discussing the nature of cash-flow information and the likelihood that underserved borrowers maintain multiple transaction accounts).

286 These include issues such as fair lending, unfair and abusive practices, and information security practices.

BOX 6.2.3.1 REEXAMINING THE SCOPE AND STRUCTURE OF LEGITIMATE PURPOSE RESTRICTIONS

As concerns about "consent fatigue" grow, some stakeholders both in the U.S. and globally have begun discussing ways to re-define the scope of legitimate data collection, use, and processing by law and the relationship between such legitimate purpose tests and customer consent more generally.

Several regimes treat consent and some version(s) of a legitimate purposes test as alternative grounds for permissible use. For example, as discussed in Box 5.2.2.1.1, Europe's General Purpose Data Regulation provides multiple bases for collecting and using customer data, including both situations in which a firm has explicit consent from the data subject and situations in which the processing is necessary for the legitimate interests of the organization and those interests are not overridden by the interests or fundamental rights of the data subject. In the U.S., the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act both define certain activities as permissible by law without the need for consumer consent, as well as providing additional "catch all" provisions that permit additional activities with consumer authorization.

However, particularly where the scope of a particular legitimate purposes test is unclear, this may prompt firms to obtain consent even where they do not in fact need it to provide a backstop against liability or in an effort to improve customer relations.

Different stakeholders have reacted to this dilemma in different ways. For example, some European officials have begun emphasizing that consent is not a "silver bullet" for GDPR compliance and emphasizing alternative grounds in particular circumstances as a way of combatting consent fatigue. In the U.S., some members of the Federal Trade Commission have begun advocating for scaling down reliance on notice-and-choice regimes in favor of limiting data collection to align with consumers' reasonable expectations.

A 2020 white paper by the Consultative Group to Assist the Poor argues for a similar approach in developing markets where underserved populations are joining the formal financial system for the first time and face particular literacy, language, and technology barriers. Specifically, the paper advocates for either (1) a legitimate purposes test that restricts data use to what is necessary or compatible with the initial delivery of products or services; or (2) a fiduciary duty requirement that permits firms to use data only in ways that are in the interests of the affected consumers. Under either standard, consent would not be permitted to override the restrictions and obligations, even if it is required to authorize data access and use for purposes of the primary product or service sought by the consumer.

One of the challenges with defining legitimate purposes tests in connection with customer expectations is defining what types of forward-looking research and product development activities are permissible, for instance under a standard that looks to the reasonable expectations of consumers. Some sources have distinguished between making improvements to the same basic type of product or service versus using data for a completely different purpose, or providing greater flexibility for use of anonymized data in order to promote innovation and research.

Sources: Medine & Murthy; Saunders, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology at 12-13; Caitlin Chin & Maria Odell, TechTank, Highlights: Commissioners Discuss the Future of the FTC's Role in Privacy, Brookings Institution (Nov. 5, 2019); Luis Alberto Montezuma & Tara Taubman-Bassirian, How to Avoid Consent Fatigue, International Association of Privacy Professionals (Jan. 29, 2019); United Kingdom Information Commissioner's Office, When Can We Rely on Legitimate Interests?, ico.org.uk (visited Feb. 8, 2020); Elizabeth Dunham, Blog, Consent Is Not the 'Silver Bullet' for GDPR Compliance, ico.org.uk (Aug. 16, 2017).

mechanisms in lieu of prescriptive protections agree that some regulatory action may be needed to effectuate a more robust customer control regime in the first instance.

In resolving these issues, policymakers (and to a certain extent, industry actors) have a number of tools for making customer control more effective. As discussed above, moving away from reliance solely on one-time blanket consent is a critical first decision. Structuring rights and establishing dashboards, dispute resolution mechanisms, and other tools that provide consumers and small businesses with ongoing transparency about the use of their data and the ability to protect their interests in different stages of the credit relationship would be a substantial step toward empowerment.[287] Where informed consent is critical to a particular topic, research and historical examples suggest that

287 Examples include providing mechanisms for applicants to monitor data sharing patterns over time and revise or revoke further data access, or requiring re-authorization after a specified time period in general or a specified period of inactivity as a prompt for the consumer or small business to confirm whether further data access or use is warranted.

streamlining both the number of issues and the options presented can be helpful rather than requiring borrowers to assess a varying range of practices or alternatives each time that they apply for a loan or other financial product.[288] Some stakeholders have also suggested that creating new types of intermediaries to act solely on behalf of consumers or small businesses in managing their data rights and decisions could also be useful.[289]

As discussed in Sections 5 and 6.1, federal regulators have the authority to begin enhancing customer control mechanisms in a variety of ways, such as improving disclosures, providing more guidance concerning the operation of exceptions to the Fair Credit Reporting Act and Gramm-Leach-Bliley Act that allow data use or sharing beyond the bounds otherwise permitted by statute, implementing the consumer rights provided by section 1033, and determining the extent to which FCRA dispute resolution procedures apply to transfers of cash-flow data for credit underwriting purposes, and similar actions. Clarifying the application of existing laws could also potentially simplify the number of customer protection issues that are managed through customer control mechanisms. However, other customer control mechanisms and recalibrating the broader balance between data rights and data protections would depend on action by Congress.

6.3 Long-term concerns about market evolution

Stepping back from the more specific debates about individual risks and mitigation tools, some stakeholders have raised concerns that cash-flow underwriting could eventually become so ubiquitous that consumers and small businesses will have no practicable alternative but to provide such information to lenders even if lenders begin to use it in ways that heighten privacy tradeoffs and other risks. Others have asked a slightly narrower version of the same question about the policy implications if large numbers of underserved borrowers are effectively forced to begin providing cash-flow information on a routine basis, while prime borrowers continue to be underwritten based largely on traditional consumer reports.

The likelihood of either of these scenarios is difficult to predict at the current stage of the market, when there are so many unanswered questions about the relative utility of the data in particular contexts, the resolution of various obstacles to its broader adoption, and the extent to which various business practices and policy tools can be used to mitigate potential customer protection risks. As discussed further in Section 7, the ways in which industry actors, regulators, and Congress engage with credit and data transfer markets over the next few years will have important impacts on whether cash-flow underwriting achieves its potential to foster a more inclusive, efficient, and competitive marketplace or begins to evolve in ways that heighten tradeoffs and risks for credit applicants.

And while it is natural to begin experimenting with cash-flow underwriting in contexts where the benefits are the most obvious relative to the risks and uncertainties, there could also be some disadvantages to constraining its use too narrowly and prematurely. For example, while it is not surprising that many initial cash-flow pilots are being structured as second look programs to consider only candidates who have been rejected using traditional information sources, there could

288 An example of limiting the issues presented might involve using protective measures to resolve secondary or downstream issues that credit applicants are less likely to focus substantial attention on anyway, such as the data use practices of vendors and aggregators who may facilitate the underwriting process. An example of limiting the alternatives presented might be to define standardized levels of account data access, such as (1) only aggregated account balances and de-identified deposit and expense information; (2) the same information plus payment history on recurring obligations; or (3) full transaction level detail.

289 Geoffrey A. Fowler, How We Survive the Surveillance Apocalypse, Wash. Post (Dec. 31, 2019); David Maher, The Trusted Intermediary Model: Supporting Both Privacy and Internet Services, International Association of Privacy Professionals (visited Feb. 8, 2020); Geoff Mulgan & Vincent Straub, The New Ecosystem of Trust, Nesta (Feb. 21, 2019); Richard Whitt, To Fix the Web, Give It Back to the Users, Fast Company (Jan. 22, 2019).

be potential risks to limiting the use of cash-flow information solely to second-look and "credit invisible" populations. For example, such applicants may be the least likely to be able to protect their own interests with regard to the scope of particular data requests or product terms precisely because they may have few practicable alternatives.[290] And there may be less general public urgency to design safeguards to reduce risk levels in such circumstances, both because the number of affected applicants would be smaller and because the benefits seem so obvious.

Thus, particularly given evidence suggesting that cash-flow data may be valuable for a broader swath of applicants, fostering further reasonable experimentation, research, and market monitoring are important to continue developing a deeper understanding of both the potential benefits and risks of cash-flow underwriting as the market continues to evolve. Resolving some of the outstanding interpretive issues particularly with regard to underlying data flows could also be helpful to reduce potential risks to consumers. The warning to step back periodically to consider the overall cumulative tradeoffs and impacts is an important one, particularly given the complex and interwoven issues facing consumers and small businesses in the cash-flow context.

290 Indeed, stakeholders have noted in the Fair Credit Reporting Act context that where the statute does require consumer permission to access consumer reports for certain employment purposes, the permissioning regime does not in practice provide substantial empowerment to job candidates because their applications are generally rejected if they decline to authorize reports to be provided.

7. POLICY ANALYSIS

Particular Considerations for Industry, Regulators, and Congress

The complex and interlocking nature of the policy issues presented by cash-flow underwriting will likely require sustained engagement by private stakeholders, regulators, and Congress to resolve. Although it may be tempting for each group to wait for action by some other party, there could be substantial opportunity costs to inaction with regard to efficiency, competitive dynamics, access to credit, and customer protection. Greater engagement by regulators in the near term could be particularly important to helping make industry and Congressional initiatives more effective and more likely to succeed.

As discussed above, there are some signs that cash-flow underwriting and in particular the new data transfer system are reaching the stage at which some level of consistency concerning the scope of data, transfer technologies, and business practices could fuel greater efficiency and better risk mitigation for borrowers.

Yet while market actors are already working to address some of these issues, there are limits to what they can accomplish alone. Market-led standards can be complicated by competitive dynamics and frustrated by the lack of effective accountability mechanisms. And given outstanding questions about the application of existing laws and guidance, increasing the certainty and consistency of legal frameworks could help both firms and borrowers be more confident in structuring their own activities. Thus, while policymakers are often reluctant to intervene too early with regard to emerging innovations for fear of chilling the market, the policy issues discussed in Sections 5 and 6 help to highlight the fact that a lack of standards and regulatory clarity can have important implications for scaling innovation and for market structure.

This section explores some of the sequencing and strategic issues faced respectively by industry, regulators, and Congress in addressing critical policy challenges concerning cash-flow underwriting and related data transfers. Given the challenges facing each group and the complex and interlocking nature of the policy issues presented, the section concludes that it may be particularly important for regulators to begin ramping up their level of engagement in the near term.

7.1 Industry actions

As discussed in Sections 3.2, 5.2, and 6.2, industry actors have a critical role to play in answering remaining research questions about the usefulness and limitations of particular cash-flow data in credit underwriting and servicing. To the extent that this research is made publicly available, it can help to shape the ways in which secondary market investors, regulators, and borrowers respond to market evolution and to various policy issues discussed above.

The second major need is for development and implementation of best practices, voluntary standards, and consistent technologies for data use, sharing, and protection. For example, various groups of stakeholders are calling for greater standardization on the following topics:

- Consistent standards for data transmission technologies between firms in order to reduce technology and coordination costs and mitigate accuracy, information security, and other disadvantages and risks of credential sharing and screen scraping.
- Consistent standards for the scope of data transferred for credit underwriting and/or other use cases, as well as for technical formatting. Depending on the decisions made, such standardization could be used not just to increase transmission efficiency but to balance privacy and predictiveness concerns.
- Consistent information security expectations for aggregators and end users, as well as better business-to-business mechanisms for investigations, liability resolution, and other matters in connection with misuse of credentials and/or data breaches in order to provide greater certainty to all market actors and reduce investigation and coordination costs.
- Best practices for creating and handling of anonymized data.

Where such voluntary measures can lower coordination costs, reduce the risk of unexpected and potentially catastrophic liability, and minimize the need for regulatory intervention, there may be strong market incentives to support adoption. As discussed in Section 5.2.2.2, there is a particular interest among some stakeholders in expanding the focus of current cross-industry discussions to concentrate more attention on such issues as tokenization, industry-wide data security standards, traceability, and other business-to-business mechanisms for managing liability issues, similar to what has evolved in the payments industry over time.

At the same time, the history of self-governance efforts in the traditional credit reporting system as discussed in Section 2.1 helps to illustrate that adoption of voluntary industry standards on certain topics can be substantially complicated by competitive interests and difficulties in coordinating consistent compliance across companies.

One of the most challenging issues for industry to solve for itself in the cash-flow underwriting context concerns questions about the scope of data access. As discussed in Section 6.1.3, the concept of "data minimization" generally holds that firms should only collect what information is reasonably necessary to provide the products that customers have contracted for, use the information in ways that customers would reasonably expect, and dispose of the information as quickly as practicable in light of record retention requirements and other considerations. A number of individual firms, industry organizations, and federal agencies have endorsed some or all of these concepts at a high level as a general good business practice to reduce privacy and security risks.[291]

291 *See, e.g.*,CFPB, Data Sharing Principles at 3; Federal Trade Commission Staff Report, Internet of Things: Privacy & Security in a Connected World iv, 33-39 (2015); American Bankers Association, Statement for the Record; Financial Data Exchange, Organization Overview at 6-7.

Yet as discussed in Section 6.1.1.1, defining specific boundaries is particularly challenging in the credit context, in part because of the open research questions regarding the value of particular cash-flow variables for predicting default risk and model development, responsible servicing and collections practices, and other issues.[292] In addition, because data has become a growing source of competitive advantage in the market and costs relatively little to store and use, there can be strong financial incentives for firms to retain as much information as possible, even where data may not have an immediate commercial use.

Thus, while the industry efforts to move toward safer and more efficient technologies are encouraging, there are substantial questions as to the scope of those efforts and their ability to balance competing interests between different market segments, consumers and small business applicants, and broader policy considerations. And even if self-governance initiatives are successful, many industry stakeholders believe that complementary regulatory or legislative efforts are also needed to produce more efficient and beneficial outcomes, particularly by resolving outstanding questions about the application of existing law.

7.2 Regulatory levers

Greater engagement by federal regulators could be helpful in managing several policy concerns with regard to cash-flow underwriting and underlying data flows. For some topics, increased research and monitoring activities may be the most useful immediate step to determine how business practices are evolving and how different options might help mitigate risks if and when they manifest in the market. In other areas—particularly with regard to underlying data flows—greater regulatory certainty could potentially help borrowers, firms, and Congress structure their own activities with more confidence.

Research and monitoring: As noted above, baseline research into such questions as the utility of particular cash-flow variables for specific products and populations, error rates at different stages of data transfer and processing, the potential benefits and risks of using cash-flow data in the servicing context, and consumer disclosure testing would help to inform both regulators and the broader market in addressing a range of potential policy issues as affected markets continue to evolve. While industry is working on some of these questions, there would be substantial value in additional research by federal regulators.

Increasing supervision activities could also be invaluable because examinations would provide both deeper and more consistent insights as market practices continue to evolve and a way to remedy any compliance violations relatively quickly and before they become entrenched in market practice. For instance, the Consumer Financial Protection Bureau could begin examining non-banks that are "larger participants" in markets for consumer lending, data aggregation, and model development once it issues rules to define the relevant size thresholds.[293] Both the CFPB and the banking agencies could step up examinations of fintech platforms, aggregators, and model developers that

292 Indeed, some stakeholders have suggested that the concept of minimization should not be applied in the credit context to the extent that it would prevent lenders and model developers from obtaining data to improve the predictiveness of their models on an ongoing basis. Defining the data that is useful for other use cases such as personal financial management services may also be challenging as products and services continue to evolve.

293 As discussed in Section 4.1.2 and 4.2.3, banks and credit unions have long been subject to federal agency supervision both for safety and soundness and for compliance with federal consumer financial laws. In 2010, the Dodd-Frank Act vested the Consumer Financial Protection Bureau with authority to examine non-bank "larger participants" in particular markets for consumer financial products and services after defining particular markets' thresholds by rule. The CFPB has issued a rule for consumer reporting markets, but it has not clarified whether data aggregators are subject to that rule or constitute a distinct market. It also has not set larger participant thresholds in the unsecured consumer credit markets where cash-flow underwriting is being used most extensively.

BOX 7.2.1 INCREASING INTEREST IN SUPERVISION OF DATA INTERMEDIARIES

Interest in the ongoing supervision of data intermediaries has been increasing since the 2017 Equifax breach, which affected nearly half of U.S. adults. As discussed in Box 4.1.2.1, the Consumer Financial Protection Bureau has supervised the nationwide consumer reporting agencies for compliance with most federal consumer financial protection laws since 2012. However, it lacks authority to examine any entities for compliance with Gramm-Leach-Bliley Act information safeguards requirements, though it has sometimes used its authority to prevent unfair, deceptive, and abusive acts and practices as a basis for acting on information security issues.

The Federal Trade Commission has enforcement authority over a wide range of non-bank financial institutions for violations of GLBA safeguards requirements, but not examination authority. And federal banking regulators have reportedly stated that they lack jurisdiction over consumer reporting agencies under the Bank Services Company Act, although they have exercised such jurisdiction over at least one data aggregator for purposes of cybersecurity and other examinations.

In the aftermath of the breach, the CFPB began conducting targeted data security and cybersecurity investigations. However, a 2019 Government Accountability Office report indicates that the Bureau is not specifically prioritizing its supervision activities with regard to consumer reporting agencies based on information security related risks. Legislation to subject nationwide CRAs to consistent data security examinations has been introduced in Congress.

Similar to the role played by consumer reporting agencies in the traditional credit system, some stakeholders have noted that data aggregators' intermediary role in the customer-permissioned data transfer system makes them attractive targets for hackers and fraudsters because they may have more information than individual banks or lenders. In addition, some sources have raised concerns that aggregators are being targeted by parties who are committing takeovers of consumers' accounts and create "synthetic identities" for purpose of fraud. The pending legislation does not specifically address supervision of aggregators, although as discussed in Section 6.1.1.2 there is a fierce debate over whether they are consumer reporting agencies under FCRA when they transfer data for credit-related purposes.

Sources: Victoria Guida, Banks, Fintech Startups Clash over 'the New Oil'—Your Data, Politico (Feb. 7, 2020); Verhage & Metcalf; Crosman, Data War?; Roy Urrico, Aggregators Banned From NCR's Digital Banking Platform Amid Account Takeovers, Credit Union Times (Nov. 6, 2019); Penny Crosman, Data Aggregators Push Back on the Notion They Have a Fraud Problem, Am. Banker (Sept. 30, 2019); Brendan Pederson, Bad Actors Targeting Fintech Aggregators: Fincen Chief, Am. Banker (Sept. 24, 2019); Brian Krebs, The Risk of Weak Online Banking Passwords, krebsonsecurity.com (Aug. 5, 2019); U.S. Government Accountability Office, Consumer Data Protection at 24-29; U.S. Government Accountability Office, Data Protection at 8-9, 25-27; Penny Crosman, Is Finra's Dire Warning about Data Aggregators on Target?, Am. Banker (Apr. 9, 2018); Kate Berry, Is CFPB Punting on Equifax? It's Complicated, Am. Banker (Feb. 5, 2018); Envestnet/Yodlee, Comment Letter to Enhanced Cyber Risk Management Standards, Docket OCC-2016-0016 (Feb. 17, 2017); Hope.

provide third-party services to entities under their primary jurisdiction.[294] Some stakeholders have also argued that the Bureau could obtain jurisdiction over all aggregators by invoking finding that they are engaged in activities that pose risks to consumers.[295]

Although federal agencies' ability to supervise non-bank actors for compliance with GLBA information safeguards requirements is limited to situations involving third-party service providers to banks, some bank and non-bank stakeholders have both suggested that increasing supervision would still be generally helpful to building greater trust and clarifying regulators' expectations within the broader data-transfer system. Some stakeholders have suggested that subjecting supervised non-bank entities to registration requirements could also increase trust, similar to what the

294 The Bureau also has direct authority to examine service providers to a substantial number of banks with less than $10 billion in assets. 12 U.S.C. § 5516(e). Service provider examinations are limited to the scope of activities performed on behalf of supervised entities. However, given that information security safeguards are often adopted on an entity-wide basis, such examinations could still be particularly helpful with regard to GLBA safeguards compliance since neither the CFPB nor the FTC can examine non-banks on that topic. The federal banking agencies reportedly disavowed authority over traditional consumer reporting agencies under the Bank Service Company Act, but they have subjected at least one data aggregator to an examination as a third-party service provider to banks. See Section 5.2.2.2 and Box 7.2.1.

