Consumer Financial Data:

Legal and Regulatory Landscape

FINANCIAL HEALTH NETWORK

flourish
A Venture of The Omidyar Group

FinRegLab

MITCHELL SANDLER

Acknowledgments

“Consumer Financial Data: Legal and Regulatory Landscape” was prepared by the law firm of Mitchell Sandler LLC for the Financial Health Network. Alex Acree, Partner at Mitchell Sandler LLC, led the preparation of this paper, and was joined by Pierce Babirak, Julia Baker, Chris Napier, and Shelby Schwartz.

“Consumer Financial Data: Legal and Regulatory Landscape” is a collaboration between the Financial Health Network, FinRegLab, Flourish, and Mitchell Sandler. Dan Murphy of the Financial Health Network led this collaboration, and was joined by Kelly Thompson Cochran of FinRegLab, Chuck Muckenfuss of Flourish, and David Silberman of the Financial Health Network, all of whom provided expert guidance and assisted in the drafting of this paper.

Special thanks to Chuck Muckenfuss of Flourish for his vision and his encouragement in making this collaboration a reality.

Contributors

- **Mitchell Sandler:** Alex Acree, Pierce Babirak, Shelby Schwartz, Julia Baker, and Chris Napier
- **Financial Health Network:** Dan Murphy and David Silberman
- **FinRegLab:** Kelly Thompson Cochran
- **Flourish:** Chuck Muckenfuss

Mitchell Sandler LLC is a majority women-owned boutique law firm headquartered in Washington, D.C., specializing in the representation of banks, financial services providers, and financial technology companies. Find out more at **mitchellsandler.com.**

Flourish backs entrepreneurs whose innovations advance financial health and prosperity for individuals and small businesses. Founded in 2019, Flourish is an early-stage, evergreen global venture fund that deploys patient capital with a long-term perspective. With a deep understanding of industry dynamics, Flourish works with startups offering a range of financial services, including fintech infrastructure, consumer and small business lending, insurtech, and digitizing money, among others. Flourish partners with industry thought leaders in research, policy, and regulation to better understand the underserved and help foster a fair, more inclusive economy. Find out more at **flourishventures.com**.

FinRegLab

FinRegLab is a nonprofit innovation center that tests new technologies and data to inform public policy and drive the financial sector toward a responsible and inclusive financial marketplace. With our research insights, we facilitate discourse across the financial ecosystem to inform public policy and market practices.

FINANCIAL HEALTH NETWORK

The Financial Health Network is the leading authority on financial health. We are a trusted resource for business leaders, policymakers, and innovators united in a mission to improve the financial health of their customers, employees, and communities. Through research, advisory services, measurement tools, and opportunities for cross-sector collaboration, we advance awareness, understanding, and proven best practices in support of improved financial health for all.

For more on the Financial Health Network, go to **finhealthnetwork.org** and join the conversation online:

- @FinHealthNet
- FinancialHealthNetwork
- Financial Health Network
- Financial Health Network
- FinHealthNet

Financial Health Network *135 S. LaSalle, Suite 2125, Chicago, IL 60603 | 312.881.5856*

FINANCIAL HEALTH NETWORK flourish A Venture of The Omidyar Group FinRegLab MITCHELL SANDLER

Executive Summary

Over the last two decades, technology has fundamentally reshaped the way consumers and small businesses interact with providers of financial services. Traditionally conducted in person with brick-and-mortar financial institutions, financial services are now increasingly managed through automated processes and delivered through digital channels. These fundamental changes have been enabled by, and in turn have contributed to, an explosion in the availability, uses, and value of data in financial services. This includes not only financial information—such as transaction history, credit performance, and other observations about financial behavior—but also nonfinancial data, such as social media and mobile device information, that may be useful for purposes such as marketing and identity verification.

The increasingly sophisticated use of data and technology could produce significant benefits for consumers and small businesses; for instance, by increasing the speed and convenience of financial services delivery, expanding access for historically underserved populations, supporting more individually tailored financial products and services, and giving customers more control over their financial lives. However, changes in data and technology also require careful evaluation and management of risks, such as protections against data breaches and unauthorized transactions, the risk of replicating or re-enforcing historical discrimination, and potential losses of personal privacy and control.

The adoption of new data and technology has also changed the landscape of the financial services industry. Driven by the advent of the Internet, widespread adoption of smart phones, and other changes, a new generation of providers—often referred to as “financial technology” or “fintech” companies—has emerged. The increasing demand for data from both newcomers and incumbents alike has in turn created opportunities for new types of data intermediaries, including “data aggregators” that access and transfer information housed in consumers’ various financial accounts. These entities have become increasingly critical linkages in the expanding financial data ecosystem, joining well-established intermediaries such as credit bureaus and payment networks. At the same time, large technology companies have also arrived at the doorstep of financial services, both competing and partnering with various financial services providers.

Yet despite the significant technology, customer experience, and business model changes permeating the financial services industry, the laws and regulations governing financial data in the United States have not evolved in parallel. The purpose of *Consumer Financial Data: Legal and Regulatory Landscape* is to describe the current U.S. federal legal framework governing consumer financial data in substantial detail with the goal of laying a foundation for future discussions and analyses. As stakeholders debate whether to update the framework governing consumer financial data specifically or to adopt broader general data governance regimes, a detailed understanding of the current financial data framework is essential. This paper—which is being released as a working paper—is intended to serve as a building block and to foster informed debates about potential gaps, changes in approach, and areas in which technology and business model changes have outstripped the existing framework.

As a navigation tool to readers, this executive summary briefly lists the legal regimes that are detailed in the full paper, along with a sampling of the kinds of interpretive questions and policy issues that are being raised by the evolution of the financial data ecosystem. Neither the recitation of issues here nor in the full paper is exhaustive. Rather, the issues listed are intended to convey a sense of the importance and breadth of questions that are being raised and issues that are being debated by stakeholders. Some cross-cutting questions, such as the efficacy of consumer protections and rights that change as financial data passes downstream to different types of companies, may need to be addressed across multiple bodies of law.

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act

The Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) was adopted after the 2008 financial crisis to modernize various aspects of financial regulation. Section 1033 provides that, subject to rules prescribed by the Consumer Financial Protection Bureau (CFPB), companies that offer or provide consumer financial products or services must make available to consumers in electronic form upon request certain consumer financial information in their control or possession. Although the CFPB outlined a set of principles for data sharing in 2017, it has not yet issued implementing rules for Section 1033. Absent formal guidance, the precise scope and current effect of Section 1033 remain uncertain, and stakeholders are debating related policy issues such as whether and, if so, how the CFPB should set standards for consumer authorization processes and for allocating liability among different types of financial

services providers in the event that data sharing results in legal injury. Open interpretive and policy issues include:

- Whether and under what conditions covered persons should be permitted to restrict data access beyond categories that are specifically excluded by statute or rule, and the scope of those statutory exceptions. **[Commentary Box 1, Commentary Box 2]**

- Whether Section 1033 has already taken effect or does not apply until the CFPB issues implementing regulations. **[Commentary Box 3]**

- Whether and under what conditions financial institutions must permit data access to agents and representatives acting on a consumer's behalf. **[Commentary Box 4, Commentary Box 5]**

- What processes and protections should be required regarding consumer consent, particularly in situations involving agents and representatives accessing data on a consumer's behalf. **[Commentary Box 6]**

- The intersection between Section 1033 and other existing statutes and regulations, particularly as to how liability and responsibilities for data accuracy, data security, and account security should be allocated among the various stakeholders in the market. **[Commentary Box 7]**

Gramm-Leach-Bliley Act

The 1999 Gramm-Leach-Bliley Act (GLBA) relaxed rules governing affiliations between banks, securities firms, insurance companies, and other financial services providers, and also adopted baseline requirements for "financial institutions" with respect to protecting the privacy and security of consumer financial information. Yet responsibility for implementing the privacy and security provisions was divided among multiple federal agencies that do not all have consistent monitoring authorities or resources. In some cases, federal agencies have adopted differing standards. Moreover, there has been substantial evolution in data, technology, business practices, and business models in the two decades since the initial rules and standards were adopted.

The Privacy Rule, composed of the applicable portions of GLBA along with the implementing regulations, generally prohibits financial institutions from sharing consumers' nonpublic personal information with nonaffiliated companies unless consumers have received notice and an opportunity to opt out. However, it contains a number of exceptions that permit data sharing without regard to whether a consumer has opted out, as well as complex provisions about the extent to which companies that receive information from a financial institution can use such data or disclose it to downstream parties. The Privacy Rule also specifies the components of required privacy policies and notices for consumers and customers of financial institutions. Open interpretive and policy questions include:

- Which requirements apply to various types of companies, particularly data intermediaries that perform various types of financial activities on behalf of another firm and do not have a direct relationship with a consumer. **[Commentary Box 8, Commentary Box 9]**

- Whether exceptions for anonymized data should be adjusted in light of advances in re-identification techniques. **[Commentary Box 10]**

- Whether consumers should have to rely on notice and opt out to manage their privacy interests. **[Commentary Box 11]**

- Similar to questions raised under Section 1033, whether processes and protections are warranted under an exception to GLBA's general notice and opt-out regime that allows information sharing with the affirmative consent or at the direction of a consumer. **[Commentary Box 11]**

- Whether regulation of information sharing between financial institutions and their affiliates is also warranted. **[Commentary Box 12]**

- What limitations should apply to companies that receive consumer information from a financial institution pursuant to GLBA with respect to their use or disclosure of the data to other downstream parties. **[Commentary Box 13]**

GLBA's Safeguards Rule establishes standards and requirements for the storage, security, and protection of financial data by financial institutions. It is administered by a number of different agencies with different authorities and resources available to them, especially with respect to entities not subject to prudential supervision by the banking authorities. Open issues include:

- Whether the regulatory mechanisms are adequate to monitor nonbank financial institutions' compliance with safeguard requirements, including data intermediaries and other key actors in the broader data ecosystem. **[Commentary Box 14]**