295 Statement by Becky Heironimus, Capital One Financial Corporation, for the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records (Feb. 18, 2020) (citing 12 U.S.C. § 5514(a)(1)(C).

United Kingdom requires for firms that receive data from banks pursuant to its open banking initiative as discussed in Box 5.2.2.1.1.[296]

Providing regulatory certainty: While research and monitoring may be a helpful first step concerning the potential for evolution toward problematic uses of transaction data in behavioral models or servicing and collections practices, there are other topics for which issuing regulatory guidance and standards in the relative near term could substantially reduce uncertainty, frictions, and/or risks in the current market. Indeed, increasing supervision activities would likely increase the urgency of resolving certain outstanding interpretive issues given that examiners and firms need to know what requirements apply.

The need for regulatory guidance appears most acute with regard to the system for customer-permissioned data flows, which has been evolving for more than two decades and has been subject to particularly acrimonious policy debates in the last few years. Failing to resolve outstanding questions about compliance requirements and liability is creating a situation in which consumers' right to access their own data as recognized by Congress in 2010 is being impeded by a lack of clear standards to govern the data flows and the relationships of affected firms. Banks are understandably concerned about security and liability risks, but the fact that the system still has not transitioned away from credential sharing underlines the challenges of relying on industry to solve these issues solely on its own volition.

The Federal Trade Commission's rulemaking to clarify and strengthen information safeguards expectations for non-bank financial institutions under the Gramm-Leach-Bliley Act is a helpful step toward greater certainty and consistency. The Consumer Financial Protection Bureau could provide substantial additional certainty by issuing guidance or rules to implement § 1033 of the Dodd-Frank Act, resolving outstanding questions about liability under the Electronic Fund Transfer Act, deciding whether and how the Fair Credit Reporting Act applies to customer-permissioned data transfers for credit purposes, and/or clarifying the application of GLBA restrictions on data sharing in the data aggregation context.[297]

Stakeholders disagree as to the prioritization between these possible elements and the potential risks that agency deliberations on particular topics would chill self-governance initiatives. Yet they widely agree that greater regulatory certainty on at least one or more of these topics would substantially benefit the market. That is not to say that regulatory initiatives would resolve all outstanding questions or satisfy all stakeholders. To take just one example, because EFTA focuses primarily on the liability of consumers relative to the financial institutions that provide them with accounts, resolving liability for unauthorized account activities that occur as a result of consumers sharing their login credentials with an aggregator is not likely to settle questions about a bank's ability to recover any losses from downstream firms.[298] And depending on the outcome, there is a risk of constraining data sharing activities, either by causing consumers to become more concerned

296 The Bureau has authority to impose recordkeeping and registration requirements on non-banks that are subject to its supervision authority, including background checks and bonding or other appropriate financial requirements. 12 U.S.C. § 5514(a)(1), (b)(7).

297 One aspect of GLBA (and FCRA, to the extent that it is deemed to apply) that may warrant careful consideration is the operation of the provisions that allow for certain data sharing or use beyond what is otherwise permitted by the statute(s) where a consumer has provided affirmative consent. Given the increasing use of authorizations for data transfer, these provisions are taking on increased significance that may not have been contemplated by regulators in earlier rulemakings. As discussed in Box 6.2.1.1, regulators have provided relatively little guidance regarding the operation of these provisions or the other compliance obligations of firms that obtain data pursuant to those provisions.

298 15 U.S.C. § 1693g. Financial institutions are defined as banks or other persons that (1) directly or indirectly hold an account belonging to a consumer, or (2) issue an access device and agree with a consumer to provide electronic fund transfer services. *Id.* § 1693a(9); 12 C.F.R. § 1005.2(i). Where the latter type of electronic fund transfer service provider is involved, the regulation and official interpretations do address compliance and liability responsibilities as between the account-holding financial institution and the EFT service provider. 12 C.F.R. § 1005.14; *id.* Supp. 1, cmt. (b)-1. However, liability as between different business parties in the payments system is generally governed by contract and network or association rules rather than by federal law. See Box 5.2.2.2.2.

about the consequences of credential sharing or by strengthening banks' concerns about releasing information that could be used to conduct unauthorized activity (at least in the absence of clarity about § 1033 requirements). Such interconnections between issues may argue for a policy process that considers the issues identified above together, although that could affect the resources and timelines for resolution.

Nevertheless, failing to resolve these questions is increasing the stakes and potential transition costs of eventual interpretive decisions as the amount of data sharing continues to increase. And there may be ways in which beginning a serious policy analysis and regulatory process could yield substantial benefits even prior to the issuance of any final guidance or rule. For instance, some stakeholders have suggested that knowing that an interpretive initiative is underway would cause firms to approach industry standardization discussions in a different and more focused posture. Beginning work in the near term would also better position the CFPB to fill gaps more quickly if industry self-governance efforts ultimately prove unsuccessful or inadequate, as well as to alert Congress if there are situations in which a statutory solution to a particular policy issue may be needed. For example, if the CFPB decides that FCRA does not apply and/or cannot be adapted in appropriate ways to govern cash-flow data that is transferred by aggregators for credit purposes, then the onus may shift to Congress to provide any needed accuracy protections and use restrictions.[299]

Thus, given the interwoven and complex nature of the issues and the potential stakes involved, there are substantial arguments for launching CFPB processes to resolve the outstanding interpretive questions noted above. Although federal prudential regulators have also expressed interesting in the data sharing system—even possibly by setting standards for their supervised banks—the CFPB is better situated to provide consistency for the system as a whole for the interpretive questions for which it has rulemaking authority.[300] A CFPB rulemaking process would allow for robust participation of all stakeholders, as well as provide the opportunity for a staged implementation process to the extent that smaller providers need more time to come into compliance. Thus, deepening CFPB engagement in 2020 could potentially sharpen the focus for related initiatives by industry, other federal agencies, and Congress, in addition to resolving longstanding interpretive issues that are within the agency's specific mandate to answer.

7.3 Potential legislation

While the discussions above identify a number of levers for industry stakeholders and federal regulators to more fully realize the benefits and manage the risks of cash-flow underwriting and related data transfers, only Congress has the authority to create a comprehensive and consistent regulatory framework. For example, legislation is likely the only way to do the following:

- **Fix gaps and strengthen protections in existing federal consumer protections:** Most of the major federal consumer financial laws that are potentially relevant to cash-flow underwriting were adopted decades ago in a much different data-sharing environment. As the volume of sharing increases exponentially and as market practices evolve to rely more

299 Some stakeholders have argued that § 1033 of the Dodd-Frank Act could provide an alternative basis for customer protections and data rights and that it would be preferable to start with a clean slate rather than adapting requirements and concepts from FCRA to address issues such as accuracy and use limitations. Section 1033 does not expressly address topics such as correcting errors or restrictions on the use of data after it is obtained from the original source, though because the statute defines "consumer" generally to include agents or representatives acting on the consumer's behalf, the Bureau could presumably define the conditions under which a firm can act as an agent or a representative. 12 U.S.C. § 5533. Again, this may argue for beginning a broad-based inquiry rather than tackling individual interpretive questions in isolation.

300 *See, e.g.*, Lydia Beyoud, FDIC Eyes Data-Sharing Standards for Banks, Bloomberg Law (Apr. 24, 2019); Federal Reserve Governor Lael Brainard, Speech, Where Do Banks Fit in the Fintech Stack? (Apr. 28, 2017).

heavily on affirmative customer permissioning, some of the gaps are taking on new significance and some stakeholders are arguing for strengthened protections. Examples include the limitations on federal regulators' ability to supervise non-bank financial institutions for GLBA information safeguards compliance, the complex way that GLBA provisions concerning information security and restrictions on data sharing apply to parties that receive customer information from a financial institution, and GLBA's reliance on an opt-out structure in connection with certain data sharing activities.[301]

- **Create comparable protections for small business borrowers:** As reflected above, the Equal Credit Opportunity Act and prohibitions on unfair and deceptive practices have been applied to protect small business owners, but various other federal consumer financial laws do not generally apply to commercial credit or borrowers. As a result, regulators have an extremely limited tool set with which to manage potential concerns about privacy, information security, accuracy, and other topics raised in Section 6.1 for business applicants. While there is momentum toward good business practices for small business lenders among the business and advocacy community and from some states,[302] only Congress can adopt a consistent federal baseline of enforceable protections.
- **Create a tailored, consistent regime for all customer-permissioned data flows or financial data more broadly:** While § 1033 of the Dodd-Frank Act provides important data access rights, it focuses primarily on retail consumer financial products and services rather than on information about investments, retirement products, and insurance. Such information is not as likely to be pivotal for credit applications, but can be important for personal financial management. The statute also does not expressly address other data rights and protections as discussed in Section 6.2, such as the ability to correct data or to compel deletion, or liability issues between businesses. Existing laws such as the Fair Credit Reporting Act and the Electronic Fund Transfer Act may be able to provide some rights and protections for some use cases and activities, but stakeholders are divided over their application and the laws do not necessarily apply to all customer-permissioned data transfers and uses. Thus, to the extent that these existing laws cannot be construed to provide satisfactory mechanisms for addressing policy concerns across various use cases, Congressional action would be required.
- **Establish a temporary re-insurance fund to help the private market develop better mechanisms for insuring against data security risks:** As noted above, all stakeholders agree that better insurance mechanisms could help to reduce risks and tensions in the system for customer-permissioned data flows. However, cyber security insurance in the financial system is not standardized or comprehensive. Several stakeholders have suggested that actions similar to what Congress did under the Terrorism Risk Insurance Act to create a government-funded reinsurance pool while private underwriters recalibrate their actuarial models.[303]

301 Less specific accuracy disclosures for adverse actions based on information from sources that are not consumer reporting agencies under the FCRA may be another example. See Section 6.1.1.2. To the extent that the market started to evolve in ways that no longer required intermediaries for transmission of cash-flow data or to the extent that data aggregators are determined not to be consumer reporting agencies under the statute, the less specific notices may be less useful to consumers in identifying the possibility of inaccuracies in the data and educating them about steps they could take to improve their chances of future approval.

302 FinRegLab, Small Business Spotlight at 25; Box 5.1.

303 TRIA was originally envisioned as a temporary program but has been extended several times due to particularly challenging issues concerning terrorism that have also caused other countries to develop various forms of hybrid public/private reinsurance models. For general discussions of cyber insurance, TRIA, and other public-private models, *see, e.g.,* Aaron Klein & Scott R. Anderson, A Federal Backstop for Insuring Against Cyberattacks? Brookings Institute (Sept. 27, 2019); Andrew Granato & Andy Polacek, The Growth and Challenges of Cyber Insurance, Federal Reserve Bank of Chicago Letter No. 426 (2019); EastWest Institute, Cyber Insurance and Systemic Market Risk 34-35 (2017).

BOX 7.3.1 GLBA OBLIGATIONS ON DOWNSTREAM PARTIES

One point of increasing concern among some stakeholders as data-sharing practices evolve and expand is that Gramm-Leach-Bliley Act obligations do not transfer in their entirety as nonpublic personal information flows downstream from "financial institutions" that have a direct customer relationship with a consumer.

As discussed in Boxes 5.2.2.2.1, 6.1.3.1, and 6.1.3.2, GLBA imposes two substantive sets of requirements, one dealing with information sharing and privacy policies and one with information security safeguards. Financial institutions that have a direct customer relationship with a consumer are subject to both parts, but as those financial institutions share data with unaffiliated companies in the course of various business activities, the way that GLBA obligations apply to the downstream parties varies depending on the circumstances.

For information safeguards, if the data recipient is a financial institution in its own right, it is subject to the full safeguards requirements. If the recipient is some other kind of vendor to the original financial institution, application of the safeguards requirements operates indirectly by contract because the law requires the original financial institution to require its vendors to implement appropriate safeguards. However, there is no obligation stated in the rules that the financial institution must require its vendors in turn to impose safeguard obligations by contract if they further share the data with other companies. And where data is transferred to non-financial institutions in other circumstances, the safeguards requirements do not transfer with the data by regulation or contract.

For GLBA's privacy-related provisions, the requirement to disclose privacy policies and practices only applies to a financial institution that has a direct customer or consumer relationship. Where financial institutions with direct customer relationships share data with non-affiliated companies, the statute generally provides that the non-affiliated company can only share the information if it would be lawful for the original financial institution source to take the same action under GLBA. However, the implementing regulations are complex and somewhat ambiguous as to how the restrictions are applied to downstream sharing.

For example, for certain types of information sharing, a recipient company can generally only use and pass the information on to additional unaffiliated companies in order to carry out the activity for which it received the information. However, where a consumer has received notice and an opportunity to opt out of the initial data sharing (for instance, if a financial institution was to sell data to nonaffiliated third parties for their own marketing purposes), a recipient company effectively steps into the shoes of the original financial institution. The statute gives such firms broad latitude to use the data for their own purposes. They can also share the data with non-affiliated parties, so long as the sharing is consistent with general GLBA limitations, the original financial institution's disclosed privacy practices, and the consumer's exercise of opt-out rights. And application of the regulations to further downstream recipients is somewhat ambiguous.

Thus, while GLBA provides certain downstream protections, the details are complex and the obligations are not entirely parallel between the two parts of the law. Some stakeholders have expressed concern that companies that are not financial institutions with direct customer relationships may not always understand their obligations, and that as data passes downstream it is progressively less likely to be protected by law or in practice. Some stakeholders have argued that the law should be amended to impose consistent baseline requirements on recipients of financial data, regardless of whether they are financial institutions or have direct customer relationships with consumers.

Sources: 15 U.S.C. § 6802(c); 12 C.F.R. § 1016.11; 16 C.F.R. § 314.4(d); 66 Fed. Reg. 8616, 8618 (Feb. 1, 2001); 65 Fed. Reg. 35162, 35171-72 (June 1, 2000); 65 Fed. Reg. 33646, 33654-56 & n.29, 33658, 33667-68 (May 24, 2000).

In short, there could be substantial benefits to increasing the consistency and comprehensiveness of protections that apply to (1) different sources of data for credit underwriting; (2) customer-permissioned data transfers for all types of use cases; and/or (3) the use of customer data in financial services more generally. Such action could not only provide important protections for groups or situations that are largely unprotected by current laws—such as small businesses—but also to help ensure that existing federal protections such as GLBA continue to have their intended and expected effect as technological and market practices have evolved over time.

However, such legislation is challenging to structure for a number of reasons, including the need to address questions about agency resources and jurisdiction in addition to setting substantive standards. For example, even without substantial adjustments in substantive rules, simply extending

existing protections to small business borrowers and filling the coverage and monitoring gaps with regard to existing information security requirements would require Congress to assign additional authorities and resources to one or more federal regulators. This presents important questions about centralization of authority and accountability versus the potential resource and subject matter benefits of a more distributed approach that spreads responsibility among multiple agencies that are already familiar with particular entities or subject matters from their existing activities.

In addressing substantive standards, an additional dilemma is whether to tailor to new activities or entities or to update existing regulatory regimes more generally to cover both traditional and new functions. Targeted approaches are often appealing because they are more context-specific and may avoid disrupting settled activities and markets. However, maintaining distinct parallel regimes can at times create awkward competitive and regulatory dynamics. For example, while some stakeholders have suggested that § 1033 of the Dodd-Frank Act could be used as a starting point for creating a tailored regulatory regime for customer-permissioned data flows, others have argued that doing so could prompt traditional credit reporting incumbents to migrate to the new system if it was perceived to be less restrictive than traditional Fair Credit Reporting Act requirements.

The broadest version of this dilemma is whether to structure legislation to focus specifically on the use of data in financial services or on data control and protections for consumers and small businesses more broadly across all commercial sectors. There are strong arguments for the latter approach, given that lines are starting to blur as nonfinancial data is increasingly being used for purposes of providing financial services and nonfinancial firms are increasingly challenging traditional providers.[304] Even in the context of cash-flow underwriting itself, for example, companies whose primary business is providing accounting software and e-commerce platforms are starting to lend to small businesses based on the data that they can evaluate from their core activities.[305] And as discussed in Box 2.3.1, financial services providers are beginning to use information from social media and other sources for fraud prevention and other activities even if they are cautious about using it for underwriting.[306]

At the same time, linking the use of data for credit and other financial services purposes to broad general concerns about the collection and use of customer data by "big tech" companies in a range of other contexts may have substantial disadvantages in terms of timing and complexity. Thus, if a comprehensive U.S. framework is not practicable to adopt at the current time, there are strong arguments for amending existing federal financial laws because they have conditioned consumers to expect certain baseline protections with regard to credit underwriting and financial data more generally that may not in fact be operating as intended in evolving markets.

304 For general discussions, *see, e.g.,* Julie Verhage & Jennifer Surane, Big Tech Is Coming for Banking: Experts Predict Fintech's 2020, Bloomberg (Dec. 23, 2019); Financial Stability Board, BigTech in Finance: Market Developments and Potential Financial Stability Implications (2019); Bank for International Settlements, Annual Economic Report: III. Big Tech in Finance: Opportunities and Risks (2019); Maria Aspan, Why Every Company Wants To Look Like a Bank—Without Becoming One, Fortune (Nov. 18, 2019); Gregory Barber, Every Tech Company Wants to Be a Bank—Someday, At Least (Nov. 16, 2019); Anton Ruddenklau, Tech Giants in Financial Services: Is Collaboration the Way Forward?, KPMG (2018).

305 FinRegLab, Small Business Spotlight at 19-22.

306 See Box 2.3.1.

8. CONCLUSION

Our research suggests that cash-flow data holds significant promise for creating more inclusive, efficient, and competitive credit markets. In light of this promise, investment of additional resources is warranted to reduce the competitive, coordination, and compliance issues that are slowing the adoption of beneficial practices and mitigation of potential risks. With thoughtful development, cash-flow based underwriting has the potential to benefit borrowers and financial services providers alike.

The issues summarized in Sections 5–7 highlight the importance of stakeholder and policymaker engagement to address the policy issues raised by cash-flow underwriting and underlying data flows. The question whether cash-flow underwriting achieves its potential to foster a more inclusive, efficient, and competitive marketplace or whether it evolves in ways that heighten risks and tradeoffs for underserved borrowers will likely depend on how and whether stakeholders begin to address these critical policy issues in the next few years.

Some degree of standardization in technologies and data elements could reduce implementation costs, improve the accuracy and efficiency of data analysis, facilitate greater investment activity, and manage customer protection risks. While the market itself is beginning to push in this direction, more research is needed on certain issues and it would be difficult for self-governance efforts to resolve all of the competitive dynamics, coordination challenges, and compliance issues that are currently complicating the adoption of cash-flow underwriting.

Thus, greater engagement by regulators through increased research, market monitoring and supervision, and interpretive initiatives could be helpful. Although regulators may be inclined to wait for further market developments or for Congress to provide a comprehensive framework before committing more resources to these issues, there can be substantial opportunity costs to inaction with regard to efficiency, competitive dynamics, access to credit, and customer protection. Increasing engagement could both sharpen the focus of industry initiatives and help inform Congress about any policy issues that are difficult to manage with current regulatory tools. And resolving market challenges and regulatory questions about the underlying system for data transfers in the next few years could better position cash-flow underwriting to reach scale as lenders and secondary market actors gain a better understanding of its strengths and limitations in predicting default risk in particular credit markets.

Ultimately, constructive action by industry, regulators, and Congress will likely each be needed to improve outcomes with regard to both cash-flow underwriting and related data flows. While

national legislation is the only way to provide an entirely consistent and comprehensive regulatory framework, industry and regulatory efforts can potentially both narrow the scope of issues that need to be addressed through legislative action and help to inform lawmakers' efforts. Such initiatives could not only ensure that cash-flow underwriting benefits borrowers and financial services providers alike, but could also serve as a stepping stone to managing continuing evolution in credit and data transfer markets more generally.

BIBLIOGRAPHY

Accenture, 2019 Global Financial Services Consumer Study (2019)

Robert M. Adams, Do Marketplace Lending Platforms Offer Lower Rates to Consumers? FEDS Notes (Oct. 22, 2018)

Andrew Ackerman, Fannie, Freddie to Consider Alternatives to FICO Scores, Wall St. J. (Aug. 13, 2019)

John Adams, Visa's $5 Billion Plaid Deal Takes a Possible Rival Off the Table, Am. Banker (Jan. 13, 2020)

Aite, Alternative Data Across the Loan Life Cycle: How FinTech and Other Lenders Use It and Why, experian.com (2018)

Alessandro Alcquisti & Ralph Gross, Predicting Social Security Numbers from Public Data (July 7, 2009)

American Bankers Association, Statement for the Record to the Task Force on Financial Technology Regarding 'Banking on Your Data: The Role of Big Data in Financial Services' (Nov. 21, 2019)

American Bankers Association, The State of Digital Lending (2018)

American Bankers Association, Understanding APIs (2019)

American Law Institute, Tentative Draft, Principles of the Law: Data Privacy (2019)

AnnaMaria Andriotis, FICO Changes Could Lower Your Credit Score, Wall St. J. (Jan. 23, 2020)

AnnaMaria Andriotis, Hairdresser, Plumber, Lawyer: A Job License Could Help You Get a Loan, Wall St. J. (Nov. 6, 2019)

AnnaMaria Andriotis, Need a Loan? Equifax Plans to Sell More Utility, Phone Records, Wall St. J. (Sept. 18, 2019)

AnnaMaria Andriotis, Need Cash? Companies Are Considering Magazine Subscriptions and Phone Bills When Making Loans, Wall St. J. (Sept. 12, 2019)

AnnaMaria Andriotis, Shopping at Discount Stores Could Help Get You a Loan, Wall St. J. (Mar. 4, 2019)

AnnaMaria Andriotis, Why Your FICO Score Could Get a Boost in 2019, Wall St. J. (Oct. 21, 2018)

Sebastian Anthony, What Is Open Banking, and Is It Safe?, bankrate.com (June 3, 2019)

Apple, Differential Privacy, Apple.com (visited Feb. 8, 2020)

Robert Armstrong, How Online Platforms Shook Small Business Lending in America, Fin. Times (Jan. 29, 2019)

Chris Arnold, FICO Is About to Change Credit Scores. Here's Why It Matters, npr.org (Jan. 30, 2020)

Maria Aspan, Why Every Company Wants To Look Like a Bank—Without Becoming One, Fortune (Nov. 18, 2019)

Aspen Institute, Income Volatility: A Primer (2016)

Association for Public Policy Analysis and Management, Panel: The Role of Income Volatility in Family Economic Security: Evidence and Policy Implications, 39th Annual Fall Research Conference (2017)

Susan Athey et al., The Digital Privacy Paradox: Small Money, Small Costs, Small Talk, National Bureau of Economic Research Working Paper No. 23488 (June 2017)

Brooke Auxier et al., Americans and Privacy: Concerned, Confused, and Feeling Lack of Control over Their Personal Information, Pew Research Center (2019)

Robert B. Avery et al., Credit Report Accuracy and Access to Credit, Fed. Res. Bull. 297 (June 2004)

Robert B. Avery et al., Does Credit Scoring Produce a Disparate Impact? 40 Real Estate Econ. 965 (2012)

Justin Baer, Fidelity Parent Launching New Online Data-Protection Business, Wall St. J. (Apr. 30, 2019)

Justin Baer, Fidelity's Parent Company Is Spinning Out Its Akoya Personal-Data Startup, Wall St. J. (Feb. 20, 2020)

Todd Baker, Marketplace Lenders Are a Systemic Risk, Am. Banker (Aug. 15, 2015)

Todd H. Baker, FinTech Alternatives to Short-Term Small-Dollar Credit: Helping Low-Income Working Families Escape the High-Cost Lending Trap, Harvard Kennedy School Mossavar-Rahmani Center for Business & Government Associate Working Paper Series No. 75, at 36-38 (May 2017)

Yannis Bakos et al., Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts, 43 J. Legal Studies 1 (2014)

Tetyana Balyuk, Financial Innovation and Borrowers: Evidence from Peer-to-Peer Lending (May 6, 2019)

Bank for International Settlements, Annual Economic Report: III. Big Tech in Finance: Opportunities and Risks (2019)

Bank Policy Institute & Covington, Artificial Intelligence Discussion Draft (2019)

Gregory Barber, Every Tech Company Wants to Be a Bank—Someday, At Least (Nov. 16, 2019)

Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Cal. L. Rev. 671 (2016)

Solon Barocas et al., The Hidden Assumptions Behind Counterfactual Explanations and Principal Reasons (December 2019)

Alistair Barr, Fully Charged Newsletter, Come on a Trip to the New Privacy Circle of Hell, Bloomberg Technology (Jan. 9, 2020)

Michael S. Barr et al., Consumer Autonomy and Pathways to Portability in Banking and Financial Services, University of Michigan Center on Finance, Law, & Policy Working Paper No. 1 (Nov. 3, 2019)

John M. Barron & Michael Staten, The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience, in Margaret J. Miller, ed., Credit Reporting Systems and the International Economy (2003)

Robert Bartlett et al., Consumer-Lending Discrimination in the Fintech Era, National Bureau of Economic Research Working Paper No. 25943 (updated November 2019)

Basel Committee on Bank Supervision, Report on Open Banking and Application Programming Interfaces, Bank for International Settlements (2019)

Basel Committee on Banking Supervision, Supervisory and Bank Stress Testing: Range of Practices (2017)

William F. Bassett & Jose M. Berrospide, The Impact of Post Stress Tests Capital on Bank Lending, Finance & Economics Discussion Series Working Paper 2018-087 (November 2018)

Majid Bazarbash, FinTech in Financial Inclusion: Machine Learning Applications in Modelling Credit Risk, IMF Working Paper 19-109 (2019)

Luisa Beltran, Envestnet Hires Goldman to Advise on Options for Yodlee. A Sale Could Be Coming, Barron's (Feb. 5, 2020)

Tobias Berg et al., On the Rise of the FinTechs: Credit Scoring Using Digital Footprints, Review of Fin. Studies (Sept. 2019)

Allen N. Berger & W. Scott Frame, Small Business Credit Scoring and Credit Availability, 47 J. of Small Bus. Mgmt. 5 (2007)

Allen N. Berger et al., Credit Scoring and the Availability, Price, and Risk of Small Business Credit, 37 J. of Money, Credit & Banking 191 (2005)

Emily Bernbaum, Lawmakers Call for FTC Probe into Top Financial Data Aggregator, The Hill (Jan. 17, 2020)

Kate Berry, Is CFPB Punting on Equifax? It's Complicated, Am. Banker (Feb. 5, 2018)

Kate Berry & Hannah Lang, 4 Questions as CFPB Closes in on Revamp of Key Mortgage Rule, Am. Banker (Jan. 21, 2020)

Lydia Beyoud, Democrats Call for FTC Probe of Financial Data Giant Yodlee, Bloomberg Law (Jan. 17, 2020)

Lydia Beyoud, FDIC Eyes Data-Sharing Standards for Banks, Bloomberg Law (Apr. 24, 2019)

Lydia Beyoud, Fintechs Step Into Payday Alternatives Where Banks Fear to Tread, Bloomberg Law (Dec. 18, 2018)

Suman Bhattacharyya, How Lending Startups Are Trying to Edge Out Payday Lenders, Tearsheet (July 31, 2017)

Suman Bhattacharya, With Plaid, Wells Fargo Gives Customers a New Lever to Control Their Data, bankinnnovation.net (Sept. 23, 2019)

Ray Birch, Time to Beef Up Fraud Detection Here?, CUToday.info (Jan. 3, 2019)

Bitglass, The Financial Matrix: Bitglass' 2019 Financial Breach Report (2019)

Octavio Blanco, Consumers Get More Control Over the Banking Data Shared with Financial Apps, Consumer Reports (Nov. 10, 2019)

Knut Blind et al., The Impact of Standards and Regulation on Innovation in Uncertain Markets, 46 Research Policy 249 (2017)

Board of Governors of the Federal Reserve System, Dodd-Frank Act Stress Test 2019: Supervisory Stress Test Methodology (2019)

Board of Governors of the Federal Reserve System, Press Release, Federal Reserve Announces Plan to Develop a New Round-the-Clock Real-Time Payment and Settlement Service to Support Faster Payments (Aug. 5, 2019)

Board of Governors of the Federal Reserve System, Report to the Congress on Credit Scoring and its Effects on the Availability and Affordability of Credit (2007)

Board of Governors of the Federal Reserve System, Report on the Economic Well-Being of U.S. Households in 2017 (2018)

Board of Governors of the Federal Reserve System, Report on the Economic Well-Being of U.S. Households in 2018 (2019)

Board of Governors of the Federal Reserve System, Report to the Congress on Reductions of Consumer Credit Limits Based on Certain Information as to Experience or Transactions of the Consumer (2010)

Board of Governors of the Federal Reserve System, Supervisory & Regulation Letter 11-7 (Apr. 4, 2011)

Board of Governors of the Federal Reserve System, Supervisory & Regulation Letter 13-19 (Dec. 5, 2013)

Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, National Credit Union Administration & Office of the Comptroller of the Currency, Interagency Statement on the Use of Alternative Data in Credit Underwriting (Dec. 3, 2019)

Casey Bond, How Employment Credit Checks Work, U.S. News & World Report (Oct. 31, 2019)

Federal Reserve Governor Lael Brainard, Speech, Where Do Banks Fit in the Fintech Stack? (Apr. 28, 2017)

Kenneth P. Brevoort & Cheryl R. Cooper, Foreclosure's Wake: The Credit Experiences of Individuals Following Foreclosure, 41 Real Estate Econ. 747 (2013)

Kenneth P. Brevoort & Michelle Kambara, Data Point, Medical Debt and Credit Scores, Consumer Financial Protection Bureau (2014)

Brian Browdie, Can Alternative Data Determine a Borrower's Ability to Repay, Am. Banker (Feb. 24, 2015)

Thomas Brown & Tyler Griffin, Visa+Plaid—A Slightly Less Hot Take, Medium (Feb. 3, 2020)

Greg Buchak et al., Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks, NBER Working Paper 23288 (revised September 2018)

Elizabeth Buchwald, The Government Has No Idea How Many Gig Workers There Are, and That's a Problem, MarketWatch (Jan. 7, 2019)

Sara Burr & Virginia Carlson, Utility Payments as Alternative Credit Data: A Reality Check, The Brookings Institution Metropolitan Policy Program Discussion Paper (2007)

Business Insider Intelligence, One Area of US Alt Lending Is Recovering, Business Insider (Feb. 23, 2017)

Caroline Cakebread, You're Not Alone, No One Reads Terms of Service Agreements, Business Insider (Nov. 15, 2017)

Nick Caley, PSD2 in 2019: A Year of Yet More Delays, FintechFutures (Dec. 30, 2019)

California Department of Justice, Notice of Proposed Rulemaking, Initial Statement of Reasons, Proposed Adoption of California Consumer Privacy Act Regulations (Oct. 11, 2019)

Scott Carey, Visa's Acquisition of Plaid Throws Up Data Reuse Concerns, TechWorld (Jan. 21, 2020)

Omri Ben-Shahar & Carl E. Schneider, More Than You Wanted to Know: The Failure of Mandated Disclosure (2014)

Peter Carroll & Ben Hoffman, Financing Small Businesses: How "New-Form Lending" Will Reshape Banks' Small Business Strategies (2013)

Peter Carroll & Saba Rehmani, Alternative Data and the Unbanked, Oliver Wyman (2017)

Peter Carroll & Cosimo Schiavone, 2018 VantageScore Market Study Report, Oliver Wyman (2018)

CBInsights, Data Is Unlocking the Mortgage Tech Business, cbinsights.com (June 29, 2017)

CDFI Fund, CDFI Certification: Your Gateway to the CDFI Community (2016)

Center for Financial Services Innovation, CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration (2016)

Center for Financial Services Innovation, Liability, Transparency and Consumer Control in Data Sharing (2017)

Jiahao Chen et al., Fairness Under Unawareness: Assessing Disparity When Protected Class Is Unobserved, Conference on Fairness, Accountability, and Transparency (FAT* '19) (January 2019)

Julia S. Cheney et al., The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches, Federal Reserve Bank of Philadelphia Payments Card Center Discussion Paper (Oct. 2012)

Sarah Chenven & Carolyn Schulte, The Power of Rent Reporting Pilot, Credit Builders Alliance (2015)

Caitlin Chin & Maria Odell, TechTank, Highlights: Commissioners Discuss the Future of the FTC's Role in Privacy, Brookings Institution (Nov. 5, 2019)

Robert Clark et al., Digital Lenders Price Loans Inside a Black Box of Alternative Data, S&P Global Market Intelligence (Nov. 8, 2018)

Clearent, Tokenization vs. Encryption, clearent.com (visited Feb. 11, 2020)

The Clearing House, Consumer Survey: Financial Apps and Data Privacy (2019)

The Clearing House, Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers (2015)

The Clearing House, Fintech Apps and Data Privacy: New Insights from Consumer Research (2018)

The Clearing House, Template for U.S. Accounts Data Sharing Agreement (Nov. 12, 2019)

Nick Clements, 5 Reasons New Lenders Are Ignoring FICO Credit Scores, Forbes (Apr. 21, 2015)

Lalita Clozel, Banks Want Reassurance on Payday-Type Loans, Wall St. J. (Sept. 6, 2019)

Commerce Ventures, Visa Buys Plaid: What Does It Mean?, Medium (Jan. 16, 2020)

Consumer Federation of America, Press Release, Survey Shows an Increasing Number of Consumers Have Obtained Their Credit Scores and Know Much More About Credit Scores (June 18, 2018)

Consumer Financial Protection Bureau, Complaint for Permanent Injunction and Other Relief, CFPB v. Equifax, Inc., No. 1:19-cv-03300-TWT (N.D. Ga. July 22, 2019)

Consumer Financial Protection Bureau, Compliance Bulletin 2015-06 (Nov. 23, 2015)

Consumer Financial Protection Bureau, Compliance Bulletin and Policy Guidance 2016-02, 81 Fed. Reg. 74410 (Oct. 26, 2016)

Consumer Financial Protection Bureau, Consent Order, In re Dwolla, Inc., File No. 2016-CFPB-0007 (Mar. 2, 2016)

Consumer Financial Protection Bureau, Consumer Credit Reports: A Study of Medical and Non-Medical Collections (2014)

Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (2017)

Consumer Financial Protection Bureau, Data Point, Becoming Credit Visible (2017)

Consumer Financial Protection Bureau, Data Point, Credit Invisibles (2015)

Consumer Financial Protection Bureau, Key Dimensions and Processes in the U.S. Credit Reporting System: A Review of How the Nation's Largest Credit Bureaus Manage Consumer Data (2012)

Consumer Financial Protection Bureau, List of Consumer Reporting Companies (2020)

Consumer Financial Protection Bureau, Press Release, Consumer Financial Protection Bureau Announces Symposia Series (April 18, 2019)

Consumer Financial Protection Bureau, Quarterly Consumer Credit Trends: Public Records (2018)

Consumer Financial Protection Bureau, Statement of the Bureau of Consumer Financial Protection on Enactment of S.J. Res. 57 (May 21, 2018)

Consumer Financial Protection Bureau, Statement of Policy Regarding Prohibition on Abusive Acts or Practices (Jan. 24, 2020)

Consumer Financial Protection Bureau, Supervisory Highlights Consumer Reporting Special Edition (2017)

Consumer Financial Protection Bureau, Symposium on Consumer Access to Financial Records (Feb. 26, 2020), available at https://www.consumerfinance.gov/about-us/events/cfpb-symposium-consumer-access-financial-records/

Consumer Financial Protection Bureau, The Consumer Credit Card Market (2019)

Consumer Financial Protection Bureau, Using Publicly Available Information to Proxy for Unidentified Race and Ethnicity: A Methodology and Assessment (2014)

Consumer Reports et al., The Digital Standard (2017)

Cheryl R. Cooper & Darryl E. Getter, Consumer Credit Reporting, Credit Bureaus, Credit Scoring, and Related Policy Issues, Congressional Research Service (2019)

Joseph Cox, Leaked Document Shows How Big Companies Buy Credit Card Data on Millions of Americans, Vice (Feb. 19, 2020)

Lorrie Cranor, A Large Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices, ACM Transactions on the Web (2016)

Credit Union National Association, Compliance: Final FHFA on Alternative Credit Scoring, news.cuna.org (Sept. 3, 2019)

Penny Crosman, Banks Aren't Following CFPB Data-Sharing Guidance, Fintechs Say, Am. Banker (Nov. 20, 2017)

Penny Crosman, Big Banks, Aggregators Launch Group to Hash Out Data Sharing Issues, Am. Banker (Oct. 18, 2018)

Penny Crosman, Data Aggregators Push Back on the Notion They Have a Fraud Problem, Am. Banker (Sept. 30, 2019)

Penny Crosman, Data-Sharing Debate Grows Contentious as Fintechs Vent Grievances, Am. Banker (Aug. 15, 2017)

Penny Crosman, Fidelity Data-Sharing Hub Aims to End Screen Scraping, Am. Banker (June 11, 2019)

Penny Crosman, Fidelity's Data-Sharing Unit Akoya to Be Jointly Owned with The Clearing House, 11 Banks, Am. Banker (Feb. 20, 2020)

Penny Crosman, How APIs Are Being Used at Citi, BBVA and Other Leading Banks, Am. Banker (May 26, 2019)

Penny Crosman, Is a New Data War about to Erupt?, Am. Banker (Dec. 23, 2019)

Penny Crosman, Is AI Making Credit Scores Better, or More Confusing?, Am. Banker (Feb. 14, 2017)

Penny Crosman, Is Finra's Dire Warning about Data Aggregators on Target?, Am. Banker (Apr. 9, 2018)

Penny Crosman, JPMorgan Chase Signs Data Sharing Agreement with Envestnet Yodlee, Am. Banker (Dec. 5, 2019)

Penny Crosman, JPMorgan Chase Moves to Block Fintechs from Screen Scraping, Am. Banker (Jan. 2, 2020)

Penny Crosman, Online Lenders Make Case for Cash-Flow Data While Acknowledging Pitfalls, Am. Banker (Aug. 5, 2019)

Penny Crosman, 'Out of the Shadows': Use of Alternative Data in Lending Gains Ground, Am. Banker (Dec. 16, 2019)

Penny Crosman, The Battle Over Bank Customer Data May Finally Be Over, Am. Banker (Nov. 6, 2017)

Penny Crosman, The Truth Behind the Hubbub Over Screen Scraping, Am. Banker (Nov. 12, 2015)

Penny Crosman, U.S. Bank Embraces Open Banking with Data Sharing Agreements, Am. Banker (Sept. 24, 2019)

Penny Crosman, Wells Fargo Strikes Data-Sharing Agreement with Plaid, Am. Banker (Sept. 19, 2019)

Penny Crosman, Wells-Finicity Deal Furthers Data Détente, Am. Banker (Apr. 4, 2017)

Penny Crosman, What the Visa-Plaid Merger Means for Banks, Fintechs, Am. Banker (Jan. 16, 2020)

Penny Crosman, Will Dropping Tax Lien Data from Credit Reports Lead to Bad Loans?, Am. Banker (Apr. 2, 2018)

Penny Crosman, Why a Clear Answer to the Data-Sharing Debate Remains Elusive, Am. Banker (Feb. 23, 2017)

Ben Cukier, In the Battle Between Online Lenders and Banks, Data Wins, Forbes (Oct. 3, 2018)

Nate Cullerton, Note, Behavioral Credit Scoring, 101 Georgetown L.J. 807 (2013)

Michael Cusumano et al., Product, Process, and Service: A New Industry Lifecycle Model (Mar. 8, 2007)

Drew Dahl et al., Compliance Costs, Economies of Scale, and Compliance Performance: Evidence from a Survey of Community Banks, Federal Reserve Bank of St. Louis (2018)

Eric Dash, Up Against the Plastic Wall, N.Y. Times (May 21, 2005)

DataGuidance & Future of Privacy Forum, Comparing Privacy Laws: GDPR v. CCPA (2018)

Michelle Davis, JPMorgan Leads Banks Flight from Poor Neighborhoods, Bloomberg (Mar. 6, 2019)

Michael Deleon, A Buyer's Guide to Data Aggregation, Tearsheet (Feb. 19, 2019)

Deloitte, How to Flourish in an Uncertain Future: Open Banking and PSD2 (2017)

Yves-Alexandre de Montjoye et al., Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata, 347 Science 536 (2015)

Telis Demos & Rachel Louise Ensign, Frustrated by the Tech Industry, Small Banks Start to Rebel, Wall St. J. (Apr. 11, 2019)

Yuliya Demyanyk, Have Stress Tests Impacted Small-Business Lending?, Federal Reserve Bank of Cleveland, Econ. Commentary (Nov. 14, 2019).