- Whether to align substantive differences between the standards for banks and nonbank financial services providers, including a recent proposal by the Federal Trade Commission to revise its rules. **[Commentary Box 15]**

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) focuses primarily on information that is compiled by "consumer reporting agencies" from various sources for use by other companies in credit and insurance underwriting, hiring, and other activities. It imposes various accuracy, privacy, fairness, and information security requirements, as well as providing consumers with the right to access their credit files in certain circumstances and to dispute inaccuracies. Although the law has been amended multiple times since its 1970 adoption, a number of open interpretive and policy questions remain unresolved, such as:

- Whether and under what conditions data aggregators and other new intermediaries qualify as consumer reporting agencies, and whether and under what conditions their data sources are "furnishers" under FCRA requirements. **[Commentary Box 16]**

- The tradeoffs between limiting use of consumer data to certain "permissible purposes" versus relying on notice and consent by the consumer to manage privacy and other policy concerns. **[Commentary Box 17]**

- Whether the FCRA accuracy and dispute resolution requirements should be adjusted for data aggregators and their data sources given differences in their operations from traditional consumer reporting agencies and furnishers. **[Commentary Box 18, Commentary Box 19]**

Other Federal Laws that Implicate Consumer Financial Data Issues

As detailed in the paper, various other federal laws implicate consumer financial data and raise open interpretive and policy questions in the context of the rapidly evolving landscape. These include:

- **Third-Party Risk Management Guidance:** Several laws give federal financial regulators authority to extend their regulatory and examination authorities over companies that act as third-party service providers to financial institutions that are subject to the agencies' ongoing supervision. The agencies have used these authorities to issue substantial guidance articulating expectations for supervised entities to engage in due diligence when selecting, working with, and monitoring vendors and other third parties. The guidance and examinations have become an important mechanism through which regulators can monitor and promote information security, data privacy, and overall legal and regulatory compliance by service providers that may not otherwise be subject to financial data restrictions. There are open questions, however, about whether and how such authorities apply to new types of data intermediaries and business arrangements. **[Commentary Box 20, Commentary Box 21]**

- **Equal Credit Opportunity Act (ECOA):** This law prohibits discrimination on the basis of race, ethnicity, gender, and various other prohibited basis in any aspect of a credit transaction. Violations of the statute are sometimes pursued under "disparate impact" theories to challenge the application of a facially neutral policy or practice that disproportionately harms protected classes, unless it effectuates a legitimate business justification that cannot be reasonably achieved through less impactful means. As new sources of financial and nonfinancial data are considered for use in credit scoring and underwriting, questions are being raised about whether particular sources will reduce or exacerbate disparities along protected-class lines and, where disparities exist, whether the use of these new data sources is consistent with ECOA. **[Commentary Box 22]**

- **Prohibitions on Unfair, Deceptive, and/or Abusive Acts and Practices:** The FTC Act's prohibition on "unfair" acts and practices applies broadly to commercial entities and DFA's prohibition on "unfair and abusive" acts and practices applies to entities that are "covered persons" under DFA. Although federal financial regulators have sometimes

- relied on these authorities as a supplement to GLBA and FCRA in addressing breakdowns in information security and notice and consent procedures, questions exist as to the extent to which these authorities can be used to address other issues or potential gaps in data regulation. **[Commentary Box 23, Commentary Box 24]**

- **Electronic Fund Transfer Act (EFTA):** This law was adopted in 1978 to govern various types of electronic fund transfers from consumer accounts. Open questions under the law are multiplying as electronic payment services diversify and account data is shared to facilitate the provision of other financial services, such as credit underwriting and financial advice. **[Commentary Box 25]** For example, the law generally limits consumers' liability for unauthorized transactions on their accounts, but contains an exception where consumers share an "access device" with a third party. This raises a number of questions about potential liability where consumers share their bank account login credentials with payment services companies and/or data aggregators that collect information on behalf of other financial services providers. **[Commentary Box 28]** Questions about application of EFTA's error correction requirements are also taking on new significance as account data is used for an increasing range of purposes and parties outside of the initial relationship between the consumer and the account provider. **[Commentary Box 26, Commentary Box 27]**

When industries undergo transformation at the speed and depth that financial services markets have over the last two decades, it is prudent to consider whether the current legal regime is well-tailored to the needs of stakeholders and whether it advances important public policy objectives. In this case, it may be worthwhile to evaluate whether the policy objectives underlying current law with respect to financial data are valid and comprehensive; whether current law and regulation are still adequate to promote those policy goals; and where the current regime is showing strain or giving rise to uncertainty.

While the interpretive and policy issues highlighted above and in the full paper are not exhaustive, we hope that they will stimulate discussion and debate concerning areas where policymakers, market participants, consumer advocates, academics, and others should be attentive to how new data, new technologies, and new financial services providers are reshaping the financial data ecosystem. Many of the topics, such as consent, accuracy, and information security, are touched on by multiple existing laws, and may benefit from a more unified approach across different financial services markets and regulatory schemes.

As stakeholders consider the future of the financial data ecosystem, our hope is that this working paper can contribute to a foundational understanding of the current framework of financial data regulation to inform future policy analyses and dialogues. We also hope that it can serve as a useful point of comparison and even inspiration for parallel efforts in other regulated industries, as the emergence of new data and technologies, new intermediaries and service providers, and new legal and regulatory questions occurs beyond the financial data ecosystem.

We welcome input on both the descriptions of current law and the commentary surrounding interpretive and policy questions. Please forward such information to ***DataLandscape@finreglab.org****.*

Table of Contents

Commentary Boxes

Introduction

A. Background and Purpose

Over the last two decades, technology has fundamentally reshaped the way consumers and small businesses interact with providers of financial services. Traditionally conducted in person with brick-and-mortar financial institutions, financial services are now increasingly managed through automated processes and delivered through digital channels.

These fundamental changes have been enabled by, and in turn have contributed to, an explosion in the availability, uses, and value of data in financial services.[1] The increasingly sophisticated use of data and technology could produce significant benefits for consumers and small businesses, for instance by increasing the speed and convenience of financial services delivery, expanding access for historically underserved populations, supporting more personally tailored financial products and services, and giving consumers and small businesses more control over their financial lives. However, changes in data and technology also require careful evaluation and management of risks, such as protections against data breaches and unauthorized transactions, the risk of replicating or reenforcing historical discrimination, and potential losses of personal privacy and control.

Yet despite the significant technology, customer experience, and business model changes permeating the financial services industry, the laws and regulations governing financial data in the United States have not evolved in parallel.[2] The purpose of this paper is to describe the current U.S. federal legal framework governing consumer financial data in substantial detail with the goal of laying a foundation for future discussions and analyses.[3] As stakeholders debate whether to update the requirements governing consumer financial data specifically or to adopt broader general data governance regimes, a detailed understanding of the current financial data framework is essential. This report—which is being released as a working paper—is intended to provide that understanding as a building block for identifying open questions and fostering informed debates about potential gaps, changes in approach, and areas in which technology and business model changes have outstripped the existing framework.

---

1 *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 17 (2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

2 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-254, FINANCIAL TECHNOLOGY: ADDITIONAL STEPS BY REGULATORS COULD BETTER PROTECT CONSUMERS AND AID REGULATORY OVERSIGHT 40-58 (2018), https://www.gao.gov/assets/700/690803.pdf.

3 The federal legal and regulatory framework for protecting consumer data is substantially more detailed than safeguards for small businesses, but this paper will note where protections apply to small business owners as well. In particular, see Section IV.C., Section VI.C., and Section VII.C.

Seeds of a Fintech Revolution

The recent financial services transformation began with the advent of the Internet but accelerated in the aftermath of the financial crisis in the late 2000s due to a confluence of factors. Rapidly increasing smartphone penetration coincided with the growth of new customer acquisition channels and a steep decline in the costs of computing power and data analytics.[4] At the same time, incumbent financial institutions had to navigate the business impacts of the Great Recession and contend with the most significant change to U.S. financial regulation in a generation.[5] Together with benign credit markets, low yields, and plentiful venture capital, the result was fertile soil for technological innovation and competition from newcomers.

Driven by these strong tailwinds, a new generation of financial services providers—often referred to as "financial technology" or "fintech" companies—has emerged. At first, many feared these upstart fintech companies would displace traditional financial institutions.[6] The consequences, however, have been much more nuanced. Although many do compete with incumbents, most fintech companies find that they must partner with traditional financial institutions to launch their products and serve their customers.[7] Another significant segment of fintech companies provides technology products to traditional financial institutions to increase efficiency and lower costs of legacy technology and operating processes.[8] More recently, large technology companies' horizontal expansion across industries has finally arrived at the doorstep of financial services, both competing and partnering with various types of financial services providers.[9]

---

4 *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 17 (2018).

5 Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*); *see also* DAVIS POLK & WARDWELL LLP, Dodd-Frank Progress Report, https://www.davispolk.com/Dodd-Frank-Rulemaking-Progress-Report/.

6 *See* DELOITTE CENTER FOR FINANCIAL SERVICES, FINTECH BY THE NUMBERS 1 (2017), https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/fintech-by-the-numbers.pdf.

7 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-111, FINANCIAL TECHNOLOGY: AGENCIES SHOULD PROVIDE CLARIFICATION ON LENDERS' USE OF ALTERNATIVE DATA 16 (2018), https://www.gao.gov/assets/700/696149.pdf.

8 *See* MCKINSEY & CO., FINTECHNICOLOR: THE NEW PICTURE IN FINANCE 26 (2016), https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/bracing%20for%20seven%20critical%20changes%20as%20fintech%20matures/fintechnicolor-the-new-picture-in-finance.ashx; *see also* SUBAS ROY, MICHAEL HEANEY, & HANJO SEIBERT, OLIVER WYMAN, REGTECH ON THE RISE: TRANSFORMING COMPLIANCE INTO COMPETITIVE ADVANTAGE (2018), https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/may/RegTech-on-the-Rise.pdf.