Yuliya Demyanyk, Your Credit Score Is a Ranking, Not a Score, Federal Reserve Bank of Cleveland Economic Commentary (2010)

Department of Finance Canada, Consumer-Directed Finance: The Future of Financial Services (2020)

Lydia DePillis, Banks Are Walking Away from Low-Income Homebuyers, CNN (May 11, 2018)

Sandeep Dhameja, Clarifying Liability for Twenty-First-Century Payment Fraud, Federal Reserve Bank of Chicago, Economic Perspectives 107 (3rd quarter 2013)

Nathan DiCamillo, Capital One Mends Fences with One Aggregator, Deepens Relationship with Another, Am. Banker (Aug. 10, 2018)

Nathan DiCamillo, In Data Dispute with Capital One, Plaid Stands Alone, Am. Banker (July 17, 2018)

Nathan DiCamillo, JPMorgan Chase Inks Fourth Data Aggregator Deal, Am. Banker (Oct. 22, 2018)

Nathan DiCamillo, Which Fintechs Are Best Positioned to Handle a Recession?, Am. Banker (June 28, 2019)

Marco DiMaggio & Vincent W. Yao, FinTech Borrowers: Lax-Screening or Cream-Skimming? (February 2019)

Anton Dimitrov, The World Needs Privacy-Preserving Computations, Medium (Jan. 15, 2019)

Nimayi Dixit, Payment Fintechs Leave Their Mark on Small Business Lending, S&P Global Market Intelligence (2018)

Amanda Dixon, Fintech Roadblocks: Why Banks Block Budgeting Apps, bankrate.com (Dec. 5, 2017)

Kelly Dilworth, New Lenders Shun FICO, Create Their Own Scores, creditcards.com (Feb. 26, 2016)

Trevor Dryer, How Machine Learning Is Quietly Transforming Small Business Lending, Forbes (Nov. 1, 2018)

Elizabeth Dunham, Blog, Consent Is Not the 'Silver Bullet' for GDPR Compliance, ico.org.uk (Aug. 16, 2017)

Thomas A. Durkin, Credit Card Disclosures, Solicitations, and Privacy Notices: Survey Results of Consumer Knowledge and Behavior, Federal Reserve Bulletin (2006)

Karen Dynan et al., The Evolution of Household Income Volatility, 12 B.E. J. of Economic Analysis & Policy 1935 (2012)

EastWest Institute, Cyber Insurance and Systemic Market Risk (2017)

Wendy Edelberg, Risk-Based Pricing of Interest Rates for Consumer Loans, 53 J. Monetary Econ. 2283 (2006)

Larry Edelman, Fidelity Spins Off Business That Helps Consumers Control Financial Data, Boston Globe (Feb. 20, 2020)

Nature, Editorial, Time to Discuss Consent in Digital-Data Studies, nature.com (July 21, 2019)

Electronic Privacy Information Center, Comments to the Federal Trade Commission on Standards for Safeguarding Customer Information (Aug. 1, 2019)

Electronic Privacy Information Center, The Gramm-Leach-Bliley Act (visited Feb. 8, 2020)

Envestnet/Yodlee, Analytics for Credit Risk Modelling: Making Better Lending Decisions, yodlee.com (visited Feb. 8, 2020)

Envestnet/Yodlee, Envestnet/Yodlee and JPMorgan Chase Sign Data Agreement to Enhance Consumer Data Protections, Bolster Overall Data Connectivity and Reliability, prnewswire.com (Dec. 5, 2019)

Envestnet/Yodlee, Comment Letter to Enhanced Cyber Risk Management Standards, Docket OCC-2016-0016 (Feb. 17, 2017)

Envestnet/Yodlee, Press Release, Envestnet/Yodlee Enapbles Comprehensive Financial Picture with Risk Insight Suite, yodlee.com (visited Feb. 22, 2020)

Equifax, Equifax Continues Leadership in Alternative Data with Worldwide Urjanet Partnership, investor.equifax.com (Sept. 18, 2019)

Equifax, Equifax Enters into Credit Bureau-Exclusive Relationship with Envestnet/Yodlee to Further Extend Alternative Data Leadership, equifax.com (Nov. 7, 2019)

European Commission, Ethics and Data Protection (2018)

European Union, What Is GDPR, the EU's New Data Protection Law?, GDPR.EU (2018)

Carol A. Evans, Keeping Fintech Fair: Thinking About Fair Lending and UDAP Risks, Consumer Compliance Outlook (2nd Issue 2017)

Experian, Blog, The Benefits of Full-File Credit Reporting and Why Communication Providers Should Consider It (June 25-29, 2011)

Experian, Fintech vs. Traditional FIs: Trends in Unsecured Personal Installment Loans (2019)

Experian, Let There Be Light: The Impact of Positive Energy-Utility Reporting on Consumers (2014)

Experian, The State of Alternative Credit Data (2018)

Experian RentBureau, Credit for Renting: The Impact of Positive Rent Reporting on Subsidized Housing Residents (2013)

Fannie Mae, Desktop Underwriter (DU) Validation Service: Leveraging the Power of DU to Provide You with Day 1 Certainty (2019)

Fannie Mae, DU Validation Service Frequently Asked Questions (July 20, 2019)

Diana Farrell & Fiona Greig, Coping with Costs: Big Data on Expense Volatility and Medical Payments, JPMorgan Chase Institute (2017)

Diana Farrell & Fiona Greig, Paychecks, Paydays, and the Online Platform Economy: Big Data on Income Volatility, JPMorgan Chase Institute (2016)

Diana Farrell & Fiona Greig, Weathering Volatility: Big Data on the Financial Ups and Downs of U.S. Individuals, JPMorgan Chase Institute (2015)

Diana Farrell & Chris Wheat, Cash Is King: Flows, Balances, and Buffer Days: Evidence from 600,000 Small Businesses, JPMorgan Chase & Co. Institute (2016)

Diana Farrell et al., Facing Uncertainty: Small Business Cash Flow Patterns in 25 U.S. Cities, JPMorgan Chase & Co. Institute (2019)

Diana Farrell et al., Growth, Vitality, and Cash Flows: High-Frequency Evidence from 1 Million Small Businesses, JPMorgan Chase & Co. Institute (2018)

Diana Farrell et al., Trading Equity for Liquidity: Bank Data on the Relationship Between Liquidity and Mortgage Default, JPMorgan Chase Institute (2019)

Diana Farrell et al., Weathering Volatility 2.0: A Monthly Stress Test to Guide Savings (2019)

Federal Deposit Insurance Corporation, 2011 FDIC National Survey of Unbanked and Underbanked Households (2012)

Federal Deposit Insurance Corporation, 2017 FDIC National Survey of Unbanked and Underbanked Households (2018)

Federal Deposit Insurance Corporation, A Template for Success: The FDIC's Small-Dollar Loan Pilot Program, FDIC Quarterly (2010)

Federal Deposit Insurance Corporation, Financial Institution Letter 44-2008 (June 6, 2008)

Federal Deposit Insurance Corporation, Financial Institution Letter 22-2017 (June 7, 2017)

Federal Deposit Insurance Corporation, Financial Institution Letter 19-2019 (Apr. 2, 2019)

Federal Deposit Insurance Corporation, Guidance on Supervisory Concerns and Expectations Regarding Deposit Advance Products (Nov. 21, 2013)

Federal Financial Institutions Examination Council Information Technology Examination Handbook II.C.20 (2016)

Federal Financial Institutions Examination Council Outsourcing Technology Services Booklet (2004)

Federal Reserve Bank of Kansas City, Disconnected: Seven Lessons on Fixing the Digital Divide (2019)

Federal Reserve Banks, 2018 Small Business Credit Survey: Report on Employer Firms (2019)

Federal Reserve Banks, 2017 Small Business Credit Survey: Report on Nonemployer Firms (2018)

Federal Trade Commission, 40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations (2011)

Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (2016)

Federal Trade Commission, Complaint for Civil Penalties, Permanent Injunction, and Other Relief, U.S. v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019)

Federal Trade Commission, Complaint for Civil Penalties, Permanent Injunction, and Other Relief, U.S. v. RockYou, Inc., No. 3:12-cv-01487-SI (N.D. Cal. Mar. 26, 2012)

Federal Trade Commission, Complaint for Permanent Injunction and Other Equitable Relief, FTC v. CompuCredit Corp., No. 1:08-cv-1976-BBM-RGV (N.D. Ga. June 10, 2008)

Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability (2014)

Federal Trade Commission, FTC Policy Statement on Deception (Oct. 14, 1983)

Federal Trade Commission, Policy Statement on Unfairness (Dec. 17, 1980)

Federal Trade Commission, Privacy & Data Security Update: 2018 (2019)

Federal Trade Commission, Report to Congress under Section 319 of the Fair and Accurate Credit Transactions Act of 2003 (2012)

Federal Trade Commission, Start with Security: A Guide for Business: Lessons Learned from FTC Cases (2015)

Federal Trade Commission, "Strictly Business" Forum: Staff Perspective (2020)

Federal Trade Commission Staff Report, Internet of Things: Privacy & Security in a Connected World (2015)

Jeffrey Feinstein, LexisNexis White Paper, Alternative Data and Fair Lending (2013)

Deirdre Fernandes, Lenders Eye Social Media for Clues, Boston Globe (Sept. 4, 2016)

Marian Fernandez Vidal & David Medine, Focus Note, Is Data Privacy Good for Business?, Consultative Group to Assist the Poor (2019)

FTC v. Wyndham Worldwide Corp., 799 F.3d. 236 (3d Cir. 2015)

Patrice Ficklin, Blog, Preventing Illegal Discrimination in Auto Lending, Consumer Financial Protection Bureau (Nov. 4, 2013)

FICO, FICO Introduces New FICO Score 10 Suite, PR Newswire (Jan. 23, 2020)

FICO, Introducing the Ultra-FICO Score, fico.com (visited Feb. 8, 2020)

FICO Decisions, Can Alternative Data Expand Credit Access, White Paper No. 90 (2015)

The Financial Brand, Banking's Digital Talent Crisis: Who Will Fill the Tech Void?, thefinancialbrand.com (Jan. 16, 2018)

Financial Data and Technology Association, Credential-Based Authentication: A Necessary Tool to Enable Consumer and Small Business Data Access for the Foreseeable Future (undated)

Financial Data and Technology Association, FDATA North America: Consumers and Small Businesses Lack Critical Access to Their Own Data Fields, fdata.global (Feb. 13, 2020)

Financial Data Exchange, Members, fdx.com (visted Feb. 8, 2020)

Financial Data Exchange, Press Release, Ally, Discover, MassMutual, and TransUnion Among 25 New Members Joining the Financial Data Exchange (Jan. 27, 2020)

Financial Data Exchange, Press Release, Financial Data Exchange Adds 16 Members (Feb. 25, 2019)

Financial Data Exchange, Press Release, Financial Data Exchange Adds 11 New Members, Makes API Publicly Available (May 28, 2019)

Financial Data Exchange, Press Release, The Financial Data Exchange Reports Strong First-Year Growth; Now Protecting Online Financial Data for Five Million Consumers, including Business Customers, through 72-Member Network (Nov. 6, 2019)

Financial Data Exchange, The ABC's of APIs (2019)

Financial Data Exchange, The Global Industry Standard for Consumer Access to Financial Data: Organization Overview (2019)

Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services (2017)

Financial Stability Board, BigTech in Finance: Market Developments and Potential Financial Stability Implications (2019)

Financial Stability Board, Financial Stability Implications from FinTech: Supervisory and Regulatory Issues That Merit Authorities' Attention (2017)

Finicity, Consumer Reporting Agency, finicity.com (visited Feb. 8, 2020)

Finicity, OAuth Connections Guide (Oct. 16, 2019)

FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (2019)

FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Policy Overview (2020)

FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Small Business Spotlight (2019)

Hollis Fishelson-Holstine, Credit Scoring's Role in Increasing Homeownership for Underserved Populations, in Nicolas P. Retsinas & Eric S. Belsky, eds., Building Assets, Building Credit (2005)

Christopher L. Foote et al., Technological Innovation in Mortgage Underwriting and the Growth in Credit, 1985–2015, Federal Reserve Bank of Boston Working Paper 19-11 (2019)

Geoffrey A. Fowler, How We Survive the Surveillance Apocalypse, Wash. Post (Dec. 31, 2019)

W. Scott Frame et al., Credit Scoring and the Availability of Small Business Credit in Low- and Moderate-Income Areas, 39 Fin. Rev. (2004)

Joshua M. Frank, Analysis of Federal Reserve Research on Behavioral Scoring, Center for Responsible Lending Research Comment (2010)

Terri Friedline & Zibei Chen, Digital Redlining and the Fintech Marketplace: Evidence from U.S. Zip Codes (2019)

Steve Fromhart & Chris Moller, Funding Takes Center Stage for Nonbank Online Lenders, Deloitte Insights (July 9, 2018)

Hiroshi Fujii et al., E-Aggregation: The Present and Future of Online Financial Services in Asia-Pacific, MIT Composite Information Systems Laboratory Working Paper 2002-06 (September 2002)

Mark Furletti, An Overview and History of Credit Reporting, Federal Reserve Bank of Philadelphia, Payment Cards Center Discussion Paper (2002)

Donna Fuscaldo, Plaid Buys Quovo in Its First Major Acquisition, Forbes (Jan. 8, 2019)

Gallup, The Gig Economy and Alternative Work Arrangements (2018)

Peter Ganong & Pascal Noel, Liquidity vs. Wealth in Household Debt Obligations: Evidence from Housing Policy in the Great Recession, National Bureau of Economic Research Working Paper No. 24964 (August 2018)

Michael Gaughan, Commentary: FinTech and the Liberation of the Community Reinvestment Act Marketplace, Cityscape 187 (2017)

GDS Link, The Evolution of Bank Transaction Data (2019)

Nizan Geslevich Packin, Big Banks Vs. Silicon Valley Startups: Whose Customer Financial Data Is It Anyway?, Forbes (Apr. 19, 2019)

Julia Alpert Gladstone, Data Mines and Battlefields: Looking at Financial Aggegrators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data, 2 J. of Computer & Info. Law 313 (2001)

Matthew Goldberg, 10 of the Biggest Data Breaches over the Last Decade, Bankrate.com (Dec. 17, 2019)

Goldman Sachs Global Markets Institute, Who Pays for Bank Regulation? (2014)

Itay Goldstein et al., FinTech and the New Financial Landscape, Banking Perspectives (Mar. 12, 2019)

Lisa Goetz, How Do Mortgage Lenders Check and Verify Bank Statements?, Investopedia (Jul. 7, 2019)

Laurie Goodman, In Need of an Update: Credit Scoring in the Mortgage Market, Urban Institute (2017)

Google, How Google Anonymizes Data, Google.com (visited Feb. 8, 2020)

Google AI, Federated Learning: Building better products with on-device data and privacy by default, Google.com (visited Feb. 8, 2020)

Peter Gordon Roetzel, Information Overload in the Information Age, 12 Bus. Research 479 (2019)

Andrew Granato & Andy Polacek, The Growth and Challenges of Cyber Insurance, Federal Reserve Bank of Chicago Letter No. 426 (2019)

Victoria Guida, Banks, Fintech Startups Clash over 'the New Oil'—Your Data, Politico (Feb. 7, 2020)

Ian Hall, Australia Delays Launch of 'Open Banking' Regime, Global Government Forum (Jan. 9, 2020)

Harvard University Privacy Tools Project, Differential Privacy, Harvard University (visited Feb. 8, 2020)

Yuka Hayashi, Venmo Glitch Opens Window on War Between Banks, Fintech Firms, Wall St. J. (Dec. 14, 2019)

Hartzog & Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 Geo. Washington L. Rev. 2230 (2015)

Statement by Becky Heironimus, Capital One Financial Corporation, for the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records (Feb. 18, 2020)

John Heltman, Is Regulation Really Keeping Banks from Lending?, Am. Banker (Aug. 8, 2017)

Will Hernandez, Can Core Providers and Small Banks Settle Grievances in 2019?, Am. Banker (Dec. 28, 2018)

Will Hernandez, The Changing Shape of Bank-Fintech Partnerships, Am. Banker (Oct. 29, 2019)

Luke Herrine, Credit Reporting's Vicious Cycles, 40 N.Y.U. Rev. Law & Social Change 305 (2016)

Jon Hilsenrath, After Record-Long Expansion, Here's What Could Knock the Economy Off Course, Wall St. J. (June 3, 2019)

Jeanne M. Hogarth & Ellen A. Merry, Designing Disclosures to Inform Consumer Financial Decisionmaking: Lessons Learned from Consumer Testing, Fed. Res. Bulletin (August 2011)

Bradley Hope, Provider of Personal Finance Tools Tracks Bank Cards, Sells Data to Investors, Wall St. J. (Aug. 6, 2015)

John Howat, Full File Utility Credit Reporting: Harms to Low Income Consumers, National Consumer Law Center (2009)

Anna Hrushka, Banks to Tighten Third-Party Data Access in 2020, Experts Say, BankingDive (Jan. 7, 2020)

Daniel Huang & Peter Rudegeair, Bank of America Cut Off Finance Sites from Its Data, Wall St. J. (Nov. 9, 2015)

Cameron Huddleston, 50% of Americans Are Cheating—on Their Bank, GOBankingRates.com (Jan. 17, 2019)

Hunton & Williams, Client Alert: Where Are We Now: A Look at the EFTA's Prohibition of Compulsory Payments of Loans by Electronic Fund Transfers (2017)

Mikella Hurley & Julius Adebayo, Credit Scoring in the Era of Big Data, 18 Yale J.L. & Tech. 148 (2016)

IBM Marketing Cloud, 10 Key Marketing Trends for 2017 (2016)

Identity Theft Resource Center, 2018 End-of-Year Data Breach Report (2019)

Oana Ifrim, Open Banking—A Very Global Business, paypers.com (Dec. 19, 2019)

Institute of International Finance, Liability and Consumer Protection in Open Banking (2018)

Julapa Jagtiani & Catharine Lemieux, Do Fintech Lenders Penetrate Areas That Are Underserved by Traditional Banks?, 100 J. of Econ. & Business 43 (2018)