9 *See* Dan Murphy, *Big Tech's Invasion of Banking*, MILKEN INST. REVIEW (Apr. 26, 2019), https://www.milkenreview.org/articles/big-techs-invasion-of-banking; Peter Rudegeair & Liz Hoffman, *Next in Google's Quest for Consumer Dominance: Banking*, WALL ST. J. (Nov. 13, 2019), https://www.wsj.com/articles/next-in-googles-quest-for-consumer-dominancebanking-11573644601; Kari Paul, *Libra: Facebook launches cryptocurrency in bid to shake up global finance*, GUARDIAN (June 18, 2019), https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions; Donna Fuscaldo, *Shopify Wants to Launch Millions of Small Businesses And Thinks $200 Loans Is The Way*, FORBES (Jan. 14, 2020), https://www.forbes.com/sites/donnafuscaldo/2020/01/14/shopify-wants-to-launch-millions-of-small-businesses-and-thinks-200-loans-is-the-way/#3e57da5e1e41.

Now, roughly a decade after the fintech revolution started to gather momentum, the financial services landscape is more diverse and complex than ever. Indirect customer relationships are increasingly common, as companies offer their products and services through a constellation of service providers and partners, which themselves may or may not be financial institutions.[10] The result is a fragmented, interconnected, and interdependent web of companies contributing various elements that are packaged into a financial product or service behind the scenes, mostly invisible to the customer.[11]

New Data and New Intermediaries

Finance has always been a data-driven industry.[12] As financial services have become increasingly digitized, however, the volume of data in financial services has exploded and new types of data intermediaries have emerged.[13] Between the nodes in the new financial services landscape flow huge volumes of customer financial data, including personally identifiable information, transaction history, and credit performance, as well as a multitude of other observations about customers and their financial behavior.[14] Although many of these flows are invisible to the customer and are initiated by financial institutions themselves, such as when a bank shares customer data with an affiliate, data is also increasingly flowing at the customer's behest. For example, many fintech customers provide permission for their fintech provider of choice to connect to their bank account in order to access their financial data.

In addition to customer financial data, financial services companies are also increasingly using external nonfinancial data, including social media and mobile phone location and device information, for various purposes, such as marketing and identity verification. As more fintech

10 The term "financial institution" has taken on a new level of ambiguity as the financial services ecosystem has evolved. The term has a number of traditional associations that may require updating as new types of entrants emerge, as well as specific statutory and regulatory definitions in certain contexts, such as in the Gramm-Leach-Bliley Act ("GLBA"), that can be challenging to apply to new business models. As used in this report, "financial institution" will refer generally to traditional providers of financial services—such as depository institutions—except where specifically defined. In the context of GLBA discussed in Section III., for example, "financial institution" refers specifically to the term as defined in the statute and implementing regulations.

11 *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 23 (2018).

12 For example, credit bureaus first originated in the 19th century to help merchants underwrite customers with whom they did not have personal relationships. *See* https://www.experianplc.com/media/1323/8151-exp-experian-history-book_abridged_final.pdf.

13 DELOITTE, CRUNCH TIME SERIES FOR CFOS, CRUNCH TIME I: FINANCE IN A DIGITAL WORLD 7, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance-transformation/sea-ft-crunchtime.pdf; Barry Libert and Megan Beck, *Leaders Need AI To Keep Pace With The Data Explosion*, FORBES (Mar. 26, 2019), https://www.forbes.com/sites/barrylibert/2019/03/26/leaders-need-ai-to-keep-pace-with-data/#61030ca691e0.

14 *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 44–54 (2018).

companies are created, the number of connections in this network and the amount and variety of data flowing among them grow geometrically.[15]

As this ecosystem has grown, both existing and new data intermediaries have sought to meet the increasing demand for customer financial data. These intermediaries have built solutions to enable the transfer of financial data between those holding data about customers ("data holders") and those seeking to use that data for a particular purpose ("data users"). Although the core function of data intermediaries may be similar—the movement of data from one location to another —there are important differences among the types of companies performing this function in different contexts. Some data intermediaries have been around for many years, and may be relatively familiar to many consumers. Credit bureaus, for example, allow lenders to access borrower data assembled from data furnished by other firms. Other data intermediaries are more novel and have emerged in response to growing demand for financial data not provided by existing intermediaries. For example, "data aggregators" have emerged relatively recently in order to provide various types of firms with access to financial data housed in consumers' various financial accounts. Without access to this type of data, many fintech companies would be unable to provide the products and services they offer to their customers today.

In many ways, the centrality of data aggregators in the new financial services landscape has made them the locus of current debates over data governance in financial services, and an appealing acquisition target for larger firms. Over the last few years, large depository institutions have sparred with data aggregators about which data they should be able to access and the means with which they access it.[16] Many of the largest independent data aggregators have been, or are in the process of being, acquired, including Yodlee by Envestnet in 2015, Quovo by Plaid in 2019, Plaid by Visa in 2020, and Finicity by Mastercard.[17] Akoya—previously a data

15 *See* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 44–54 (2018).

16 Penny Crosman, *Wells Fargo's Bid to Vanquish Screen Scraping*, AM. BANKER (June 7, 2016), https://www.americanbanker.com/news/wells-fargos-bid-to-vanquish-screen-scraping.

17 Bradley Hope, *Envestnet Deal Values Yodlee at $590 Million*, WALL ST. J. (Aug. 10, 2015), https://www.wsj.com/articles/envestnet-deal-values-yodlee-at-590-million-1439245934#:~:text=Bradley%20Hope.-Biography&text=Envestnet%20Inc.%2C%20ENV%20%2D2.38.company%20at%20about%20%24590%20million; Kate Rooney, *Fintech start-up Plaid to buy competitor Quovo for $200 million in its first major deal*, CNBC (Jan. 8, 2019), https://www.cnbc.com/2019/01/08/fintech-start-up-plaid-to-buy-competitor-quovo-for-200-million-in-its-first-major-deal.html; Telis Demos, ***Visa's Bet on Plaid Is Costly but Necessary***, WALL ST. J. (Jan. 14, 2020), https://www.wsj.com/articles/visas-bet-on-plaid-is-costly-but-necessary-11579001400; David Heun, *Mastercard to buy Finicity to improve open banking services*, AM. BANKER (June 23, 2020), https://www.americanbanker.com/news/mastercard-to-buy-finicity-to-improve-open-banking-services.

aggregation service created by Fidelity—was spun out in 2020 as an independent company jointly owned by Fidelity, The Clearing House, and 11 of its member banks.[18]

Recent acquisitions and partnerships among different types of data intermediaries may indicate that the financial data ecosystem is in a moment of transition where previously distinct business models are blending together.[19] For example, Finicity, whose acquisition by Mastercard has recently been announced and which also received a significant investment from Experian, partnered with Experian and FICO to launch a new credit score powered by Finicity's data aggregation technology.[20]

Context and Principles

When industries undergo transformation at the speed and depth that financial services markets have over the last two decades, it is prudent to consider whether the current legal regime is well-tailored to the needs of stakeholders and whether it advances important public policy objectives. In this case, it may be worthwhile to evaluate whether the policy objectives underlying current law with respect to financial data are valid and comprehensive; whether current law and regulation are still adequate to promote those policy goals; and where the current regime is showing strain or giving rise to uncertainty.

The rapid evolution of the financial services industry and commerce more generally has already spurred significant changes to the laws and regulations governing data in other countries and among several U.S. states. For example, through its Payment Services Directive (PSD2)[21] and General Data Protection Regulation (GDPR),[22] the European Union has implemented sweeping changes to regulations governing payment systems and general data protection and privacy, respectively. In addition, U.S. states are increasingly active in considering or adopting new

18 Justin Baer, *Fidelity's Parent Company Is Spinning Out Its Akoya Personal-Data Startup*, WALL ST. J. (Feb. 20, 2020), https://www.wsj.com/articles/fidelitys-parent-company-is-spinning-out-its-akoya-personal-data-startup-11582202940#:~:text=Fidelity%20Investments'%20parent%20company%20is,called%20Akoya%2C%20two%20years%20ago; *see also* Press Release, Fidelity Investments, Financial Industry To Give Consumers More Control Over Their Data (Feb. 20, 2020), https://www.fidelity.com/bin-public/060_www_fidelity_com/documents/press-release/akoya-independent-company-022020.pdf.

19 Penny Crosman, *What the Visa-Plaid merger means for banks, fintechs*, AM. BANKER (Jan. 16, 2020), https://www.americanbanker.com/news/what-the-visa-plaid-merger-means-for-banks-fintechs; *see also* Sam Adriance, *The Future of Interconnected Banking is Now, and It's Brought to You by APIs*, AM. BAR ASS'N—CONSUMER FIN. SERVS. COMM. NEWSLETTER (Dec. 5, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/consumer/2019/201911/banking/; Donna Fuscaldo, *Plaid And Quovo Just Scratching The Surface With Data Aggregation*, FORBES (Feb. 6, 2019), https://www.forbes.com/sites/donnafuscaldo/2019/02/06/plaid-and-quovo-just-scratching-the-surface-with-data-aggregation/#1f3627a01841.

20 Press Release, Finicity, Experian, FICO and Finicity Launch New UltraFICO Score (Oct. 22, 2018), https://www.finicity.com/experian-fico-and-finicity-launch-new-ultrafico-credit-score/.

21 European Union, European Commission, *Frequently Asked Questions: PSD2* (Sept. 13, 2019), https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_5555.

22 European Union, European Commission, *Two years of the GDPR: Questions and answers* (June 24, 2020), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166.

privacy and general data protection laws largely outside of the financial context, most notably the California Consumer Privacy Act[23] that went into effect on January 1, 2020. Interest in a general federal consumer data privacy law that would not be limited to financial services has also attracted attention on Capitol Hill on both sides of the aisle.[24]

Over the last few years, there have also been several important efforts by both regulators and nonprofits to articulate principles to guide the regulation of financial data and consumer data more generally in the United States.[25] Each of these proposals is predicated on the observation that technology and business model changes are challenging the existing legal and regulatory system governing financial data. Although the details vary, the principles encompass several important common themes, including data access, accuracy, control, security, minimization, and transparency, among others.