Julapa Jagtiani & Catharine Lemieux, The Roles of Alternative Data and Machine Learning In Fintech Lending: Evidence from the LendingClub Consumer Platform, Federal Reserve Bank of Philadelphia Working Paper 18-15 (updated January 2019)

Julapa Jagtiani & Wenli Li, Credit Access After Consumer Bankruptcy Filing: New Evidence, 89 Am. Bankruptcy L.J. 327 (2015)

Robert M. Jaworski, US National Credit Reporting Agencies to Amend Practices, E-Finance & Payments Law & Policy (2015)

Joseph Jerome, Financial Dashboards: Enhancing User Control Outside a Traditional 'Privacy Dashboard,' Center for Data & Technology (Sept. 27, 2017)

Jason Jones, 2017 Will Be a Huge Year for Bank Partnerships, Lend Academy (Nov. 14, 2016)

Leslie John, We Say We Want Privacy Online, But Our Actions Say Otherwise, Harvard Business Review (Oct. 16, 2015)

Leslie K. John et al., Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information, J. of Consumer Research (February 2011)

Heidi Johnson & Jesse Leary, Policy Watch: Research Priorities on Disclosure at the Consumer Financial Protection Bureau, 36 J. Pub. Policy & Marketing 184 (2017)

JPMorgan Chase, Press Release, JPMorgan Chase, Envestnet Yodlee Sign Agreement to Increase Customers' Control of Their Data, businesswire.com (Dec. 5, 2019)

JPMorgan Chase, Press Release, Plaid Signs Data Agreement with JPMorgan Chase, media.chase.com (Oct. 22, 2018)

JPMorgan Chase Institute, Estimating Family Income from Administrative Banking Data: A Machine Learning Approach (2018)

Dave Keever & Chris Sifter, Does Your Bank Have the Stress Testing Data You Need?, bankdirector.com (Sept. 26, 2016)

Jarred Keneally, Blog, Intuit Financial Data APIs (CAD) Update, intuit.com (Mar. 15, 2016)

Henry King, 5 Ways That Standardization Can Lead to Innovation, Fast Company (Aug. 3, 2011)

Aaron Klein & Scott R. Anderson, A Federal Backstop for Insuring Against Cyberattacks? Brookings Institute (Sept. 27, 2019)

Sarah Kocianski, How Banks Are Driving the Evolution of Personal Financial Management, Forbes (Nov. 2, 2018)

Donald Kohn & Nellie Liang, Understanding the Effects of the U.S. Stress Tests, Brookings Institution (July 9, 2019)

Alex Konrad, Fintech's Happy Plumbers, Forbes (April 12, 2018)

Roman Kraussl et al., The Performance of Marketplace Lenders: Evidence from Lending Club Payment Data (November 2019)

Brian Krebs, The Risk of Weak Online Banking Passwords, krebsonsecurity.com (Aug. 5, 2019)

Andrew Latham, 2019 Personal Loans Industry Study, Supermoney (Aug. 9, 2019)

W.A. Lee, Opt-Out Notices Give No One a Thrill, Am. Banker (July 10, 2001)

Stefan Lembo Stolba, Blog, Can Experian Boost Lower My Credit Score?, experian.com (Oct. 4, 2019)

Stefan Lembo Stolba, Blog, What Is Experian Boost?, experian.com (Oct. 15, 2019)

Lending Club, Banks and Lending Club, lendingclub.com (visited Feb. 11, 2020)

Wei Li et al., The Lasting Impact of Foreclosures and Negative Public Records, Urban Institute Housing Policy Finance Center (2016)

Barbara J. Lipman & Ann Marie Wiersch, Alternative Lending Through the Eyes of 'Mom & Pop' Small Business Owners: Findings from Online Focus Groups, Federal Reserve Bank of Cleveland 17 (2015)

Barbara J. Lipman & Ann Marie Wiersch, Browsing to Borrow: 'Mom & Pop' Small Business Perspectives on Online Lenders, Board of Governors of the Federal Reserve System (2018)

Barbara J. Lipman & Ann Marie Wiersch, Uncertain Terms: What Small Business Borrowers Find When Browsing Online Lender Websites, Board of Governors of the Federal Reserve System (2019)

James B. Lockhart III, Why Fannie and Freddie Need Newer Credit Scoring Models, Roll Call (Apr 8, 2019)

Cara Lombardo & AnnaMaria Andriotis, Visa to Pay $5.3 Billion for Fintech Startup, Wall St. J. (Jan. 13, 2020)

Heather Long, After a Summer of Panic, Fears of a U.S. Recession Ease a Bit, Wash. Post (Nov. 5, 2019)

Joseph Lorenzo Hall, Blog, The Beginning of the End for Sharing Bank Credentials, Center for Data & Technology (Jan. 25, 2017)

Marshall Lux & Guillaume Delepine, Revolution in Data: How New Technologies Are Upending Borrowing, Harvard Kennedy School Mossavar-Rahmani Center for Business & Government Associate Working Paper Series No. 107 (February 2019)

Mark MacCarthy, Fairness in Algorithmic Decision-Making, Brookings Institute (Dec. 6, 2019)

Tanaya MacHeel, Why Customer Acquisition Is So Difficult for Financial Startups, Tearsheet (Nov. 7, 2017)

Mary Madden, Privacy, Security and Digital Inequality, Data & Society Research Institute (2017)

Mary Madden et al., Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans, 95 Wash. U.L. Rev. 53 (2017)

David Maher, The Trusted Intermediary Model: Supporting Both Privacy and Internet Services, International Association of Privacy Professionals (visited Feb. 8, 2020)

Jack Mardack, Layman's Guide to Machine Learning and Customer Data Privacy, Actian (Jan. 16, 2020)

Jim Marous, Can Community Banks and Credit Unions Survive in Today's Digital World?, thefinancialbrand.com (Oct. 19, 2017)

Rey Mashayekhi, With Plaid Acquisition, Visa Makes a Big Play for the 'Plumbing' That Connects the Fintech World, Fortune (Jan. 14, 2020)

Bett Mattson-Teig, How to Make Small-Dollar Lending Make Sense, Independent Banker (Feb. 1, 2019)

Joseph McCafferty, Compliance Staffing a Key Risk for Banks, Internal Audit 360 (May 28, 2019)

Aleecia M. McDonald & Lorrie Faith Cranor, The Costs of Reading Privacy Policies, I/S: A Journal of Law & Policy for the Information Society, vol. 4, issue 3 (2008)

Giulia McHenry et al., Digital and Financial Inclusion: How Internet Adoption Impacts Banking Status, National Telecommunications & Information Administration Working Paper (Aug. 31, 2017)

Signe-Mary McKernan, et al., Thriving Residents, Thriving Cities: Family Financial Security Matters for Cities, Urban Institute (2016)

McKinsey & Co., New Credit-Risk Models for the Unbanked (2012)

McKinsey Global Institute, The Age of Analytics: Competing in a Data-Driven World (2016)

Bethany McLean, Payday Lending: Will Anything Better Replace It?, The Atlantic (May 2016)

Brendan McMahan & Daniel Ramage, Blog, Federated Learning: Collaborative Machine Learning without Centralized Training Data, Google AI (April 6, 2017)

David Medine & Gayatri Murthy, Focus Note, Making Data Work for the Poor: New Approaches to Data Protection and Privacy, Consultative Group to Assist the Poor (2020)

Steven Melendez, Now Wanted by Big Credit Bureaus Like Equifax: Your 'Alternative' Data, fastcompany.com (Apr. 6, 2019)

Diana Milanesi, A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom, and the United States, Stanford-Vienna Transatlantic Technology Law Forum Working Paper No. 29 (2017)

Ron Miller, Plaid Expands Financial Service API to Include All US Banks, techcrunch.com (Feb. 5, 2019)

Zack Miller, Al Goldstein on Avant's Move into Powering Digital Lending for Banks with Amount, Tearsheet (Sept. 13, 2019)

Karen G. Mills, Fintech, Small Business and the American Dream [eBook] (2019)

Robert Moffitt & Sisi Zhang, The PSID and Income Volatility: Its Record of Seminal Research and Some New Findings, Annals of the American Academy of Political & Social Science (2018)

Luis Alberto Montezuma & Tara Taubman-Bassirian, How to Avoid Consent Fatigue, International Association of Privacy Professionals (Jan. 29, 2019)

Jonathan Morduch & Rachel Schneider: The Financial Diaries: How American Families Cope in a World of Uncertainty (2017)

Jonathan Morduch et al., An Invisible Finance Sector: How Households Use Financial Tools of Their Own Making, U.S. Financial Diaries (2014)

Rick Morgan, Clearing House Sets Data-Sharing Framework, But the Devil Is in the Detail, bankinnovation.net (Nov. 25, 2019)

Geoff Mulgan & Vincent Straub, The New Ecosystem of Trust, Nesta (Feb. 21, 2019)

Chris Myers, For Alternative Lenders to Be Successful, Differentiation Is Key, Forbes (Oct. 15, 2015)

MyFico, What's in my FICO Score?, myfico.com (visited Feb. 8, 2020)

Arvind Narayanan et al., A Precautionary Approach to Big Data Privacy (2015)

Shahien Nasiripour, Fintech Lenders Tighten Standards, Become More Like Banks, Bloomberg (Dec. 16, 2019)

National Consumer Law Center, Access to Utility Service (6th ed. 2018)

National Consumer Law Center, Data Gatherers Evading the FCRA May Find Themselves Still in Hot Water (2019)

National Consumer Law Center, Past Imperfect: How Credit Scores and Other Analytics "Bake In" and Perpetuate Past Discrimination (2016)

National Consumer Law Center, Solving the Credit Conundrum: Helping Consumers' Credit Records Impaired by the Foreclosure Crisis and the Great Recession (2013)

National Consumer Reporting Association, A Position on Non Traditional or Alternative Credit Data and the Equal Credit Opportunity Act. Regulation B (visited Feb. 8, 2020)

National Telecommunications and Information Administration, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities (2016)

New York City Comptroller, Making Rent Count: How NYC Tenants Can Lift Credit Scores and Save Money (2017)

Alfred Ng, Blog, Microsoft Wants a US Privacy Law That Puts the Burden on Tech Companies, CNET (May 20, 2019)

Chris Nichols, What Commercial Loans Matter for Banks, Center State Correspondent Division (Aug. 11, 2019)

The Nilson Report, Blog, 50 Largest U.S. Prepaid Card Issuers (July 31, 2019)

Laura Noonan, JPMorgan to Ban Fintech Apps from Using Customer Passwords, Fin. Times (Jan. 1, 2020)

Jonathan A. Obar & Anne Oeldorf-Hirsch, The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services, Information, Communication & Society 1 (June 2018)

Rourke L. O'Brien & Barbara Kiviat, Disparate Impact? Race, Sex, and Credit Reports in Hiring, American Sociological Association Socius (May 2018)

Office of the Comptroller of the Currency, Bulletin 1997-24 (May 20, 1997)

Office of the Comptroller of the Currency, Bulletin 2001-12 (Feb. 28, 2001)

Office of the Comptroller of the Currency, Bulletin 2011-12 (Apr. 4, 2011)

Office of the Comptroller of the Currency, Bulletin 2013-29 (Oct. 30, 2013)

Office of the Comptroller of the Currency, Bulletin 2013-40 (Nov. 26, 2013)

Office of the Comptroller of the Currency Bulletin 2017-21 (June 7, 2017)

Office of the Comptroller of the Currency, Bulletin 2018-14 (May 23, 2018)

Office of the Comptroller of the Currency, News Release 2017-118, Acting Comptroller of the Currency Rescinds Deposit Advance Product Guidance (Oct. 5, 2017)

Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010)

Oliver Wyman, A New Age in Mortgage (2017)

Oliver Wyman & Ideas42, Reimagining Financial Inclusion (2015)

Emma Olson, JPMorgan: US Banks to Adopt Standard API, PaymentEye (Jan. 16, 2020)

Open Banking Implementation Entity, Third Party Providers, openbanking.org.uk (visited Feb. 13, 2020)

Open Financial Exchange, About OFX (visited Feb. 8, 2020)

Opinion 05/2014 on Anonymisation Techniques (EU), Technical Report, Article 29 Data Protection Working Party (Apr. 10, 2014)

Organization for Economic Co-Operation and Development, New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments (2015)

Bev O'Shea, FICO XD: A Credit Score for Those with No Credit, nerdwallet (Jan. 24, 2019)

Bev O'Shea, UltraFICO Score Could Boost Credit Access for Consumers, nerdwallet (Jan. 24, 2019)

Maija Palmer, Fintech for Gig Workers Is the Next Big Untapped Market, Sifted (May 13, 2019)

Barry Paperno, Q&A: How Cardholder Behavior Can Impact Your Credit, creditcards.com (Nov. 9, 2017)

Kevin A. Park, Policy Brief, Risks of Risk-Based Pricing, UNC Center for Community Capital (2014)

Tom Parrent & George Haman, Updated Credit Scoring and the Mortgage Market, Quantilytic (2017)

HIPAA Journal, Patient Privacy and Security Are Greatest Healthcare Concerns for Consumers, hipaajournal.com (Jul. 10, 2018)

PaymentsJournal, FICO Scores Used in Over 90% of Lending Decisions According to New Study, Mercator Advisory Group (Feb. 27, 2018)

PaymentsJournal, How Many Bank Accounts Do Consumers Have?, Mercator Advisory Group (July 2, 2019)

Payments Source, Capital One Restricts Third-Party Data Access, Upsets Customers, paymentssource.com (June 27, 2018)

Brendan Pederson, Bad Actors Targeting Fintech Aggregators: Fincen Chief, Am. Banker (Sept. 24, 2019)

David W. Perkins, Marketplace Lending: Fintech in Consumer and Small-Business Lending, Congressional Research Service (updated Sept. 4, 2018)

Andrew Perrin & Erica Turner, Blog, Smartphones Help Blacks, Hispanics Bridge Some—But Not All—Digital Gaps with Whites, Pew Research Center (Aug. 20, 2019)

Petra Persson, Attention Manipulation and Information Overload, Behavioural Public Policy 78-106 (May 2018)

Pew Charitable Trusts, Issue Brief: How Income Volatility Interacts with American Families' Financial Security (2017)

Pew Charitable Trusts, The Precarious State of Family Balance Sheets (2015)

Pew Charitable Trusts, How Do Families Cope with Financial Shocks? The Role of Emergency Savings in Family Financial Security (2015)

Pew Charitable Trusts, Why Americans Use Prepaid Cards: A Survey of Cardholders' Motivations and Views (2014)

Matt Phillips, Risky Borrowing Is Making a Comeback, but Banks Are on the Sideline, N.Y. Times (June 11, 2019)

Ping Identity, 2018 Consumer Survey: Attitudes and Behavior in a Post-Breach Era (2018)

John Pitts, Letter to Chairman Mike Crapo and Ranking Member Sherrod Brown, Senate Committee on Banking, Housing and Urban Affairs (Mar. 15, 2019)

John Pitts & Sam Taussig, Plaid, Kabbage: Clearing House Model Agreement Creates "Uneven Playing Field," bankinnovation.net (Dec. 6, 2019)

Plaid, Financial Data Access Methods: Creating a Balanced Approach (2016)

Policy & Economic Research Council, Alternative Data in the US: Progress, Promise, and Paralysis (2019)

Policy & Economic Research Council & Brookings Institution Urban Markets Initiative, Give Credit Where Credit Is Due (2006)

Nathaniel Popper, Banks and Tech Firms Battle Over Something Akin to Gold: Your Data, N.Y. Times (Mar. 23, 2017)

Nathaniel Popper & Michael J. de la Merced, Dealbook, Intuit to Buy Credit Karma to Create Financial Data Giant, N.Y. Times (Feb. 24, 2020)

PYMNTS, Fidelity Teams with TCH to Launch Personal Data Startup, pymnts.com (Feb. 20, 2020)

PYMNTS, Open Banking Overcomes the Data Obstacle of Paper, pymnts.com (Dec. 30, 2019)

PYMNTS, US Bank Launches Loan to Compete with Payday Lenders, pymnts.com (Sept. 11, 2018)

PwC, Consumer Intelligence Series: Protect.me (2017)

QED Investors & Oliver Wyman, The Brave 100: The Battle for Supremacy in Small Business Lending (2015)

Lee Rainie & Maeve Duggan, Privacy and Information Sharing, Pew Research Center (2016)

David Reinsel et al., Data Age 2025: The Digitization of the World from Edge to Core, IDC (2018)

Peter Renton, The Inevitable Movement Towards No Overdraft Fees, Lend Academy (Sept. 23, 2019)

Jonathan Riber & Christopher D'Onofrio, U.S. Structured Finance Newsletter: Student Loan Refinance Sector—Not All Free Cash Flow Is Created Equal, Morningstar/DBRS (2019)

Lisa Rice & Deidre Swesnik, Discriminatory Effects of Credit Scoring on Communities of Color, 46 Suffolk L. Rev. 935 (2013)

Luc Rocher et al., Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models, 10 Nature Communications 3069 (2019)

Kate Rooney, Meet the Start-Up You've Never Heard of That Powers Venmo, Robinhood, and Other Big Consumer Apps, CNBC (Oct. 4, 2018)

Elizabeth Rosenthal, News Analysis, I Disclose ... Nothing, N.Y. Times (Jan. 21, 2012)

Andrew Rossow, The Birth of GDPR: What Is It And What You Need To Know, Forbes (May 25, 2018)

Peter Rudegair et al., Big Banks Find a Back Door to Finance Subprime Loans, Wall St. J. (Apr. 10, 2018)

Anton Ruddenklau, Tech Giants in Financial Services: Is Collaboration the Way Forward?, KPMG (2018)

Sam Sabin, Most Voters Say Congress Should Make Privacy Legislation a Priority Next Year, Morning Consult (2019)

David Sanchez et al., How to Avoid Reidentification with Proper Anonymization (2018)

SAS, Data Privacy: Are You Concerned? Insights from a Survey of US Consumers (2018)

Lauren Saunders, National Consumer Law Center, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology (Nov. 21, 2019)

Lauren Saunders, Fintech and Consumer Protection: A Snapshot, National Consumer Law Center (2019)

Salvatore Scanio & Jason W. Glasgow, Payment Card Fraud, Data Breaches, and Emerging Payment Technologies, 21 Fidelity L.J. 59 (2015)

Pete Schroeder & Anna Irrera, JPMorgan Sets July Deadline for Fintechs to Sign New Data Access Deals: Sources, Reuters (Feb. 13, 2020)

Mark Schwanhausser, Blog, Intuit Is Selling Quicken: Will Banks Seize the Moment?, javelinstrategy.com (Aug. 21, 2015)

Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev. 1085 (2018)

Senate Committee on Banking, Housing, and Urban Affairs, Hearing, Financial Privacy and Consumer Protection (2002) (testimony of Fred H. Cate and John C. Dugan)

Senate Committee on Banking, Housing, and Urban Affairs, Hearing, The Fair Credit Reporting Act and Issues Presented by Reauthorization of the Expiring Preemption Provisions (2008) (written responses of Martin Wong)

Pete Sepp & Thomas Aiello, Risky Road: Assessing the Costs of Alternative Credit Scoring, National Taxpayers Union (Mar. 21, 2019)

Ron Shevlin, Gig Economy Banking Is Booming (And Banks Are Missing The Boat), Forbes (Sept. 23, 2019)

Ron Shevlin, The Real Story Behind The PNC-Venmo Clash, Forbes (Dec. 18, 2019)

Ron Shevlin, What's Visa Going to Do with Plaid?, Forbes (Jan. 20, 2020)

Baker Shogry, Blog, Making Sense of Messy Bank Data, Plaid (updated Nov. 21, 2018)

Robin Sidel, Big Banks Lock Horns with Personal-Finance Web Portals, Wall St. J. (Nov. 4, 2015)

Tara Siegel Bernard, Your Credit Scores May Soon Change. Here's Why, N.Y. Times (Jan. 25, 2020)

Singapore Personal Data Commission, Guide to Basic Data Anonymization Techniques (2018)

Pramod Singh, Blog, Enriched Data for Better Banking Decisions, Envestnet/Yodlee (Oct. 5, 2018).