Foundation for the Future

As stakeholders consider the future of the financial data ecosystem, our hope is that this report can contribute to a foundational understanding of the current framework of financial data regulation to inform future policy analyses and dialogues.[26] The paper opens in the remainder of Section I with a description of relevant private sector participants in the financial data ecosystem and a summary of the primary regulatory agencies responsible for their oversight. In each subsequent section, the paper discusses the main bodies of U.S. federal law governing consumer financial data, and, in particular, the types of entities and data covered, nature of regulatory oversight, and substantive requirements pertaining to financial data. Throughout the paper, commentary sections provide a sampling of open issues, areas of ambiguity, and other

23 CAL. CIV. CODE § 1798.100 *et seq.*

24 Cong. Research Serv., LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS (2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10441 (detailing and comparing six consumer privacy bills introduced by members of Congress in 2019 and 2020). Most recently, Senator Sherrod Brown of Ohio introduced the Data Accountability and Transparency Act ("DATA"), which broadly aims to shift the burden of responsibility for protecting consumer data from consumers to companies. See Data Accountability and Transparency Act, Discussion Draft, 116th Cong. (2020), https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf; Geoffrey A. Fowler, *Nobody reads privacy policies. This senator wants lawmakers to stop pretending we do.*, WASHINGTON POST (June 18, 2020), https://www.washingtonpost.com/technology/2020/06/18/data-privacy-law-sherrod-brown/.

25 *See* CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; CTR. FOR FIN. SERVS. INNOVATION, CFSI'S CONSUMER DATA SHARING PRINCIPLES: A FRAMEWORK FOR INDUSTRY-WIDE COLLABORATION (2016), https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2016/10/31152340/2016_Data-Sharing-Principles1.pdf; FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS—APPENDIX D: DATA SHARING PRINCIPLES AND FRAMEWORKS 158–65 (2020), https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf.

26 Any such effort necessarily must omit some detail, and this paper is no exception. Readers are encouraged to consult other sources to learn about the important regulatory developments pertaining to data regulation in the individual fifty states as well as internationally.

timely topics related to the application of current law and regulation to the rapidly evolving financial services landscape.

While the recitation of interpretive and policy issues is not exhaustive, it is intended to convey a sense of the importance and breadth of questions that are being raised and issues that are being debated by stakeholders. Some cross-cutting questions, such as the efficacy of consumer protections and rights that change as financial data passes downstream to different types of companies, may need to be addressed across multiple bodies of law. Similarly, broad issues touched on by multiple existing laws, such as consent, accuracy, and information security, may benefit from a more unified approach across different financial services markets and regulatory schemes.

This report is being released as a working paper, and we welcome input on both the descriptions of current law and the list of issues. Please forward such information to **DataLandscape@finreglab.org.**

For some, this paper will be an introduction to the topic of financial data regulation. For others, it will be a refresher or a reference. In all cases, however, we hope that it will stimulate discussion and debate of areas where policymakers, market participants, consumer advocates, academics, and others should be attentive to how new data, new technologies, and new financial services providers are reshaping financial services. We also hope that it can serve as a useful point of comparison and even inspiration for parallel efforts in other regulated industries, as the emergence of new data and technologies, new intermediaries and service providers, and new legal and regulatory questions occurs beyond the financial data ecosystem.

B. Market Participants

The last two decades have witnessed a rapid evolution in the financial services ecosystem and an explosion in the quantity and use cases of financial data, as well as an increasing diversity in the kinds of companies holding data, using data, and serving as data intermediaries. The lines between the three types of companies have become increasingly blurred as individual companies may act in more than one capacity at different times.

For example, fintech companies may use financial data held by banks to offer their own consumer finance products, but then may generate and hold their own financial data from those new products. Account-holding financial institutions, such as banks, credit unions, and

broker-dealers, historically have been the primary creators and repositories of consumer and small business financial data. As they strive to deepen existing relationships and attract new customers, however, account-holding financial institutions may themselves also pull together data from other sources and share data with service providers. Just as the lines between data holder and data user have become more blurred, the types of data intermediaries have grown more varied.

The purpose of this section is to serve as an introduction to the different market participants to inform later discussion of the legal and regulatory landscape governing them.

1. Depository Institutions

Depository institutions refer to financial institutions chartered under federal or state law, with powers provided under law to accept deposits, pay checks, and make loans.[27] U.S. depository institutions can be chartered at the federal or state level and may be overseen by several different regulatory agencies. National banks and federal savings associations are chartered and supervised by the Office of the Comptroller of the Currency (OCC).[28] State-chartered banks are overseen by state bank regulators, as well as by either the Federal Reserve Board (FRB), if they are members of the Federal Reserve System, or the Federal Deposit Insurance Corporation (FDIC), if they are nonmember banks.[29] The FDIC has backup authority over all insured banks and savings associations in its role as the administrator of the Deposit Insurance Fund, the fund created to protect deposits at insured banks.[30] The FRB also supervises all holding companies of insured banks as defined in the Bank Holding Company Act (BHCA).[31]

Industrial loan companies (ILCs), also referred to as industrial loan banks, are financial institutions that have many of the same powers as traditional banks,[32] but are excluded from the definition of "bank" under BHCA.[33] Parent companies of ILCs thus are not bank holding companies supervised by the FRB and do not need to adhere to BHCA requirements, such as

27 See, e.g., 12 U.S.C. §24.

28 12 U.S.C. § 21 *et seq.*

29 12 U.S.C. §§ 248, 1811 *et seq.*

30 12 U.S.C. §§ 1815, 1821.

31 12 U.S.C. §§ 1841, 1844.

32 One notable exception is that ILCs are prohibited from accepting demand deposits. *See* 12 C.F.R. § 204.2(b)(1).

33 12 U.S.C. § 1841(c)(2)(H).

activity restrictions.[34] Instead, ILCs are chartered by the states and supervised at the federal level by the FDIC.[35]

Credit unions are cooperative, nonprofit depositories.[36] Credit unions can be federally or state-chartered, but all federally chartered credit unions, and nearly all state-chartered credit unions, are overseen and insured by the National Credit Union Administration (NCUA).[37]

2. Nonbank Lenders, Finance Companies, and Alternative Financial Services Companies

There are a wide variety of non-bank lenders, finance companies, and alternative financial services companies that provide consumers and small businesses with access to cash and credit pursuant to different terms, cost, and structures. These providers include licensed lenders, loan brokers, payday lenders, pawn companies, and check cashers, among others. Such companies are often subject to licensure and examination at the state level, as well as enforcement by the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) and in some cases examination and supervision at the federal level by the CFPB.[38]

3. Loan Servicers and Other Credit-Related Companies

A host of companies exist to serve the needs of creditors and borrowers in connection with existing credit and other debts. Loan servicers manage the repayments from borrowers after loans have been made. Debt collectors seek to act on behalf of third-party debt holders by collecting on liabilities that are delinquent or in default. Debt buyers purchase debt and seek to collect in their own name. In addition, a host of nonprofit and for-profit companies offer products and services to borrowers who are not able to meet their financial commitments, such as credit counselors and debt settlement firms. Companies known as credit repair organizations offer to help consumers improve their credit scores by reviewing and correcting inaccurate data held by credit reporting agencies, among other activities. Many of these companies are subject to state

34 *See* 12 U.S.C. § 1843.

35 *See* 12 U.S.C. § 1813(a)(2).

36 Under federal law, credit unions are excluded from the definition of depository institutions but play a nearly identical functional role in the financial ecosystem. *See* 12 U.S.C. 1813(c).

37 12 U.S.C. §§ 1756, 1757, 1784. Most state-chartered credit unions participate in the NCUA's deposit insurance program and, as such, are subject to oversight by the NCUA as well as by their state regulator. *See* NAT'L ASS'N OF FEDERALLY INSURED CREDIT UNIONS, 2018 NAFCU REPORT ON CREDIT UNIONS 5 (Nov. 2018), https://www.nafcu.org/sites/default/files/uploads/Data%20%26%20Tools/Report%20on%20CUs/NAFCU%20Report%20on%20Credit%20Unions%20-%202018.pdf.

38 See Section I.C.1. for more information regarding the jurisdiction of the CFPB and FTC.

licensing and oversight, as well as enforcement by the FTC and CFPB and, in some cases, examination and supervision at the federal level by the CFPB.[39]

4. Payment Networks, Payment Processors, Remittance Companies, and Other Payment-Related Companies

Payment networks, often called card networks or associations, are the companies that provide the infrastructure to enable point-of-sale and e-commerce transactions. Usually branded on debit and credit cards issued by depository institutions, the four major payment network companies are Visa, MasterCard, American Express, and Discover.[40] Payment networks primarily rely on self-governance standards and processes through the Payment Card Industry Data Security Council that issues the industry wide Payment Card Industry Data Security Standards (PCI DSS).[41]

Beyond effectuating specific individual transactions, payment networks are increasingly acting as data intermediaries for secondary purposes. By virtue of their position in the payment flows, payment networks have visibility into billions of annual transactions that comprise an enormous amount of financial data. They can download and store information about the transactions that move across their networks. These troves of financial data can be analyzed, sorted, and packaged into anonymized, aggregated analytics sold to third parties for a variety of reasons, including marketing, consumer spending research, and investment analysis.[42] In January 2020, Visa announced the purchase of the prominent data aggregator Plaid,[43] and in June 2020, MasterCard announced the purchase of Finicity.[44]

In addition to payment networks themselves, there are large and diverse group companies serving the payments needs of consumers and small and large businesses. These companies include payment processors, payment facilitators, remittance companies, and payment

39 See Section I.C.1. for more information regarding the jurisdiction of the CFPB and FTC.

40 CONG. RESEARCH SERV., R45927, U.S. PAYMENT SYSTEM POLICY ISSUES: FASTER PAYMENTS AND INNOVATION 10 (2019), https://fas.org/sgp/crs/misc/R45927.pdf.

41 *See* PCI DSS, https://www.pcisecuritystandards.org/pci_security/.

42 Peter Cohan, *Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data*, FORBES (Jul. 22, 2018), https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/; Geoffrey A. Fowler, *The spy in your wallet: Credit cards have a privacy problem*, DENVER POST (Aug. 31, 2019), https://www.denverpost.com/2019/08/31/credit-card-privacy-concerns/.

43 Cara Lombardo & AnnaMaria Andriotis, *Visa to Pay $5.3 Billion for Fintech Startup*, WALL ST. J. (Jan. 13, 2020), https://www.wsj.com/articles/visa-nears-deal-to-buy-fintech-startup-plaid-11578948426.

44 Lulsa Beltran, *Mastercard Is Going Deeper Into Fintech With Deal for Finicity*, BARRON'S (June 23, 2020), https://www.barrons.com/articles/mastercard-to-acquire-finicity-in-a-nearly-1-billion-deal-51592928431.

technology providers, among others. Many of these companies are subject to money transmission or money services business licensing and examination requirements at the state level, FTC and CFPB enforcement authority, and, in some cases, CFPB examinations.[45]

5. Securities and Commodities Firms

Securities firms, such as broker-dealers and registered investment advisers, provide consumers and businesses with access to trading, wealth management, and investment fund products. Broker-dealers are subject to oversight by the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA), and registered advisers are overseen by the SEC.[46] Providers of derivatives products, such as futures, swaps, and certain kinds of options, are subject to the authority of the Commodity Futures Trading Commission (CFTC).[47]

6. Insurance Companies

The insurance industry is composed of a number of different types of actors, including insurance carriers, insurance agents and brokers, managing general agents, and reinsurers. Insurance companies offer a variety of insurance products and services, such as property and casualty insurance, health insurance, and life insurance. Insurance companies, agents, and brokers are licensed and supervised by state insurance regulators.

7. Consumer Reporting Agencies

Consumer reporting agencies (CRAs) collect information about consumers from various third parties, compile that information, and then provide "consumer reports" to companies that use that information. CRAs, companies that supply information to the CRAs ("furnishers"), and users of consumer reports are governed by the Fair Credit Reporting Act (FCRA), which limits the provision of consumer reports by CRAs only for "permissible purposes."[48] Although there are a large number of specialty CRAs providing consumer reports for specific use cases or market

45 See Section I.C.1. for more information regarding the jurisdiction of the CFPB and FTC.

46 15 U.S.C. § 78d *et seq.*; *see also* CONG. RESEARCH SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 18 (2020), https://crsreports.congress.gov/product/pdf/R/R44918/8.

47 7 U.S.C. § 1 et seq; *see also* CONG. RESEARCH SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 19 (2020).

48 15 U.S.C. § 1681b. See Section IV. for more information on the Fair Credit Reporting Act.

segments, the Big 3 nationwide CRAs—TransUnion, Equifax, and Experian—are the largest and most well-known.[49]

8. Data Aggregators

Data aggregators are technology companies that facilitate the transfer of financial data. Data transfers could be for internal use by data holders, such as to transfer data between the internal systems of two companies that have merged but not yet integrated their systems. Alternatively, and increasingly more common, such transfers can be at the direction of consumers who want to move their data from data holders (often account-holding depository institutions) to nonaffiliated financial services providers (such as consumer-facing fintech companies). Data aggregators typically obtain financial data from data holders in one of two ways: by "screen scraping" the data holder's website or through the data holder's application programming interface (API).

Screen scraping refers to "the automated, programmatic use of a website impersonating a web browser, to extract data or perform actions that users would usually perform manually on the website."[50] By accessing the consumer account with login credentials provided by a consumer to a data aggregator, the data aggregator can extract financial data from a financial institution's website and, in turn, provide that data to the data user. API transfer occurs when a data holder opens a connection between itself and the aggregator that allows the aggregator to directly request and receive financial data from the data holder.[51] Unlike screen scraping, APIs do not require the data aggregator to store users' login credentials.[52] API access, however, typically requires a relationship between the aggregator and data holders, whereby data holders permit the aggregator to query and receive requested data.

As noted above, many of the largest independent data aggregators have been acquired or are in the process of being acquired, including Yodlee by Envestnet in 2015, Quovo by Plaid in 2019, Plaid by Visa in 2020, and Finicity by Mastercard in 2020 (although the latter two

49 *See* CFPB, LIST OF CONSUMER REPORTING COMPANIES (2020), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-companies-list.pdf.

50 The Open Banking Hub, *Screen Scraping 101: Who, What, Where, When?* (July 19, 2017), https://openbankinghub.com/screen-scraping-101-who-what-where-when-f83c7bd96712.

51 *See* MCKINSEY & CO., *Data sharing and open banking* (Sept. 5, 2017), https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking (defining an API as "an intelligent conduit that allows for the flow of data between systems in a controlled yet seamless fashion").

52 U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 26 (2018).

acquisitions are still awaiting approval).[53] Akoya—previously a data aggregation service created by Fidelity—was spun out in 2020 as an independent company jointly owned by Fidelity, The Clearing House, and 11 of its member banks.[54] Finicity, which recently announced it is going to be acquired by Mastercard, partnered with Experian and FICO to launch a new credit score powered by Finicity's data aggregation technology.[55]

9. Data Brokers

Data brokers collect and sell data but are not unique to the financial services industry. Indeed, the term "data broker" is a catchall term for the companies that collect and sell data of all sorts—financial and non-financial alike. Although they do not necessarily traffic in financial data, data brokers play an important role in the financial ecosystem. Data brokers generally do not have any formal relationship with the persons about whom they store data and do not generally seek permission from consumers before transferring such information.[56] Many participants in the financial data ecosystem transact with data brokers for nonfinancial data to improve their product offerings or outsource data collection or verification. For example, depository financial institutions have statutory and regulatory obligations to "know your customer" (KYC) and prevent their services from being used for fraudulent activities and money laundering. Upon collecting information from a customer or business applying for a loan or opening a new account, banks may cross-check the provided information with data brokers to query whether the information is accurate.

10. Financial Technology Companies

Financial technology companies—frequently referred to as "fintech companies" or just "fintechs"—have emerged as important players in the financial services ecosystem. Although fintech companies are included in many of the categories discussed above, they are also discussed separately here. Despite the recent emergence of the term "fintech," technology and

53 Bradley Hope, *Envestnet Deal Values Yodlee at $590 Million*, WALL ST. J. (Aug. 10, 2015); Kate Rooney, *Fintech start-up Plaid to buy competitor Quovo for $200 million in its first major deal*, CNBC (Jan. 8, 2019); Telis Demos, *Visa's Bet on Plaid Is Costly but Necessary*, WALL ST. J. (Jan. 14, 2020); David Heun, *Mastercard to buy Finicity to improve open banking services*, AM. BANKER (June 23, 2020).

54 Justin Baer, *Fidelity's Parent Company Is Spinning Out Its Akoya Personal-Data Startup*, WALL ST. J. (Feb. 20, 2020); *see also* Press Release, Fidelity Investments, Financial Industry To Give Consumers More Control Over Their Data (Feb. 20, 2020).

55 Press Release, Finicity, Experian, FICO and Finicity Launch New UltraFICO Score (Oct. 22, 2018), https://www.finicity.com/experian-fico-and-finicity-launch-new-ultrafico-credit-score/.

56 FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 11 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

innovation have always played an important role in financial services.[57] Over the last decade, however, the number and diversity of technology-enabled companies have grown significantly, expanding across the financial services industry.[58] The term "fintech" in this paper refers to this trend and "fintech companies" refers to the array of companies that have come to define this movement.

The growth in new fintech companies and related products and services has been driven by a number of simultaneous trends: rapid increase in smartphone penetration; increasing expectations around quality of user experience; lower costs for data processing and computing power; the emergence of new data analytical tools, such as machine learning; and legacy technology overhead among incumbent financial institutions. By leveraging increased digitalization and new technological capabilities in data storage, data processing, and predictive analytics, fintech companies have introduced new products to meet those consumer demands.[59] These products and services can be categorized broadly into the following verticals: (i) payments, clearing, and settlement; (ii) deposits, lending, and capital raising; (iii) insurance; (iv) investment management; (v) personal financial management; and (vi) market and operational support.[60]

Differentiating between traditional financial services providers and fintech companies, however, is increasingly challenging. As alluded to above, some fintechs innovate upon pre-existing financial products, while other fintechs disrupt the system in such a way that makes the pre-existing product class obsolete altogether. Man y fintech companies are no longer the small, scrappy startups they once were, but rather have grown into mature companies commanding significant market share in their specific market segments. Indeed, many fintech companies are examined or regulated at the state and federal level, and some have even sought bank charters.[61] At the same time, many depository institutions and more traditional nondepository financial institutions have invested significantly in technology[62] to update their legacy systems, to acquire

57 Each financial product consumers use today at one point represented a significant financial industry innovation. For example, in the 1960s and 1970s, credit cards, debit cards, and ATMs facilitated consumers' and small businesses' access to funds held in bank accounts. In the 1980s and 1990s, the deregulatory environment produced new financial innovation around derivatives, swaps, and securitization products.

58 SEE DELOITTE CENTER FOR FINANCIAL SERVICES, FINTECH BY THE NUMBERS (2017).

59 MCKINSEY & CO., FINTECHNICOLOR: THE NEW PICTURE IN FINANCE 10 (2016).

60 FIN. STABILITY BD., FINANCIAL STABILITY IMPLICATIONS FROM FINTECH 8 (2017), https://www.fsb.org/wp-content/uploads/R270617.pdf (drawing on categorization from the World Economic Forum (June 2015), "The Future of Financial Services").

61 Press Release, Fed. Deposit Ins. Corp., FDIC Approves the Deposit Insurance Application for Square Financial Services, Inc., (Mar. 18, 2020), https://www.fdic.gov/news/news/press/2020/pr20033.html; *see also* FDIC Order, *Approved: Application for Federal Deposit Insurance and Consent to Merge*, (Feb. 7, 2020) https://www.fdic.gov/regulations/laws/bankdecisions/depins/varo-bank-na-draper-utah.pdf.