Michelle Singletary, Sallie Mae, Moving in Slo-Mo, Wash. Post (Feb. 29, 2004)

Skadden, California Consumer Privacy Act: A Compliance Guide (2019)

David Skanderson & Dubravka Ritter, Fair Lending Analysis of Credit Cards, Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper 34-40 (August 2014)

Sarah Skidmore Sell, FICO to Test New Type of Credit Score That May Help Those with Weaker Credit, Chicago Times (Oct. 22, 2018)

Aaron Smith, FactTank, Half of Online Americans Don't Know What a Privacy Policy Is, Pew Research Center (Dec. 4, 2014)

Andrew Smith, Federal Trade Commission, Testimony before the House Committee on Oversight and Reform Subcommittee on Economic and Consumer Policy (Mar. 26, 2019)

Steve Smith, How Data Aggregation Can Shake Up Credit Decisioning, infoworld.com (Dec. 15, 2017)

David S. Smith et al., Memo: The Future of Income Volatility Research, Aspen Institute (2017)

S&P Global Market Intelligence, 2018 US Digital Lending Market Report (2018)

Evan Sparks, How to Understand and Partner with Marketplace Lenders, ABA Banking Journal (Feb. 17, 2016)

Special Issue: Household Economic Instability and Social Policy, 91 Soc. Service Rev. 371-584 (2017)

Sarah Spiekermann et al., E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior, EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce (2001)

Ann H. Spiotto, Financial Account Aggregation: The Liability Perspective, Fordham J. of Corp. & Fin. Law 557 (2003)

Square, Payment Tokenization Explained, square.com (visited Feb. 11, 2020)

Jay Stanley, Blog, Do Young People Care about Privacy, aclu.org (Apr. 29, 2013)

Michael Staten, Risk-Based Pricing in Consumer Lending, Center for Capital Markets Competitiveness (2014)

Catherine Stupp, Companies Scramble to Respond to Spam GDPR Requests, Wall St. J. Pro (Nov. 25, 2019)

Bob Sullivan, The Simple Chart That Can Explain Why Your Credit Score Dropped, credit.com (Jan. 13, 2015)

Richard J. Sullivan, Controlling Security Risk and Fraud in Payment Systems, Federal Reserve Bank of Kansas City, Economic Perspectives 47 (3rd quarter 2014)

Jennifer Surane, Big Banks' Clampdown on Data Puts Silicon Valley Apps on Alert, Bloomberg (Mar. 26, 2019)

Jennifer Surane, Big Banks Want to Make It Easier to Share Consumer Data with Startups, Bloomberg (Nov. 12, 2019)

Jennifer Surane, Capital One Restricts Third-Party Data Access, Upsets Customers, Bloomberg (June 27, 2018)

Dan Svirksky, Why Are Privacy Preferences Inconsistent?, John M. Olin Center for Law, Economics, and Business, Fellows' Discussion Paper Series No. 81 (June 2018)

Jann Swanson, Freddie Mac Announces More "Big Data" Tools, Mortgage News Daily (Oct. 15, 2018)

Jann Swanson, Lenders: Income Verification Needs for "Gig" Economy, Mortgage News Daily (May 21, 2018)

Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University Data Privacy Working Paper 3 (2000)

Peter P. Swire, The Surprising Virtues of the New Financial Privacy Law, 86 Minn. L. Rev. 1263 (2002)

Statement of Natalie S. Talpas, PNC Bank, for the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records (Feb. 26, 2020)

Huan Tang, Peer-to-Peer Lenders Versus Banks: Substitutes or Complements?, 32 Rev. of Fin. Studies 1900 (2019)

Gregory Tassey, Standardization in Technology-Based Markets, 29 Research Policy 587 (2000)

Matt Tatham, Blog, More Than 1 Million Americans Have Improved Their FICO® Scores with Experian Boost, experian.com (Dec. 13, 2019)

Allen Taylor, The Rise of Marketplace Lending Securitization, Lending Times (Dec. 19, 2018)

Winnie F. Taylor, Meeting the Equal Credit Opportunity Act's Specificity Requirement: Judgmental and Statistical Scoring Systems, 29 Buff. L. Rev. 73 (1980)

Mekebeb Tesfaye, Financial Service Consumers Are Willing to Share Their Personal Data for Benefits and Discounts, Business Insider (Mar. 18, 2019)

Texas Dep't of Housing & Community Affairs v. Inclusive Communities Project, Inc., 135 S. Ct. 2507 (2015)

Richard H. Thaler & Cass R. Sunstein, Nudge: Improving Decisions about Health, Welfare, and Happiness (2008)

Kwamina Thomas Williford & Brian J. Goodrich, Why Data Sources Aren't Furnishers under Credit Report Regs, hklaw.com (Sept. 25, 2019)

Ben Thompson, Visa, Plaid, Networks, and Jobs, Stratechery (Jan. 14, 2020)

Ryan Tracy, Lawmakers Call for Investigation of Fintech Firm Yodlee's Data Selling, Wall St. J. (Jan. 17, 2020)

TradeIt Blog, Aggregation Wars, Part 1: Near History, blog.trade.it (Jan. 18, 2017)

TransUnion, Press Release, FinTechs Continue to Drive Personal Loan Growth, transunion.com (Feb. 21, 2019)

TransUnion, Press Release, TransUnion Analysis Finds Reporting of Rental Payments Could Benefit Renters in Just One Month, transunion.com (2014)

TransUnion, Press Release, TransUnion Reveals Almost Half of Landlords Consider Renters' Credit Health as a Key Factor in Leasing Decision, transunion.com (May 12, 2014)

Edward L. Truitt Jr. & James Lawler, Marketplace Lending ABS Moves Closer to Mainstream, Maples Group (2019)

Michael Turner & Patrick Walker, Potential Impacts of Credit Reporting Public Housing Rental Payment Data, U.S. Department of Housing & Urban Development & Policy and Economic Research Council (2019)

Joseph Turow et al., The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, University of Pennsylvania (2015)

John Ulzheimer, Blog, The Best Kept Secret in Lending, Bar None, mint.com (March 14, 2011)

United Kingdom Information Commissioner's Office, When Can We Rely on Legitimate Interests?, ico.org.uk (visited Feb. 8, 2020)

Roy Urrico, Aggregators Banned From NCR's Digital Banking Platform Amid Account Takeovers, Credit Union Times (Nov. 6, 2019)

U.S. Chamber of Commerce Technology Engagement Center & Political & Economic Research Council, Data Flows, Technology, & the Need for National Privacy Legislation (2019)

U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation (2018)

U.S. Department of the Treasury, Opportunities and Challenges in Online Marketplace Lending (2016)

U.S. Government Accountability Office, Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies (2019)

U.S. Government Accountability Office, Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach (2018)

U.S. Government Accountability Office, Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight (2018)

U.S. Government Accountability Office, Financial Technology: Agencies Should Provide Clarification on Lenders' Use of Alternative Data (2018)

U.S. Government Accountability Office, Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data (2006)

U.S. House of Representatives Committee on Financial Services, Hearing, Credit Reports: Consumers' Ability to Dispute and Change Inaccurate Information (June 19, 2007)

U.S. House of Representatives Committee on Financial Services, Subcommittee on Financial Institutions & Consumer Credit, Hearing, An Examination of the Availability of Credit for Consumers (Sept. 22, 2011)

Bart van Liebergen, Machine Learning: A Revolution in Risk Management and Compliance?, 45 Capco Inst. J. of Fin. Transformation 60 (Apr. 2017)

VantageScore, Improved Assessment of Credit Health Using Trended Credit Data (2019)

VantageScore, Press Release, Annual Survey Reveals that Consumer Knowledge about Credit Scores Has Steadily Declined Over the Past Eight Years (June 10, 2019)

VantageScore, What Influences Your Score?, yourvantagescore.com (visited Feb. 8, 2020)

Julie Verhage, Visa's Plaid Takeover Signals Wave of Fintech Dealmaking, Bloomberg (Jan. 15, 2020)

Julie Verhage & Tom Metcalf, Plaid's Founders Are Latest Fintech Royalty with Visa Deal, Bloomberg (Jan. 14, 2020)

Julie Verhage & Jennifer Surane, Big Tech Is Coming for Banking: Experts Predict Fintech's 2020, Bloomberg (Dec. 23, 2019)

Lisette Voytko, Report: FICO Credit Score Adjustments Could Hurt Consumers with Growing Debt, Forbes (Jan. 23, 2020)

J. Christina Wang, Technology, the Nature of Information, and FinTech Marketplace Lending, Federal Reserve Bank of Boston Current Policy Perspectives No. 18-3 (Oct. 2018)

Rep. Maxine Waters et al., Letter to the Hon. Gene L. Dodaro (Jan. 16, 2020)

N. Eric Weiss & Rena S. Miller, The Target and Other Financial Data Breaches: Frequently Asked Questions, Congressional Research Service (2015)

Wells Fargo, Customers Will Have More Control, Convenience and Transparency When Sharing Financial Data with Plaid-Supported Fintech Apps, businesswire.com (Sept. 19, 2019)

Kristy Welsh, New Scoring Model Aimed at Those with No Credit Score, creditinfocenter.com (Sept. 26, 2017)

Darrell M. West, TechTank, Brookings Survey Finds Three-Quarters of Online Users Rarely Read Business Terms of Service, Brookings Institution (May 21, 2019)

Liz Weston, Why Banks Want You to Drop Mint, Other 'Aggregators,' Reuters (Nov. 9, 2015)

Alan M. White, Risk-Based Mortgage Pricing: Present and Future Research, 15 Housing Policy Debate 503 (2004)

Gillian B. White, Can the Flaws in Credit Scoring Be Fixed? Not Easily, The Atlantic (Jan. 10, 2017)

Richard Whitt, To Fix the Web, Give It Back to the Users, Fast Company (Jan. 22, 2019)

Kimberly L. Wierzel, If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions, 5 N.C. Banking Inst. 457 (2001)

Kyle Wiggers, AI Has a Privacy Problem, But These Techniques Could Fix It, Venture Beat (Dec. 21, 2019)

Robin Wigglesworth & Keith Fray, The Record-Breaking US Economic Recovery in Charts, Fin. Times (July 4, 2019)

Colin Wilhelm, Citibank, Lending Club to Partner on CRA Loans, Am. Banker (Apr. 14, 2015)

Statement of Natalie R. Williams, JPMorgan Chase & Co., for the Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records (Feb. 26, 2020)

Kurt Wimmer & Gabe Maldoff, India Proposes Updated Personal Data Protection Bill, Inside Privacy, Covington (Dec. 12, 2019)

Cheryl Winokur Munk, How Community Banks Are Innovating from the Core, Independent Banker (Aug. 1, 2019)

Mary Wisniewski, 80% of Financial App Users Admit Not Fully Realizing Their Banking Credentials Are Shared: Survey, bankrate.com (Nov. 19, 2019)

Mary Wisniewski, Data Aggregation's New Frontier: Lending Decisions, Am. Banker (Mar. 6, 2017)

Mary Wisniewski, Fintechs' Vulnerability Apparent in Capital One Data-Access Flap, Am. Banker (June 29, 2018)

Mary Wisniewski, These Challenger Banks Killed the Overdraft Fee. Now, They're Reinventing It, Bankrate (Sept. 12, 2019)

Brian Wolfe & Woongsun Yoo, Crowding Out Banks: Credit Substitution by Peer-to-Peer Lending (Mar. 30, 2018)

World Economic Forum, The Appropriate Use of Customer Data in Financial Services (2019)

World Economic Forum, White Paper, The Appropriate Use of Customer Data in Financial Services (2018)

World Economic Forum & Deloitte, The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value (2019)

ChiChi Wu, National Consumer Law Center, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology (July 25, 2019)

Sen. Ron Wyden et al., Letter to Joseph J. Simons (Jan. 17, 2020)

Bryan Yurcan, Open Banking's Early Adopters Bet on 'Tremendous Value," Am. Banker (Feb. 1, 2018)

David A. Zetoony & Courtney K. Stout, Credit Card Data Breaches: Protecting Companies from Hidden Surprises, Lexis Practice Advisor Journal (Nov. 8, 2016)

Wenyu Zhang et al., Financial Forecasting and Analysis for Low-Wage Workers (2018)

Yan Zhang, Assessing Fair Lending Risks Using Race/ Ethnicity Proxies, 64 Management Science 178 (2018)

Nick Zulovich, TransUnion's New Scoring Tool Blends 2 Data Sets Together, autoremarketing.com (Oct. 9, 2015)

APPENDIX A

FinRegLab Policy Working Groups

FinRegLab convened more than 80 representatives of lenders, banks, data aggregators, advocacy organizations, researchers, and other stakeholders to engage in an extended dialogue about the challenges that are shaping both the adoption of cash-flow based underwriting and the underlying system for data transfers. Representatives of several federal banking agencies and the Consumer Financial Protection Bureau attended the sessions in an observer capacity.

This report was informed by the feedback of these and other stakeholders but represents FinRegLab's independent analysis in all respects. It does not necessarily accord with the views of the individual participants or their employers.

CASH-FLOW DATA IN UNDERWRITING WORKING GROUP PARTICIPANTS

- Alliance Partners LLC
- Allon Advocacy
- Bank of America
- Brigit
- Capital One
- Center for Financial Services Innovation
- Center for Responsible Lending
- Charles River Associates
- Citi
- Coinbase
- Columbia University
- Conference of State Bank Supervisors*
- Consumer Financial Protection Bureau*
- Consumers Union
- CoreLogic
- Federal Deposit Insurance Corporation*
- Federal Reserve Board*
- Federal Trade Commission*
- FICO
- Finicity
- Fundation
- Gibson, Dunn, & Crutcher LLP
- JP Morgan Chase
- Kabbage
- LendUp
- Marstone
- Mayer Brown
- Milken Institute
- National Consumer Law Center
- National Urban League
- New York University
- Office of the Comptroller of the Currency*
- Oliver Wyman
- Oportun
- Petal
- Plaid
- PNC
- Quovo
- Relman, Dane, & Colfax PLLC
- The Pew Charitable Trusts
- VantageScore Solutions
- Wells Fargo

APPENDIX B

Common Terms and Acronyms

Ability-to-repay: Ability-to-repay is a measure of an applicant's financial capacity or capability. In the process of evaluating an application for credit, firms have developed underwriting processes that estimate resources an applicant is likely to have to repay a loan under various conditions. In certain markets, such as credit cards and mortgages, such an analysis of a consumer's potential to perform under the loan is required by federal law. These resources might include income, assets, expenses, and other financial indicators.

Adverse action: An adverse action is a credit decision in which a lender declines to provide credit in the amount or terms requested or makes a negative change to an existing account. Federal law requires lenders to provide disclosures to consumers and small businesses after taking an adverse action to explain the principal reason(s) for the decision.

Alternative/Non-traditional data: These terms are commonly used to refer to any information that is not typically contained in traditional credit reports and/or credit applications (such as annual income). Alternative data evaluated as part of a credit decision can be financial in nature (such as deposit and payments history) or non-financial (such as the date, time, or place of a transaction).

API: Application Programming Interfaces are software-based communication protocols or functions between websites or applications, allowing them to exchange information and data using a common format. Compared to screen scraping (another data gathering technique), APIs can provide greater security, accuracy, and precision as to the scope of data sharing and predictability with regard to transfer costs.

Behavioral data: Behavioral data is a type of alternative data that firms may use in the context of credit underwriting and more widely. That includes a range of possible data, such as the date, time, or place of a transaction, digital activities, or social media data.

Cash-flow data: Cash-flow data is a type of alternative or non-traditional data that shows income, expenses, and other reserves. Cash-flow data can be derived from bank and prepaid accounts, small business accounting software, and other sources.

CCPA: The California Consumer Privacy Act took effect in January 2020, though enforcement will not start until later in the year. The CCPA provides consumers with various rights concerning data collected by businesses from their transactions and devices, including the right to information, the ability to opt out of certain data sales, and the right to demand deletion. Where firms respond to consumers' requests for access to their data in electronic form, the format must be readily transmittable to other companies. The CCPA excludes certain categories of personal information from its privacy protection, including information collected pursuant to the Fair Credit Reporting Act and Gramm-Leach-Bliley Act.

CFPB: The Consumer Financial Protection Bureau is a federal agency with authority to supervise, enforce, and write rules to implement certain federal consumer protection statutes, including the Equal Credit Opportunity Act (ECOA) and the Fair Credit Reporting Act (FCRA). The agency's supervision jurisdiction broadly encompasses major providers of consumer financial products and services. The CFPB was created pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

CDFIs: Community Development Financial Institutions are certified by the U.S. Department of the Treasury to serve low-income communities and are eligible for various types of assistance and programs. They are private financial institutions that fund small businesses, nonprofits, real estate and housing designed to help disadvantaged people via lending or banking advice. They are funded and certified through the Treasury CDFI Fund.

Consumer report: Consumer report (codified at 15 U.S.C. § 1681a(d)(1)) means any communication of any information by a consumer reporting agency relevant to a consumer's creditworthiness, character or general reputation which is used as a factor in establishing the consumer's eligibility for credit or insurance or employment purposes or for other activities defined by the Fair Credit Reporting Act.

CRAs: A consumer reporting agency (codified at 15 U.S.C. § 1681a(f)) is any firm which regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

Credit invisible: Individuals who do not have a file at one of the nationwide credit reporting agencies are commonly referred to as credit invisibles.

Customer-permissioned data transfers: This refers to the transfer of data between two firms that is initiated by the individual accountholder.

Data aggregators: Data aggregators are intermediaries that facilitate the acquisition and transfer of information between firms.

Disparate impact: Disparate impact is a framework for establishing legal liability for facially neutral practices that have unintended discriminatory effects on classes of persons protected under the Equal Credit Opportunity Act (ECOA) or Fair Housing Act (FHA). Disparate impact is a basis for evaluating whether discrimination has occurred that is distinct from disparate treatment.

Disparate treatment: Disparate treatment is a framework for establishing legal liability when a lender, seller, or landlord treats an individual differently during any aspect of a credit transaction based on one of the bases protected under the Equal Credit Opportunity (ECOA) Act or Fair Housing Act (FHA). It does not require any showing that the treatment was motivated by prejudice or a conscious intention to discriminate against a person beyond the difference in treatment itself.

Dodd-Frank Act: Passed in the aftermath of the financial crisis of 2008, The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (codified at Pub. L. No. 111-203, 124 Stat. 1376) affected almost every aspect of the nation's financial services industry and every federal financial regulatory agency. Foremost among these changes was the creation of the CFPB which consolidated consumer protection authorities previously exercised by several agencies in an independent agency for the first time.

ECOA: The Equal Credit Opportunity Act of 1974 is a federal statute (codified at 15 U.S.C. § 1691 et seq.) that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the basis of race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to contract); to the fact that all or part of the applicant's income derives from a public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act. ECOA is implemented by the Consumer Financial Protection Bureau through Regulation B (codified at 12 C.F.R. Part 1002).

EFTA: The Electronic Fund Transfer Act of 1978 is a federal statute (codified at 15 U.S.C. § 1601 et seq.) that establishes the rights and liabilities of consumers as well as the responsibilities of all participants in electronic funds transfer activities and remittance transfers. EFTA is implemented by the Consumer Financial Protection Bureau through Regulation E (codified at 12 C.F.R. Part 1005).