62 *See, e.g.*, Elisa Martinuzzi, *The Banking Industry is Spending Wildly on the Latest Tech*, WASHINGTON POST (Jan. 23, 2020), https://www.washingtonpost.com/business/the-banking-industry-is-spending-wildly-on-the-latest-tech/2020/01/23/f9467668-3db2-11ea-afe2-090eb37b60b1_story.html; Dan

or partner with fintech companies, and to develop fintech-like products themselves.[63] As such, there is significant overlap and engagement today between fintech companies and more traditional financial services providers.

11. Large Consumer Technology Companies

Large consumer technology firms, such as Amazon, Apple, Facebook, Google, and Microsoft, have quickly followed in the footsteps of the recent growth and success of independent financial technology companies. From launching their own payment,[64] banking,[65] and lending[66] services to powering the back-end technology enabling financial technology applications,[67] the largest technology companies are increasingly significant participants in the financial services ecosystem.

12. Trade Associations

In recent years, new industry organizations have emerged to help promote standard-setting and policy objectives with respect to the use of financial data by different market actors. For example, the Financial Data and Technology Association (FDATA) is a diverse membership trade group that advocates for general technology-driven innovation that benefits consumers across the financial services ecosystem.[68] The Financial Data Exchange (FDX), on the other hand, was established explicitly to "unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data."[69] FDX promotes the adoption of its common API. The Consumer Data Industry

---

Rosenbaum, *Banks' big tech spending is testing shareholders' patience*, AM. BANKER (Feb. 5, 2020), https://www.americanbanker.com/opinion/banks-big-tech-spending-is-testing-shareholders-patience.

63 *See, e.g.*, Rochelle Toplensky, *Technology is Banks' New Battleground*, WALL ST. J. (Sept. 10, 2019), https://www.wsj.com/articles/technology-is-banks-new-battleground-11568114378.

64 Mike Isaac & Nathaniel Popper, *Facebook Plans Global Financial System Based on Cryptocurrency*, N.Y. TIMES (June 18, 2019), https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html; Mariella Moon, *Tim Cook: Apple Pay transactions doubled year-over-year*, ENGADGET (Oct. 31, 2019), https://www.engadget.com/2019-10-31-apple-pay-growth-census.html.

65 Peter Rudegeair & Liz Hoffman, *Next in Google's Quest for Consumer Dominance: Banking*, WALL ST. J. (Nov. 13, 2019), https://www.wsj.com/articles/next-in-googles-quest-for-consumer-dominancebanking-11573644601.

66 Ron Shevlin, *Amazon's Impending Invasion of Banking*, FORBES (Jul. 8, 2019), https://www.forbes.com/sites/ronshevlin/2019/07/08/amazon-invasion/#7560a7567921.

67 Ron Shevlin, *Google: The Next Big Fintech Vendor*, FORBES (May 11, 2020), https://www.forbes.com/sites/ronshevlin/2020/05/11/google-the-next-big-fintech-vendor/#26f243464cbd; Tom Groenfeldt, *Microsoft And Finastra Partner To Make Finance More Digital*, FORBES (July 20, 2020), https://www.forbes.com/sites/tomgroenfeldt/2020/07/20/microsoft-and-finastra-partner-to-make-finance-more-digital/#391e953761ac; William Girling, *Mastercard and Microsoft empower FinTech innovation*, FINTECHMAGAZINE (July 30, 2020), https://www.fintechmagazine.com/financial-services/mastercard-and-microsoft-empower-fintech-innovation.

68 FIN. DATA AND TECH. ASS'N, https://fdata.global/about/purpose.

69 FIN. DATA EXCHANGE, https://financialdataexchange.org/FDX/About/FAQ.

Association (CDIA) and the National Consumer Reporting Association ("NCRA") are the primary trade groups for CRAs and credit reporting issues.[70] These groups, among others that represent particular types of lenders, payments companies, and other direct financial services providers, drive public conversations about the salient and upcoming issues that financial data market participants face.

C. Regulatory Agencies

The U.S. financial services industry is overseen at the federal level by a diverse group of regulators with broad and often overlapping jurisdiction. In addition, state regulatory agencies and state attorneys general play an important role in the licensing and oversight of depository and non-depository financial institutions. Regulators generally have one or more of the following three broad categories of authority:

Rulemaking authority, which refers to the power to issue rules and regulations to govern covered persons

Examination authority, often referred to as supervisory authority, which is the power to examine, inspect, and oversee covered persons with respect to violations of law and, in some cases, safety and soundness

Enforcement authority, which is the power to take legal action against covered persons for violations of law or regulation, often including the power to mandate remediation and, in some cases, financial penalties

1. Consumer Protection Regulators

The Consumer Financial Protection Bureau and the Federal Trade Commission share responsibility at the federal level with each other (and, for banks and similar entities, with the prudential regulators as well) for protecting consumers from potentially harmful consumer financial products and services. In some cases, the consumer protection laws administered by these agencies also cover commercial financial transactions or relationships.[71]

70 CONSUMER DATA INDUS. ASS'N, https://www.cdiaonline.org/about/about-cdia/; NAT'L CONSUMER REPORTING ASS'N, https://www.ncrainc.org/about-us.html.

71 *See, e.g.*, Section VI.C. discussing the application of the Equal Credit Opportunity Act ("ECOA") to commercial credit.

a. Consumer Financial Protection Bureau

The Dodd-Frank Wall Street Reform and Consumer Financial Protection Act of 2010 (DFA)[72] created the Consumer Financial Protection Bureau (CFPB) to "regulate the offering and provision of consumer financial products or services under the Federal consumer financial laws."[73] The statutory objectives of the CFPB cover the following broad goals:

- Ensuring consumer access to timely and understandable information to make responsible decisions about financial transactions
- Protecting consumers from unfair, deceptive, or abusive acts and practices ("UDAAPs) and from discrimination[74]
- Identifying and addressing outdated, unnecessary, or unduly burdensome regulations to reduce unwarranted regulatory burdens
- Enforcing federal consumer financial laws consistently to promote fair competition
- Promoting transparent and efficient operation of markets for consumer financial products and services to facilitate access and innovation[75]

DFA transferred primary rulemaking authority related to most pre-existing consumer financial protection laws from several other federal financial agencies to the CFPB.[76] When issuing rules, however, the CFPB is required to consult with the prudential bank regulators and other federal agencies "regarding consistency with prudential, market, or systemic objectives administered by such agencies,"[77] and for certain rules to convene panels pursuant to the Small Business Regulatory Enforcement Fairness Act in order to obtain input on regulatory burdens from directly regulated small businesses.[78] Rulemaking authority remained with other federal regulators, however, for segments of certain laws and industries.[79] In particular, rulemaking,

72 Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*).

73 12 U.S.C. § 5491(a).

74 See Section VII.D. discussing the differences between the CFPB's authority over UDAAPs and the FTC's authority over unfair or deceptive acts or practices ("UDAPs").

75 12 U.S.C. § 5511(b).

76 12 U.S.C. § 5581. These laws include the Electronic Fund Transfer Act ("EFTA"), the Equal Credit Opportunity Act ("ECOA"), the Fair Credit Reporting Act ("FCRA"), the Fair Debt Collection Practices Act ("FDCPA"), the Home Mortgage Disclosure Act, the Real Estate Settlement Procedures Act, the Secure and Fair Enforcement for Mortgage Licensing Act, the Truth in Lending Act, and the Truth in Savings Act. *See* 12 U.S.C. § 5481(12).

77 12 U.S.C. § 5512(b)(2); *see also* 12 U.S.C §§ 5531(e), 5581(b)(5)(D).

78 5 U.S.C. §§ 603, 604(a), 609(d) (applying small business regulatory flexibility requirements to CFPB).

79 *See, e.g.*, 12 U.S.C. §§ 5581, 5517. For example, FTC retained rulemaking authority under certain sections of GLBA and FCRA relating to information security issues.

examination, and enforcement authority under federal consumer financial laws focused specifically on data security issues did not transfer to the CFPB from other federal regulators.[80]

DFA also created new substantive consumer protection laws that generally apply to "covered persons," defined as "(A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person."[81] Such consumer financial products and services include, among others, deposit-taking; mortgages, credit cards and other extensions of credit; loan servicing; check guaranteeing; consumer report data collection; debt collection with respect to debts arising out of a consumer financial product; real estate settlement; money transmitting; and financial data processing when such products and services are offered or provided for use by consumers primarily for personal, family, or household purposes.[82]

DFA also reallocated supervisory and enforcement jurisdiction over covered persons. The CFPB has supervisory and enforcement authority over the following covered persons' compliance with most federal consumer financial protection laws:

Nonbanks

The CFPB has plenary supervisory authority over any non-depository covered person that:

- offers or provides origination, brokerage, or servicing of loans secured by real estate for use by consumers primarily for personal, family, or household purposes, or loan modification or foreclosure relief services in connection with such loans;
- offers or provides to a consumer any private education loan; or
- offers or provides to a consumer a payday loan.[83]

The CFPB may also exercise supervisory authority over any nondepository covered person:

- That is a larger participant of a market for other consumer financial products or services as defined by the CFPB rule

80 See Section IV.E.3. for a discussion of the regulatory jurisdiction for FCRA's data security-related rules and Section III.C. for GLBA's Safeguards Rule.

81 12 C.F.R. § 5481(6).

82 *See* 12 U.S.C. § 5481(5), (15).

83 12 U.S.C. § 5514(a)(1)(A), (D)–(E).