End user: End users are firms that seek an individual's permission to obtain his or her financial data from other institutions and acquire that information through aggregators, direct interfaces, or other means for the purposes of providing financial products or services to consumers or small businesses. Such firms may have a wide variety of uses for this data: evaluating an application for credit, servicing a loan, providing personal financial management services or advice, and providing payment-related services and products.

FCRA: The Fair Credit Reporting Act is a federal statute (codified at 15 U.S.C. § 1681 et seq.) enacted to protect consumers from the willful and/or negligent inclusion of inaccurate information in their credit reports and to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. FCRA regulates the collection, dissemination, and use of consumer information credit purposes as well as activities such as employment, insurance, and housing. It is implemented by the Consumer Financial Protection Bureau through Regulation V (codified at 12 C.F.R. Part 1022).

FDIC: The Federal Deposit Insurance Corporation is one of two federal agencies that provide deposit insurance to depositors in U.S. commercial banks and savings banks. The FDIC was created by the 1933 Banking Act. It supervises participants in the insurance fund within its jurisdiction to ensure that they operate in a safe and sound manner.

FDX: The Financial Data Exchange is a cooperative industry-body formed in late 2018 which promotes the adoption of a standardized API, related data specifications for particular use cases, and aims to improve authentication standards.

FHA: The Fair Housing Act refers to Titles VIII and IX of the Civil Rights Act of 1968 (codified at 42 U.S.C. § 3601 et seq.), which prohibit discrimination concerning the sale, rental, and financing of housing based on race, religion, and national origin. These prohibitions were subsequently extended to include discrimination based on sex, disability status, and family status. The Department of Housing and Urban Development implemented a portion of the FHA through a rule prohibiting practices with disparate impact.

FRB: The Board of Governors of the Federal Reserve System, also known as the Federal Reserve Board, refers to the governing body of the Federal Reserve System. Established by the Banking Act of 1935, the Federal Reserve Board is responsible for, among other things, monitoring, inspecting, and examining certain financial institutions to ensure that they operate in a safe and sound manner. The Federal Reserve supervises several kinds of institutions: bank and financial holding companies (the corporations that own banks and other financial operating units); state-chartered banks that are members of the Federal Reserve System; and various international banking operations. Prior to the Dodd-Frank Act, the Federal Reserve Board had primary responsibility for implementing many of the federal consumer protection statutes now under the aegis of the CFPB.

FTC: The Federal Trade Commission is a federal agency charged with protecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education. Its consumer protection function encompasses privacy and data security, including articulation of rules to implement the Gramm-Leach-Bliley Act. The FTC's jurisdiction reaches virtually every area of commerce, with some exceptions for banks, savings and loans, federal credit unions, insurance companies, and common carriers such as airlines. In financial services, the FTC's nonbank jurisdiction overlaps with that of the CFPB, and the two agencies have coordinated in areas like debt collection. Prior to the Dodd-Frank Act, the FTC had primary responsibility for implementing the Fair Credit Report Act and still retains enforcement authority.

Furnisher: Firms that choose to report consumer data to credit reporting agencies are generally furnishers. Firms that provide such information are required under the Fair Credit Reporting Act to implement front-end processes to promote accuracy and to investigate and resolve consumer disputes about the accuracy of specific information.

GDPR: The General Data Protection Regulation is a legal framework that requires businesses to protect the personal data and privacy of European Union (EU) citizens for transactions that occur within EU member states. It also addresses the transfer of personal data outside the EU and the European Economic Areas, GDPR covers all companies that deal with the data of EU citizens, including but not limited to banks, insurance companies, and other financial companies.

GLBA: The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, is a federal statute that contained, among other things, provisions that require financial institutions to explain how they share and protect their customers' private information. Financial institutions must communicate to their customers how they share the customers' data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution. Regulations promulgated by the FTC and prudential regulators differ in the specific compliance requirements they set forth, as well as in the nature and intensity of oversight.

Metro 2: Metro2 is a data specification created by the Consumer Data Industry Association for firms providing information to nationwide consumer reporting agencies designed to enable electronic furnishing in a standardized format. Metro 2 was adopted in 1997, but furnishers were not required to use it until the NCRAs entered settlements with several states in 2015 to stop accepting reports in previous formats by mid-2018.

NCRAs: The term Nationwide Consumer Reporting Agency refers to three primary companies (Equifax, Experian, and TransUnion) that are repositories of consumer credit information. These firms provide credit history reports show an individual's current credit obligations and past repayment history. NCRA credit reports, as well as generic credit scores derived from that information, are disproportionately used by lenders when evaluating applications for credit.

NCUA: The National Credit Union Administration is one of two federal agencies that provide deposit insurance to depositors in U.S. depository institutions. The NCUA is an independent federal agency created by the United States Congress to regulate, charter, and supervise federal credit unions. It supervises participants in the insurance fund within its jurisdiction to ensure that they operate in a safe and sound manner.

OCC: The Office of the Comptroller of the Currency is an independent bureau within the United States Department of the Treasury that was established by the National Currency Act of 1863 and serves to charter, regulate, and supervise all national banks and federal savings associations, as well as federal branches and agencies of foreign banks in the United States.

Open banking: Open banking refers to a system in which financial institutions are required to provide other firms their customers' financial information when so directed by individual customers. That information might be derived from use of consumer banking, investment, payments, or other financial products. Open banking can allow the networking of accounts and data across institutions for use by consumers, financial institutions, and third-party service providers.

Permissible purpose: Under the FCRA (as codified at 15 U.S. Code § 1681b), users of a consumer report must act with a permissible purpose in obtaining and using a report. One such permissible purpose is "to use the information in connection with a credit transaction," Including originating loans, reviewing accounts, and collections. Users of consumer reports generally do not need consumer consent to obtain the information so long as they have a permissible purpose.

PFM: Personal financial management services may be designed to help users manage daily finances, choose products and services that fit their needs and goals, achieve particular financial objectives, and / or improve their financial health. PFM services generally rely on customer-permissioned data transfers to provide users access to consolidated or holistic information about their financial condition.

Propensity-to-repay: Propensity-to-repay is a measure of an individual's likely willingness to repay a loan, regardless of his or financial capacity or capability to do so. It is generally evaluated based on an individual's prior repayment history.

Protected class: Like anti-discrimination statutes applicable in other areas, ECOA identifies protected classes or specific groups of people against whom it is illegal to discriminate unfairly. Those include race, color, religion, national origin, sex, marital status, or age (provided the applicant has the capacity to contract); reliance on a public assistance program; or those who have in good faith exercised any right under certain federal consumer financial laws.

Prudential regulators: Prudential regulators supervise financial firms for compliance with a type of financial regulation that seeks to ensure that regulated entities operate in a safe and sound manner by controlling risks and holding adequate capital given the size and complexity of their operations. Capital and liquidity requirements, concentration risk limits, and enterprise risk management are examples of prudential regulatory expectations. In the U.S. financial system, the FDIC, the Federal Reserve, NCUA, and the OCC are examples of prudential regulators.

PSD2: The term PSD2 is used to describe two separate but interrelated initiatives. PSD2 refers to a major component of the United Kingdom's open banking initiative that took effect in January 2018 and requires the nation's nine largest banks to comply with customers' directions to share standardized payments data online with firms certified by the Financial Services Authority. The initiative will expand to other financial products and services over time. The term also refers to Revised Payment Services Directive 2 (Directive (EU) 2015/2366), EU legislation aimed at enhancing protections for online payments and promoting the development and use of innovative online and mobile payments. Although the UK actions are an outgrowth of EU legislation, they are not expected to be reversed as the U.K. withdraws from the Union.

Risk-based pricing: Risk-based pricing refers to a common approach for evaluating an applicant's creditworthiness and determining the cost of credit for that individual. In this system, lenders offer different consumers interest rates or other loan terms based on the estimated risk that each individual consumer will fail to pay back the loan. This generally means that an applicant with a good credit score and employment record will be offered a lower interest rate, whereas someone who has previously fallen behind on loan payments or declared bankruptcy will receive an offer with a higher interest rate for a loan of the same kind and amount. Under risk-based pricing, each lender uses its own process to estimate the risk that an individual will not be able to repay a loan, but most lenders rely on third-party credit scores, employment status, income, and outstanding debts, among other factors.

Section 1033: This Dodd-Frank Act provision (codified at 15 U.S.C. § 5533) directs certain financial services companies to make available to a consumer upon request financial account and transaction data concerning a product or service obtained from that company. The CFPB is directed to right regulatons under the law.

Screen scraping: Screen scraping refers to the dominant method of third-party data collection. To collect data by screen scraping, proprietary software copies information displayed on the data source's customer-facing webpages. Where such information is password-protected, the individual whose data is being collected generally provides his or her username and password to firms authorized to acquire and use the data. Those credentials allow the firm acquiring the data to interface with the website or app as if it were the individual accountholder, such that the company has the technological ability to access any data that can be seen by the accountholder and to conduct transactions in the account.

Shoebox rule: The shoebox rule refers to a provision of the Equal Credit Opportunity Act (codified at 12 C.F.R. § 1002.6(b)(6); supp. I cmt. 6[b][6]-1) that requires lenders who consider credit history or other information from credit bureaus in their underwriting processes to give further consideration if applicants provide comparable information from other sources, such as a shoebox of bank statements or receipts.

Specialty CRAs: Specialty CRAs produce reports that may focus on repayment of specific types of expenses, such as rent or very short-term loans that are not typically reported the NCRAs, or of specific types of credit obligations, such as short-term loans. Some product-specific firms have been acquired by NCRAs in recent years.

Third-party service provider: A third-party service provider is a firm that provides products or services to regulated financial institutions. Depending on the nature of the product or service being provided and the relationship between the third-party and regulated entity, the third party may be responsible for meeting the regulatory requirements of its clients and subject to oversight by its clients' regulators under the Bank Service Company Act and the Dodd-Frank Act.

TILA: The Truth in Lending Act of 1968 is a federal statute (codified at 15 U.S.C. § 1601 et seq.) that is designed to promote the informed use of consumer credit. It applies to open- and closed-end products and requires disclosures about its terms and cost to standardize the manner in which costs associated with borrowing are calculated and disclosed. For certain products, it also requires consideration of specific information to evaluate a credit applicant's ability to repay. TILA is implemented by the Consumer Financial Protection Bureau through Regulation Z (codified at 12 C.F.R. Part 1026).

Tokenization: Tokenization refers to a data security practice in which a sensitive data element is replaced by a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. For instance, a tokenized means of access to bank account data enables read-only access to the information, without the ability to conduct transactions on the underlying account. Tokens typically can be used only for a limited time, so that account holders do not have to change their login passwords to cut off access.

UDAP: Section 5(a) of the Federal Trade Commission Act (codified at 15 U.S.C. Sec. 45[a][1]) conferred on the Federal Trade Commission and prudential regulators authority to prohibit companies in their jurisdiction from engaging in unfair or deceptive acts or practices. Individual states have also adopted statutes similar to federal UDAP requirements.

UDAAP: The Dodd-Frank Act's prohibition on unfair, deceptive or abusive acts or practices confers on the CFPB authority to issue regulations to prevent such practices in connection with consumer financial products and services as defined in the statute and to use supervision and enforcement authority to monitor compliance with these prohibitions. The statutory standards for unfairness and deceptiveness codify prior practice developed pursuant to Section (5)(a) of the Federal Trade Commission Act. See FTC, Policy Statement on Deception; FTC, Policy Statement on Unfairness. The CFPB issued a policy statement in January 2020 indicating that it generally intends to avoid challenging conduct as abusive that relies on all or nearly all of the same facts that the Bureau alleges are unfair or deceptive. CFPB, Statement of Policy Regarding Prohibition on Abusive Acts or Practices. Individual states have also adopted statutes similar to federal UDAAP requirements.

APPENDIX C

Recent Research on Related Topics

C.1 The importance of income shocks, volatility, and financial reserves

Several bodies of recent research emphasize the impact of income shocks, volatility, and financial reserves, both in loan repayment and in determining the long-term financial health and stability for both consumers and small businesses more generally.

Mortgage defaults: Research on mortgage defaults since the financial crisis has highlighted the role of income shocks, reserves, and household liquidity.[1] For example, a 2019 study by JPMorgan Chase Institute found stronger relationships between mortgage default rates and cash reserves than the amounts of equity that borrowers had in their homes, both within the first few years after origination and in the context of loan modifications. Although the mortgage market has tended to emphasize large down payments as a means of reducing default risks, the study suggests that establishing emergency reserve accounts might better protect borrowers and lenders from the risk that borrowers will experience income shocks.[2]

Ability to cover unexpected expenses: The annual Survey of Household Economics and Decisionmaking by the Federal Reserve Board has been asking respondents since 2013 whether they would be able to cover an unexpected $400 expense using cash, savings, or a credit card that would be paid off by the next statement. The percentage of respondents who said they could do so has increased from 50 percent to 61 percent over six years; the majority of the remaining respondents said they would have to borrow or sell something to cover the expense. And even without unexpected costs, 1 in 5 respondents have reported in recent years that they expected not to pay all of their bills in full in the month that the survey was conducted.[3]

Financial diaries: A 2015 joint initiative by NYU Wagner's Financial Access Initiative and the Center for Financial Services Innovation (now Financial Health Network) worked closely with 235 low- to moderate-income households for more than a year to produce both quantitative research and a detailed narrative picture of how participants coped with high levels of income uncertainty. For example, the study found relatively high levels of reliance on loans from friends and family in addition to use of credit from traditional and alternative lenders.[4]

1 Christopher L. Foote et al., Technological Innovation in Mortgage Underwriting and the Growth in Credit, 1985–2015, Federal Reserve Bank of Boston Working Paper 19-11 (2019); Peter Ganong & Pascal Noel, Liquidity vs. Wealth in Household Debt Obligations: Evidence from Housing Policy in the Great Recession, National Bureau of Economic Research Working Paper No. 24964 (August 2018).

2 Diana Farrell et al., Trading Equity for Liquidity: Bank Data on the Relationship Between Liquidity and Mortgage Default, JPMorgan Chase Institute (2019).

3 Board of Governors of the Federal Reserve System, Report on the Economic Well-Being of U.S. Households in 2018 at 21-22 (2019); Board of Governors of the Federal Reserve System, Report on the Economic Well-Being of U.S. Households in 2017 at 21-22 (2018).

4 Jonathan Morduch & Rachel Schneider: The Financial Diaries: How American Families Cope in a World of Uncertainty (2017); Jonathan Morduch et al., An Invisible Finance Sector: How Households Use Financial Tools of Their Own Making, U.S. Financial Diaries (2014).

Increases in income volatility and low savings rates more generally: A range of policy and research organizations and academic researchers have produced studies documenting relatively high levels of income volatility and low levels of emergency savings, despite the nation's general economic recovery and increases in household income since the 2008 financial crisis. Estimates of the number of households that experience substantial income volatility range from one-third to nearly one-half, depending on the source, time period measured (monthly vs. annual), and methodology used.[5]

Small business reserves: Research in small business markets has also provided new insights into the extent to which companies operate with limited cash reserves, such that delays in receiving revenue can create tremendous financial strain absent access to operating capital. Although reserves vary by business type and geography, some research suggests that the median small business holds only enough cash reserves to continue operations for two to four weeks.[6]

C.2 Fintech and marketplace lenders' customer bases

A number of recent studies have looked at the customer bases and business models of fintech and marketplace lenders generally. These sources do not focus specifically on whether the particular firms in question are using cash-flow data, but they are instructive to broader debates about the extent to which these new market entrants are deviating from traditional credit underwriting inputs, finding "invisible prime" customers that are overlooked by traditional lenders, and otherwise reaching underserved populations. The results of the studies are mixed, which may in part be the result of focusing on different lenders and using different methodologies to study particular questions.

Comparisons between fintech loans and credit card debt: Several studies have compared publicly available data about refinancing loans from marketplace lenders such as LendingClub and Prosper, which tend to release more data than other lenders as part of their outreach to investors, with data on credit card loans that is reported publicly to government regulators or available through companies that track mailing offers. The two types of loans are assumed to be generally similar since borrowers are likely to be refinancing credit card debts. These studies generally suggest that the fintech lenders are offering lower prices and are increasing access to credit to borrowers

5 Diana Farrell et al., Weathering Volatility 2.0: A Monthly Stress Test to Guide Savings (2019); Robert Moffitt & Sisi Zhang, The PSID and Income Volatility: Its Record of Seminal Research and Some New Findings, Annals of the American Academy of Political & Social Science (2018); Special Issue: Household Economic Instability and Social Policy, 91 Soc. Service Rev. 371-584 (2017); Association for Public Policy Analysis and Management, Panel: The Role of Income Volatility in Family Economic Security: Evidence and Policy Implications, 39th Annual Fall Research Conference (2017); Pew Charitable Trusts, Issue Brief: How Income Volatility Interacts with American Families' Financial Security (2017); David S. Smith et al., Memo: The Future of Income Volatility Research, Aspen Institute (2017); Diana Farrell & Fiona Greig, Coping with Costs: Big Data on Expense Volatility and Medical Payments, JPMorgan Chase Institute (2017); Signe-Mary McKernan, et al., Thriving Residents, Thriving Cities: Family Financial Security Matters for Cities, Urban Institute (2016); Aspen Institute, Income Volatility: A Primer (2016); Diana Farrell & Fiona Greig, Paychecks, Paydays, and the Online Platform Economy: Big Data on Income Volatility, JPMorgan Chase Institute (2016); Pew Charitable Trusts, The Precarious State of Family Balance Sheets (2015); Pew Charitable Trusts, How Do Families Cope with Financial Shocks? The Role of Emergency Savings in Family Financial Security (2015); Diana Farrell & Fiona Greig, Weathering Volatility: Big Data on the Financial Ups and Downs of U.S. Individuals, JPMorgan Chase Institute (2015); Karen Dynan et al., The Evolution of Household Income Volatility,12 B.E. J. of Economic Analysis & Policy 1935 (2012).