- That the CFPB has reasonable cause to determine, by order, after notice to the covered person and a reasonable opportunity for such covered person to respond, based on complaints collected or information from other sources, that such covered person is engaging, or has engaged, in conduct that poses risks to consumers with regard to the offering or provision of consumer financial products or services[84]

The CFPB has issued rules defining larger participants of the consumer reporting market, the consumer debt collection market, the student loan servicing market, the international money transfer market, and the automobile financing market.[85] Under its supervisory authority over covered persons in its jurisdiction, the CFPB is required to conduct periodic examinations, which must be based on the CFPB's assessment of the risks posed to consumers based on asset size, transaction volume, state regulatory oversight, and other factors related to the covered person.[86] The CFPB must coordinate its supervisory activities with those of prudential regulators and state bank regulators to minimize regulatory burdens on covered persons.[87]

The CFPB also has enforcement authority over covered persons that are nondepository institutions—irrespective of whether the CFPB has supervisory authority—but must coordinate its efforts with the FTC, which has overlapping jurisdiction.[88] The agencies have entered into a Memorandum of Understanding to coordinate on their regulatory and enforcement efforts.[89] Certain nondepository persons are generally excepted from the scope of the CFPB's rulemaking, supervisory and enforcement authority, including certain providers of retail installment credit, most automobile dealers, real estate brokers and agents, financial intermediaries registered with the SEC and CFTC, and insurance companies.[90]

Depository Institutions

The CFPB has supervisory and examination authority over depository institutions with over $10 billion in assets and their affiliates with respect to compliance with most federal consumer financial laws.[91] In contrast, depository institutions with $10 billion or less in total assets are

84 12 U.S.C. § 5514(a)(1)(B)–(C).

85 12 C.F.R. §§ 1001, 1090.

86 12 U.S.C. § 5514(b)(2).

87 12 U.S.C. § 5514(b)(3).

88 12 U.S.C. § 5514(c)(3).

89 FTC-CFPB, MEMORANDUM OF UNDERSTANDING (Feb. 25, 2019), https://www.ftc.gov/system/files/documents/cooperation_agreements/ftc-cfpb_mou_225_0.pdf.

90 12 U.S.C. §§ 5517, 5519. In some cases, persons are not excepted from CFPB jurisdiction if they offer or provide a consumer financial product or service in addition to their other offerings.

91 12 U.S.C. §§ 5581(c)(1), 5515.

subject to consumer financial protection supervision by their applicable prudential regulator.[92] The CFPB may require such depository institutions to submit reports to aid in detecting consumer risks and participate on a limited basis in examinations conducted by the prudential regulator.[93]

Similarly, the CFPB has primary enforcement authority over depository institutions with over $10 billion in assets and their affiliates with respect to most federal consumer protection laws.[94] Federal prudential regulators may recommend that the CFPB initiate an enforcement action against a large depository institution; if the CFPB does not initiate the enforcement action within 120 days, the other agency may itself initiate an enforcement action.[95] The CFPB has no enforcement authority over depository institutions with $10 billion or less in assets or their affiliates.[96]

Service Providers

Under DFA, the CFPB has supervisory and enforcement authority over service providers to covered persons that are subject to CFPB supervision, whether such entities are affiliated or unaffiliated with the covered person.[97] As defined in Section 1002 of DFA, a "service provider" is "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service."[98]

b. Federal Trade Commission

The Federal Trade Commission (FTC) plays a significant role in the federal regulation of consumer protection issues. Although its jurisdiction overlaps with the CFPB with respect to nondepository providers of consumer financial products and services, the FTC's authority also extends to areas where the CFPB does not have oversight powers.[99] The Federal Trade Commission Act of 1914 (FTC Act) established the FTC for the purpose of "busting the trusts."

---

92 12 U.S.C. §§ 5581(c)(1), 5516.

93 12 U.S.C. § 5516(b)–(c).

94 12 U.S.C. § 5515(c)(1). Prudential regulators may also initiate UDAPs actions against institutions under their oversight, regardless of asset size. See Section VII. for a detailed discussion of UDA(A)P.

95 12 U.S.C. § 5515(c)(2)–(3).

96 12 U.S.C. § 5516(d).

97 *See* 12 U.S.C. §§ 5514(e), 5515(d), 5516(e); *see also* CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 2 (2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceServiceProviderBulletin.pdf. Note that, in the case of smaller depository institutions, persons must be service providers to a "substantial number" of smaller depository institutions in order to be subject to CFPB jurisdiction. 12 C.F.R. § 5516(e). See Section V.B. for further treatment of the regulation of service providers.

98 12 U.S.C. § 5481(26). See Section VII.D.1. for further discussion of the FTC's UDAP authority.

99 *See, e.g.*, the "Safeguards Rule" of GLBA. 15 U.S.C. §§ 6801(b), 6805(b)(2).

[100] The FTC's mandate was later expanded under Section 5 of the FTC Act to police "unfair or deceptive acts or practices," also referred to as "UDAPs," in commerce.[101]

The FTC has jurisdiction over most entities engaged in interstate commerce, which has been interpreted to include most for-profit entities operating within the United States.[102] The FTC Act, however, excepts banks, savings and loan institutions, and federal credit unions from the scope of FTC jurisdiction.[103] FTC's consumer financial protection jurisdiction overlaps significantly with that of the CFPB, covering a broad range of nondepository institutions, such as mortgage companies, mortgage brokers, creditors, and debt collectors, along with service providers to these entities.[104] Under DFA, however, the FTC retained exclusive jurisdiction over most motor vehicle dealers.[105] The FTC has also construed its Section 5 authority broadly to enforce UDAPs with respect to acts or practices that harm small businesses, in addition to consumers.[106]

The FTC is authorized to issue rules and statements of policy regarding UDAPs;[107] however, its UDAP rulemaking authority is subject to substantial procedural requirements beyond that required by the Administrative Procedure Act (APA) for most federal agency rulemakings.[108] The FTC has additional limited rulemaking authority for discrete topics under several other statutes, including the Children's Online Privacy Protection Act (COPPA), the Credit Repair Organizations Act (CROA), FCRA, the Gramm-Leach-Bliley Act (GLBA), and the Telemarketing and Consumer Fraud and Abuse Prevention Act.[109]

---

100 15 U.S.C. § 41 *et seq.*

101 15 U.S.C. §§ 45, 46, 57a.

102 *See F.T.C. v. Sperry & Hutchinson Co.*, 405 U.S. 233, 238–44 (1972) (discussing case law development of the scope of FTC jurisdiction).

103 *See* 15 U.S.C. §§ 46(a)–(b), 57a(f). Violations of Section 5 of the FTC Act are enforced by the prudential bank regulators with respect to the institutions under their jurisdiction pursuant to their powers under Section 8 of the FDI Act. *See* FED. DEPOSIT INS. CORP., FIL-26-2004, UNFAIR OR DECEPTIVE ACTS OR PRACTICES UNDER SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT (2004), https://www.fdic.gov/news/financial-institution-letters/2004/fil2604.html.

104 12 U.S.C. §§ 5514, 5517.

105 12 U.S.C. § 5519(a).

106 *See F.T.C. v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 943 (N.D. Ill. 2008) (noting that the "FTC has construed the term 'consumer' to include businesses as well as individuals. Deference must be given to the interpretation of the agency charged by Congress with the statute's implementation"); *see also*, Fed. Trade Comm'n, *Operation Main Street: Stopping Small Business Scams*, https://www.ftc.gov/news-events/blogs/business-blog/2018/06/operation-main-street-targets-scams-against-small-business.

107 15 U.S.C. § 57a(a).

108 *See* 15 U.S.C. § 57a. Prior to rulemaking, the FTC is required to have reason to believe that the practices to be addressed by the rulemaking are "prevalent." 15 U.S.C. § 57a(b)(3). Once it decides to proceed, it must "(A) publish a notice of proposed rulemaking stating with particularity the text of the rule, including any alternatives, which the Commission proposes to promulgate, and the reason for the proposed rule; (B) allow interested persons to submit written data, views, and arguments, and make all such submissions publicly available; (C) provide an opportunity for an informal hearing in accordance with subsection (c); and (D) promulgate, if appropriate, a final rule based on the matter in the rulemaking record (as defined in subsection (e)(1)(B)), together with a statement of basis and purpose." 15 U.S.C. § 57a(b). Congress has the ability to review proposed rule during this process. 15 U.S.C. § 57a(b).

109 12 U.S.C. § 5519(d); 15 U.S.C. §§ 1679h(a), 6102(a)(1), 6502(b), 6801(b), 6804(a)(1)(C), 6805(b)(2).

The FTC does not have supervisory authority but may request examination reports of covered persons from the CFPB.[110] The FTC may bring enforcement actions for UDAP violations under the FTC Act,[111] as well as for violations of specific statutes, including the Truth in Lending Act (TILA)[112] and the Electronic Fund Transfer Act (EFTA).[113] DFA also authorized the FTC to enforce any CFPB rule applicable to entities within its jurisdiction.[114] Given the significant overlap in jurisdiction, the FTC and CFPB have entered into a Memorandum of Understanding, as required under DFA, to coordinate regulatory and enforcement efforts.[115]

2. Prudential Regulators

The prudential regulators are a group of federal regulators responsible, among other things, for the federal oversight of U.S. insured depository institutions, their holding companies, and foreign banking organizations operating in the United States. Although they share authority in some areas with other regulators, such as the Consumer Financial Protection Bureau and state banking agencies, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration have primary federal responsibility for ensuring the safety and soundness of depository institutions under their jurisdiction. The Federal Financial Institution Examination Council, meanwhile, is the federal body charged with managing the coordination among the prudential regulators, the CFPB, and the State Liaison Committee.

a. Federal Reserve

Established in 1913 with the passage of the Federal Reserve Act, the Federal Reserve System is the central bank of the United States.[116] The Federal Reserve Board of Governors (Federal Reserve or FRB) is the primary governing body of the Federal Reserve System. The Federal Reserve plays a number of important roles with respect to the healthy functioning of the U.S. financial system, including (i) monetary policy implementation, (ii) regulatory oversight, (iii) payment systems operations, and (iv) short-term liquidity to banks through the discount window.[117]

110 12 U.S.C. § 5512(c)(6)(C).

111 15 U.S.C. § 45.

112 15 U.S.C. § 1607(c).

113 15 U.S.C. § 1693o(c).

114 12 U.S.C. § 5581(b)(5)(C)(ii).

115 12 U.S.C. § 5581(b)(5)(D); FTC-CFPB, MEMORANDUM OF UNDERSTANDING (Jan. 12, 2012).

116 12 U.S.C. § 226 *et seq.*

117 12 U.S.C. § 248.

With respect to regulatory oversight, the FRB has authority over a variety of domestic and foreign financial institutions.