6 Diana Farrell et al., Facing Uncertainty: Small Business Cash Flow Patterns in 25 U.S. Cities, JPMorgan Chase & Co. Institute (2019) (analyzing cash-flow management challenges among samples of small businesses from 2013-2017); Mills, Chapter 3 (discussing substantial impact of federal government program to ensure that invoices were paid in 15 rather than 30 days); Diana Farrell et al., Growth, Vitality, and Cash Flows: High-Frequency Evidence from 1 Million Small Businesses, JPMorgan Chase & Co. Institute 25 n.14, 31, 44 (2018) (reporting a median of 12 cash buffer days based on 2016 data); Diana Farrell & Chris Wheat, Cash Is King: Flows, Balances, and Buffer Days: Evidence from 600,000 Small Businesses, JPMorgan Chase & Co. Institute 14 (2016) (reporting a median of 27 cash buffer days based on data from February to October 2015).

with non-prime scores or residences in areas that are underserved by banks.[7] In 2015, for example, one study found that about 8 percent of the loans that LendingClub designated as A-rated and 28 percent of B-rated loans were to borrowers with FICO scores in the non-prime range. Based on loan performance over two years, the borrowers did not have an increased likelihood of default and their credit did not appear mispriced in terms of risk. Holding FICO scores constant across the broader pool of borrowers, the study concluded that LendingClub borrowers paid less than the pool of credit card borrowers from large banks, but they had a slightly higher delinquency rate.[8]

Loan substitution for borrowers that have "thick" files: Several studies have found evidence that a substantial portion of fintech borrowers have relatively thick credit files and are using the loans to substitute for or augment bank products. One study focused on borrowers from Prosper, finding that they often were able to access more bank credit after obtaining a fintech loan and that the increased access to credit was not associated with higher delinquencies.[9] Another compared loans by six fintech lenders (LendingClub, SoFi, Avant, Loan Depot, Upstart, and CashCall) to all other lenders who report to a particular nationwide consumer reporting agency. The study concluded that many fintech borrowers were using their loans to increase consumption rather than to refinance existing debts, and that they had a higher risk of default after obtaining the loans.[10] Other studies have focused on the substitution effects between bank and fintech loans, concluding that there are some positive impacts on access to credit with regard to small loans and for borrowers that already have relatively strong credit histories, but that fintechs otherwise may largely substitute for bank lenders in other market segments.[11]

Use of fintech in mortgage lending: A few studies have examined the evolution of non-bank platform lenders in the mortgage market. For example, one study found that non-bank lenders' market share grew from roughly 30 percent in 2007 to 50 percent by 2015, with particularly rapid growth among fintech lenders that accounted for about one quarter of non-bank originations by 2015. The fintech firms appeared to be relying less heavily on traditional variables such as FICO scores and loan-to-value ratios compared to other lenders, were likely to serve more creditworthy borrowers than other non-banks, and were heavily concentrated in the refinancing market.[12] A second study focused on racial disparities in mortgage lending, finding that the same group of fintech lenders tended to have smaller gaps in pricing between LatinX and African-American borrowers and whites and no gaps in loan approvals as compared to lenders as a whole. More generally across the market, the study found a substantial decline in unexplained pricing differentials between

7 Julapa Jagtiani & Catharine Lemieux, The Roles of Alternative Data and Machine Learning In Fintech Lending: Evidence from the LendingClub Consumer Platform, Federal Reserve Bank of Philadelphia Working Paper 18-15 at 3-6, 12-13 (updated January 2019); Julapa Jagtiani & Catharine Lemieux, Do Fintech Lenders Penetrate Areas That Are Underserved by Traditional Banks?, 100 J. of Econ. & Business 43-54 (2018); Robert M. Adams, Do Marketplace Lending Platforms Offer Lower Rates to Consumers? FEDS Notes (Oct. 22, 2018). For studies considering loan performance from an investor perspective, see Roman Kraussl et al., The Performance of Marketplace Lenders: Evidence from Lending Club Payment Data (November 2019).

8 Jagtiani & Lemieux, The Roles of Alternative Data and Machine Learning.

9 Tetyana Balyuk, Financial Innovation and Borrowers: Evidence from Peer-to-Peer Lending (May 6, 2019).

10 Marco DiMaggio & Vincent W. Yao, FinTech Borrowers: Lax-Screening or Cream-Skimming? 13, 16 (February 2019). The study concluded that the fintech firms were not really increasing access to credit to underserved populations, but that conclusion may have been affected by the decision to exclude borrowers with less than 440 credit scores or no scores and trade lines with less than a $500 credit limit. The average borrower studied had 20 financial accounts on their credit report.

11 Huan Tang, Peer-to-Peer Lenders Versus Banks: Substitutes or Complements?, 32 Rev. of Fin. Studies 1900 (2019); Brian Wolfe & Woongsun Yoo, Crowding Out Banks: Credit Substitution by Peer-to-Peer Lending (Sept. 17, 2018).

12 Greg Buchak et al., Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks, NBER Working Paper 23288 (revised September 2018).

demographic groups as online competition and reliance on automated underwriting increased from 2008 to 2015.[13]

Borrower demographics: Although fintech and marketplace lenders are often described as focusing on underserved populations, studies of the sector as a whole suggest a more complicated picture. For example, one study by Experian of unsecured personal lending found that fintech lenders tend to draw a larger portion of their customer base from younger borrowers and near prime populations than traditional lenders. However, average credit scores and the average number of open trade lines were slightly higher for fintech lenders across different age buckets as compared to traditional sources. As a group, a smaller portion of fintechs' customer base was made up of sub-prime and deep sub-prime borrowers than traditional sources, though the study noted that some individual companies have focused specifically on borrowers with weaker credit.[14]

13 Robert Bartlett et al., Consumer-Lending Discrimination in the Fintech Era, National Bureau of Economic Research Working Paper No. 25943 (updated November 2019). Specifically, the authors estimated pricing differentials of about 7.9 basis points for purchase mortgages and 3.6 basis points for refinance mortgages overall, compared to 5.3 and 2.0 basis points for platform lenders. The smaller group of lenders also did not have disparities in rejection rates once underwriting criteria were controlled for, while there were disparities of 9.6 percentage points for purchase loans and 7.3 percentage points for refinance loans across lenders as a whole. The study excluded loans that may have been originated to satisfy bank obligations under the Community Reinvestment Act.

14 Experian Fintech vs. Traditional FIs at 5-8; *see also* Latham; Nasiripour.

APPENDIX D

Data Sharing Principles and Frameworks

In addition to the Consumer Financial Protection Bureau's Data Sharing Principles, several other organizations and jurisdictions have released lists of principles or frameworks for data rights and protections in response to the era of increasing data generation and sharing. Some of these are focused specifically on financial services, while others are more generalized. This appendix provides a brief overview of the CFPB principles as well as various other mostly non-governmental sources, including the Center for Financial Services Innovation (2016 & 2017), World Economic Forum (2018), California Consumer Protection Act (2018), American Law Institute (ALI), American Bankers Association (ABA), Financial Data Exchange (FDX), the Consultative Group to Assist the Poor (CGAP), and Consumer Reports and other organizations (CR et al.). As discussed in Box 5.2.2.1.1, the European Union, United Kingdom, Canada, Mexico, Australia, New Zealand, Singapore, Hong Kong, Japan, and India are also in the process of considering and adopting new data regimes.

CONCEPT	SOURCE	DETAILS
CONSUMER'S ACCESS TO DATA HELD BY FIRMS	CFPB	» Consumers are able to obtain data from providers of financial products and services upon request in a timely manner and readily usable format. Data may include any transaction, series of transactions, or other aspects of consumer usage; terms of the account; realized costs and benefits (e.g., fees, interest paid, interest earned, rewards).
	CFSI	» Consumers have the ability to view financial information that is timely, consistent, and complete.
	WEF	» Companies should, where appropriate, allow customers to access and download data about them in machine-readable format or through standardized APIs. Consumers should be able to view or know the data that are collected about them, how they are used, and whether they are shared with a third party.
	CCPA	» Consumers have a right to access the specific data collected about them.
	ALI	» If a data controller or any data processor acting on its behalf stores personal data about a data subject, the data subject is entitled to obtain access to the personal data.
	ABA	» Customers should have the ability to access their financial account data in a way that is safe and secure.
	FDX	» Financial data belongs to the account owner. They should have quick and convenient access.
	CGAP	» Consumers ought to have the right to access their personal data in an easy-to-read format.
	CR ET AL.	» Users can obtain all public-facing and private user information the company hold about them.

CONCEPT	SOURCE	DETAILS
CONSUMER'S ABILITY TO DIRECT DATA SHARING WITH OTHER FIRMS	CFPB	» Consumers are generally able to authorize trusted third parties to obtain data from account providers to use on their behalf, for their benefit, and in a safe manner. Third parties only access the data necessary to provide the products or services selected by the consumer. Data is provided upon request in a timely manner and readily usable format.
	CFSI	» Consumers have the ability to view their financial information with the trusted and secure third-party application of their choice. Data are timely, consistent, and complete, but sharing does not lead to the transfer and storage of excess information.
	WEF	» Companies should, where appropriate, allow customers to transfer and/or permit third parties to manage data about them by allowing downloads of data in machine-readable format or through standardized APIs.
	CCPA	» Where firms respond to requests for data access electronically, they must generally provide the data in a readily usable format that allows transmission to others without hindrance.
	ALI	» Upon the request of the data subject and when appropriate, reasonable, and practical or when required by applicable law, the data controller shall provide a copy of the personal data in a usable format.
	ABA	» Banks support our customer's ability to use third parties to access their financial account data in a way that is safe and secure.
	FDX	» Consumers should be able to easily permission their data according to their needs. Hand-offs between parties and systems should be convenient, smooth, secure, and efficient.
	CGAP	» Consumers ought to have a right to port their data to other firms, not only for switching services but to leverage the value of their data for other services.
	CR ET AL.	» The company complies only with legal and ethical third-party requests for user information.

CONCEPT	SOURCE	DETAILS
DEGREE OF CUSTOMER CONTROL OVER DATA USE AND SHARING	CFPB	» Financial account agreements do not seek to deter consumers from accessing or granting access. Consumers are not coerced into granting third-party access to data. Revocation procedures can be readily understood and exercised by consumers and are implemented in a timely and efficient manner by providers, including deletion of personally identifiable information at the discretion of the consumer. Third parties obtain authorization to initiate payments separately from authorization to access data.
	CFSI	» Consumers provide explicit consent for third parties to access and use their data. Consumers can easily view, modify, and revoke consent for data sharing. Consent is considered to be revoked if a consumer leaves an application dormant for a reasonable length of time.
	WEF	» Customers should be able to request that data about them no longer be used by an organization (e.g., right to revoke access and be forgotten). Companies may not need to seek consent when using the data for legitimate interests (e.g., those required by law).
	CCPA	» Consumers have a right to opt out of certain data "sales" of personal information to third parties at any time. Parents must opt in for sales of data involving consumers under age 16 under certain circumstances. Firms cannot discriminate against consumers who exercise their rights under the law. Consumers have a general right to demand deletion.
	ALI	» An individual shall be given understandable and easy-to-use mechanisms to permit exercise of a meaningful choice in relation to personal-data activities regarding his or her personal data. Personal data shall not be used for unrelated secondary activities without notice and consent. Consumers must generally have a right to withdraw consent.
	ABA	» When consumers share their financial data they should have control over what information is shared and how it is used. This includes the ability to modify access and revoke access when a service is no longer used. Services that go beyond financial account aggregation, such as money movement, should be subject to separate agreements and require separate informed consent.
	FDX	» Consumers should have the ability to determine which financial data parties will have access to their data and be able to easily permission their data according to their needs. Consumers should have the ability through easy, intuitive interfaces to effortlessly grant, modify, and revoke access to their financial data.
	CGAP	» Consumers should have the right to reconsider prior authorizations of data access and to opt out of new types of processing and use. Consumers should have a right to erase their data.
	CR ET AL.	» Users can control the collection of their information and can delete their information. Privacy controls exist and are effective. Users have a clear explanation of how users can control whether their information is used for targeted advertising and can control how their information is used to target advertising.

CONCEPT	SOURCE	DETAILS
DISCLOSURES AND MECHANICS OF INFORMED CONSENT	CFPB	» Consumers are not required to share account credentials with third parties to provide data access. Terms of access, storage, use, and disposal are fully and effectively disclosed and understood by the consumer, including access frequency, scope, and retention period. Consumers have ready access to information detailing the identity and security of authorized third parties that are accessing or using their data throughout the period in which the firms are accessing, using, or storing data. This includes information on the scope of data accessed, the nature of use, and frequency of access.
	CFSI	» Third-party application providers seek consumer permission for the specific data access necessary to enable application functionality at the time of enrollment. The ability to clearly review and revoke access is available at any time through the third-party application.
	WEF	» Companies need to provide clear and accessible information about how customer data will be used. Customers should be able to view or know the data that are collected about them, how they are used, and whether they are shared with a third party.
	CCPA	» Requires various types of disclosures regarding data and privacy practices. Specifies requirements for verified consumer requests for data access and other follow up.
	ALI	» Specifies requirements for general and heightened notices about data activities. Form of consent must be reasonable under the circumstances, and must be clear and affirmative for situations in which heightened notice is required.
	ABA	» Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data a technology company are accessing, how long the company is holding this data, and how it is using the data. Intuitive control would allow consumers to see easily who is authorized to receive their data.
	FDX	» When permissioning a new service, consumers should be fully informed regarding what their data is used for, how long the service can access that data, who it is used by, and under which terms the service is provided. Interfaces should be easy and intuitive for granting, modifying, and revoking access.
	CGAP	
	CR ET AL.	» Users are provided a disclosure of what user information is shared, the types of third parties with which user information is shared, and whether user information could be shared with government or legal authorities. Third party domains contacted by the product are named in the privacy policy. The company provides clear notification when it changes its privacy policy and/or terms of service.

CONCEPT	SOURCE	DETAILS
MINIMIZATION OR OTHER RESTRICTIONS ON USE AND SHARING APART FROM CUSTOMER CONTROL	CFPB	» Authorized third parties only access the data necessary to provide products or services selected by the consumer and only maintain data for as long as necessary. Authorized terms of access, storage, use, and disposal are not overly broad and are consistent with the consumer's reasonable expectations in light of the products or services selected by the consumer.
	CFSI	» Only the minimum amount of data required for application functionality are collected, and the data are stored only for the minimum amount of time needed.
	WEF	» Companies may not need to seek consent when using the data for legitimate interests (e.g., those required by law). Where reasonable, a maximum time period that data can be retained by companies should exist, as well as limits on certain sensitive data types or uses. Companies should be able to create individual customer-level profiles that allow them to provide differentiated customer service, but should be able to comprehensively test, validate, and explain their use of data analytics and models to customers.
	CCPA	» Some restrictions on providing consumer information to service providers.
	ALI	» A data controller shall retain personal data only as consistent with the scope of the notice, the purposes for which it is provided, and purposes that are consistent with the principles. A data controller or processor that stores personal data may only make onward transfers for personal-data activities for which the subject has received notice. Personal data shall not be used in data activities unrelated to those stated in the notice to individuals without the consent of the individuals. When it is reasonably foreseeable that personal data will be used in the future, the transparency statement and individual notice to data subjects shall be updated to state this fact.
	ABA	» Consumers should expect that data-sharing is limited to the data that are needed to provide the service they have authorized and only maintain these data as long as necessary.
	FDX	» Consumers should provide informed consent (with the ability to revoke that consent) for any and all access granted to Financial Data Parties. These parties will then only have access for the purposes for which the consent was provided. Only data that is required to provide such services should be shared with the organization providing the service.
	CGAP	» Consumers should have a right to receive an explanation of processing based on AI or machine learning and the right not to be subject to a decision based solely on automated processing.
	CR ET AL.	» The user information collected is only that which is directly relevant and necessary for the service. Users have a clear understanding of what user information the company is collecting. The product still works when all permissions not relevant to product's functionality are declined.

CONCEPT	SOURCE	DETAILS
SECURITY	CFPB	» All parties that access, store, transmit, or dispose of consumer data and access credentials use strong protections and effective processes to mitigate the risks of, detect, promptly respond to, and resolve and remedy data breaches, transmission errors, unauthorized access, and fraud, and transmit data only to third parties that also have such protections and processes.
	CFSI	» All entities follow applicable laws and industry best practices with regard to data privacy and security. Best practices contain tiers of rigor commensurate with the type and amount of data sharing engage in, so as not to unduly limit innovation or competition.
	WEF	» Companies should be held responsible and accountable for data security.
	CCPA	» Imposes a duty to implement and maintain reasonable security procedures and practices but does not define standards. Gives consumers a right to sue firms where nonencrypted or nonredacted personal information is subject to unauthorized access, theft, disclosure, etc. as a result of a business's violation of its duties.
	ALI	» A data controller shall protect personal data with reasonable security safeguards against foreseeable risks. Reasonable security safeguards shall be proportionate to the risk of harm in the event that the personal data is compromised.
	ABA	» Consumers deserve bank-level security and protection regardless of where they choose to share their data. This means that consumer data are treated the same – and subject to GLBA protections – whether at a bank or a third party.
	FDX	» Consumers must know where their data is going. Data must be protected across all points of access, transport, and at rest. All parties involved in the data-sharing ecosystem must have appropriate security policies and practices in place. These practices should reflect best-in class standards and be improved upon continuously.
	CGAP	
	CR ET AL.	» The company is willing and able to address reports of vulnerabilities. The company has systems in place to limit and monitor employee access to user information, an internal security team that conducts security audits on the company's products and services, and commissions third-party security audits on its products and services.

CONCEPT	SOURCE	DETAILS
ACCURACY OF DATA, DECISIONMAKING, AND RELATED CONSUMER RIGHTS	CFPB	» Consumers can expect the data they access or authorize others to access or use to be accurate and current. They have reasonable means to dispute and resolve data inaccuracies regardless of how or where inaccuracies arise.
	CFSI	» Consumer financial data are timely, consistent, accurate and complete.
	WEF	» Companies should be able to comprehensively test, validate, and explain their use of data analytics and models to customers. Customers should have the right to request why a decision was made and the right to correct incorrect or incomplete data.
	CCPA	
	ALI	» Data controllers shall provide data subjects with a reasonable process by which they can challenge the accuracy of their data. In the event that data subject provides a reasonable basis in proof to demonstrate errors, the data controller shall correct the record.
	ABA	
	FDX	
	CGAP	» Consumers should have a right to update and correct their data. Consumers should have a right to receive an explanation of processing based on AI or machine learning and the right not to be subject to a decision based solely on automated processing.
	CR ET AL.	
CONSUMER DISPUTE RESOLUTION AND REMEDIES	CFPB	» Consumers have reasonable and practical means to dispute and resolve instances of unauthorized access and data sharing, unauthorized payments conducted in connection with or as a result of either authorized or unauthorized data sharing access, and failures to comply with the terms of customer authorizations or other obligations. Consumers are not required to identify the responsible parties to receive appropriate remediation. Parties responsible for unauthorized access are held accountable for the consequences of such access.
	CFSI	
	WEF	
	CCPA	» See above regarding violations of the duty to maintain reasonable security procedures and practices.
	ALI	» See above regarding data correction.
	ABA	
	FDX	
	CGAP	
	CR ET AL.	

CONCEPT	SOURCE	DETAILS
BROADER SYSTEM WIDE ACCOUNTABILITY MECHANISMS, REMEDIES	CFPB	» The goals and incentives of parties that grant access to, access, use, store, redistribute, and dispose of consumer data align to enable safe access and deter misuse. Commercial participants are accountable for the risks, harms, and costs they introduce to consumers, and are incentivized and empowered to prevent, detect, and resolve insecurity of data, data inaccuracies, unauthorized activities, and failures to comply with customer authorizations and other obligations.
	CFSI	» Providers of financial services should develop an agreed-upon framework for apportioning liability related to data sharing among financial institutions, data aggregators, and financial technology companies that can be shared and replicated in contracts between the different parties. The framework should limit consumer risk exposure to the greatest extent possible and determine minimum security standards.
	WEF	» A clear liability framework should be in place that ensures the responsible party is held accountable for data security and for harms caused by breaches of its respective data security duties of care. Companies need to be able to identify where data were improperly used or accessed in the event of a security breach.
	CCPA	» Subject to enforcement by the California Attorney General. Consumers have a limited private right of action in the event of data breaches involving non-encrypted or nonredacted personal information.
	ALI	» Data controllers and data processors shall be accountable for complying with the principles. Accountability requires that data controllers and processors regularly assess privacy and security risks associated with their data activities and maintain comprehensive oversight and governance mechanisms. Enforcement proceedings can include actions by government agencies as well as civil proceedings.
	ABA	
	FDX	
	CGAP	
	CR ET AL.	

Funding and engagement from:

Flourish is an evergreen, early-stage venture fund investing globally in entrepreneurs whose innovations help people achieve financial health and prosperity. Spun out of Omidyar Network in 2019 with an existing portfolio of $200 million, Flourish received a new commitment of $300 million from Pam and Pierre Omidyar, the founder of eBay. Flourish invests in a number of themes in fintech, insurtech, regtech and other technologies, as well as supports nonprofit organizations, that empower people and help foster a fair, more inclusive economy. Flourish is managed by a global team with offices in Silicon Valley, Washington DC, London, and India.

The **Milken Institute** is a nonprofit, nonpartisan think tank that helps people build meaningful lives, in which they can experience health and well-being, pursue effective education and gainful employment, and access the resources required to create ever-expanding opportunities for themselves and their broader communities.

Digital version available at finreglab.org

Published by FinRegLab, Inc.

900 19th Street NW, Suite 600
Washington, DC 20005
United States