Holding Companies: The FRB has safety and soundness oversight powers over companies that control U.S. depository institutions, including (i) bank holding companies and (ii) financial holding companies[118] under BHCA,[119] and (iii) savings and loan holding companies under the Home Owners Loan Act (HOLA).[120] In this role, the FRB also has supervisory authority over the nonbank subsidiaries of such holding companies.[121]

Depository Institutions: The FRB is the primary federal regulator of state-chartered banks that are members of the Federal Reserve System and has broad safety and soundness authority over them.[122] In this role, the FRB shares oversight responsibilities with state bank regulators. With respect to consumer protection issues, the FRB has primary supervisory authority over state member banks (i) with $10 billion or less in consolidated assets for all consumer protection laws; and (ii) with greater than $10 billion in consolidated assets for consumer protection laws that were not transferred to the CFPB under DFA.[123]

Service Providers: In connection with its safety and soundness oversight powers, the FRB may also exercise supervisory powers over service providers to state member banks.[124]

Foreign Banks: The FRB also coordinates the oversight of foreign banking organizations operating in the United States.[125]

Systemically Significant Companies: The FRB has primary responsibility for supervising nonbank companies designated as systemically significant by the Financial Stability Oversight Council.[126]

---

118 A bank holding company "means any company which has control over any bank or over any company that is or becomes a bank holding company" under BHCA. 12 U.S.C. § 1841. A "financial holding company" is any "bank holding company that meets the requirements of section 1843(l)(1)" of BHCA. Authorized by GLBA in 1999, financial holding companies have authority to engage in a broader set of activities than bank holding companies. *See* 12 U.S.C. § 1843(k); 12 C.F.R. § 225.86.

119 12 U.S.C. § 1841 *et seq.*

120 12 U.S.C. § 1467a.

121 12 U.S.C. §§ 1844(c), 1467a(b)(4).

122 12 U.S.C. § 248(a), (n); 12 U.S.C. § 325.

123 12 U.S.C. §§ 5581(c), 5516.

124 See Section V.B.2. for more information on prudential bank regulators' third-party oversight powers.

125 12 U.S.C. § 3105.

126 12 U.S.C. § 5365.

b. Office of the Comptroller of Currency

The Office of the Comptroller of the Currency (OCC) is an independent branch of the United States Department of the Treasury.[127] Established in 1863 by the National Bank Act,[128] the OCC is responsible for chartering, regulating, and supervising federal depository institutions, including national banks[129] and federal savings associations,[130] as well as federal branches and agencies of foreign banking organizations.[131] In this role, the OCC has broad safety and soundness oversight authority over its regulated institutions. The OCC may also exercise supervisory powers over operating subsidiaries[132] and service providers to such institutions.[133]

With respect to consumer protection laws, the OCC has primary supervisory and enforcement authority over national banks (i) with $10 billion or less in consolidated assets for all consumer protection laws; and (ii) with greater than $10 billion in consolidated assets for consumer protection laws that were not transferred to the CFPB under DFA.[134]

c. Federal Deposit Insurance Corporation

The Federal Deposit Insurance Corporation (FDIC) is an independent federal agency established by the Banking Act of 1933, also known as the Glass-Steagall Act.[135] Created in the aftermath of the Great Depression, the FDIC's primary mission is to provide insurance for banking deposits at depository institutions to instill confidence in the U.S. banking system.[136] The FDIC is governed by a Board of Directors composed of three members appointed by the President and confirmed by the Senate, the Comptroller of the Currency, and the Director of the CFPB.[137]

Under the Federal Deposit Insurance Act (FDI Act), the FDIC is the primary federal supervisor of state-chartered banks and savings associations that are not members of the Federal Reserve System and has backup supervisory authority over the remaining insured federally and

127 12 U.S.C. § 1.

128 12 U.S.C. § 1.

129 12 U.S.C. § 21 *et seq.*

130 12 U.S.C. § 1463(a)(1)(A). Prior to DFA, federal savings associations were supervised by a separate federal agency, the Office of Thrift Supervision.

131 12 U.S.C. § 3102.

132 12 C.F.R. § 5.34(e)(3).

133 See Section V.B.2. for more information on prudential bank regulators' third-party oversight powers.

134 12 U.S.C. §§ 5516, 5581.

135 Pub. L. No. 73-66, 48 Stat. 162 (1933) (codified as amended at 12 U.S.C. § 227).

136 12 U.S.C. § 1811 *et seq.*

137 12 U.S.C. § 1812.

state-chartered banks in the United States.[138] The FDIC also oversees third-party service providers to insured depository institutions under its jurisdiction.[139] The FDIC administers the Deposit Insurance Fund (DIF), to which insured depository institutions make periodic contributions as required by law.[140] The FDIC has broad resolution powers over insured depository institutions in the event of their failure.[141]

With respect to consumer protection laws, the FDIC has supervisory and enforcement authority over state-chartered nonmember banks (i) with $10 billion or less in consolidated assets for all consumer protection laws and (ii) with greater than $10 billion in consolidated assets for consumer protection laws that were not transferred to the CFPB under DFA.[142]

d. National Credit Union Administration

The National Credit Union Administration (NCUA) is an independent federal agency responsible for chartering federal credit unions.[143] Established by the Federal Credit Union Act of 1934, the NCUA has exclusive regulatory and supervisory authority over federal-chartered credit unions.[144] The NCUA also has broad examination authority over state-chartered credit unions that elect to be federally insured.[145] Unlike the other federal prudential regulators, the NCUA does not have supervisory authority over service providers to federal credit unions.[146]

Similar to the FDIC's operation of the DIF, the NCUA operates and manages the National Credit Union Share Insurance Fund (NCUSIF).[147] All federal credit unions, and those state-chartered credit unions that elect to be federally insured, must contribute to the NCUSIF in order to insure their deposits.[148]

With respect to consumer protection laws, the NCUA has supervisory and enforcement authority over credit unions (i) with $10 billion or less in consolidated assets for all consumer protection

138 12 U.S.C. §§ 1811, 1818, 1821, 1831p-1.

139 See Section V.B.2. for more information on prudential bank regulators' third-party oversight powers.

140 12 U.S.C. § 1821.

141 12 U.S.C. §§ 1821a, 1822.

142 12 U.S.C. §§ 5516, 5581.

143 12 U.S.C. §§ 1753, 1754.

144 12 U.S.C. §§ 1756, 1757.

145 12 U.S.C. § 1784.

146 See Section V.B.2. for more information on prudential bank regulators' third-party oversight powers.

147 12 U.S.C. §§ 1782, 1783.

148 12 U.S.C. §§ 1781, 1787(k).

laws and (ii) with greater than $10 billion in consolidated assets for consumer protection laws that were not transferred to the CFPB under DFA.[149]

e. Federal Financial Institutions Examination Council

Established by the Financial Institutions Regulatory and Interest Rate Control Act of 1978,[150] the Federal Financial Institutions Examination Council (FFIEC) is an interagency body assigned to "prescribe uniform principles and standards for the Federal examination of financial institutions" and "make recommendations to promote uniformity in the supervision of these financial institutions."[151] The FFIEC is composed of six representatives from the following member agencies: the FRB, the OCC, the FDIC, the NCUA, the CFPB, and the State Liaison Committee.[152] The FFIEC's statutory functions include:

- Establishing uniform principles, standards and report forms for use by the prudential regulators in their supervisory examinations
- Making "recommendations for uniformity in other supervisory matters, such as, but not limited to, classifying loans subject to country risk, identifying financial institutions in need of special supervisory attention, and evaluating the soundness of large loans that are shared by two or more financial institutions"
- Developing a uniform reporting system for federally supervised depository institutions and their affiliates
- Conducting schools for federal prudential examiners[153]

In fulfilling its responsibilities for interagency coordination among the prudential bank regulators, the FFIEC issues rules and guidance on a variety of topics, including information technology, cybersecurity, third-party risk management, and Bank Secrecy Act and anti-money laundering compliance.[154] The prudential regulators are required to give the FFIEC access to their books

149 12 U.S.C. §§ 5516, 5581.

150 Pub. L. No. 95-630, 92 Stat. 3641 (1978) (codified at 12 U.S.C. § 226).

151 12 U.S.C. § 3301.

152 The State Liaison Committee ("SLC") is composed of a primary state banking regulator from five separate states, one of whom is elected Chairman. The Chairman represents the SLC on the FFIEC. The purpose of the SLC is to "encourage the application of uniform examination principles and standards" by state and federal supervisory agencies. 12 U.S.C. § 3306.

153 12 U.S.C. § 3305.

154 *See* FED. FIN. INST. EXAMINATION COUNCIL, ANNUAL REPORT 2019, https://www.ffiec.gov/PDF/annrpt19.pdf.

and records, including reports of examination of supervised entities under their jurisdiction.[155] The FFIEC is also required by statute to assist the prudential regulators in periodically reviewing all regulations issued under their collective jurisdictions to "identify outdated or otherwise unnecessary regulatory requirements imposed on insured depository institutions."[156]

3. Other Federal Regulators

The Securities and Exchange Commission and the Commodity Futures Trading Commission lead the federal oversight and regulation of the securities and derivatives markets, respectively.

a. Securities and Exchange Commission

In 1934, Congress passed the Securities Exchange Act, establishing the Securities and Exchange Commission (SEC).[157] The SEC has broad authority over all aspects of the securities industry, including registration, regulation, and oversight of brokerage firms, transfer agents, and clearing agencies.[158] The SEC also oversees securities industries' self-regulatory organizations, such as the Financial Industry Regulatory Authority (FINRA), which play an important role in the governance of the securities market.[159] Since the passage of the Securities Exchange Act, the SEC has garnered additional authority over securities markets from statutes such as the Trust Indenture Act,[160] the Investment Company Act,[161] the Investment Advisers Act,[162] the Sarbanes-Oxley Act,[163] and DFA.[164] This collection of laws is "broadly aimed at (1) protecting investors; (2) maintaining fair, orderly, and efficient markets; and (3) facilitating capital formation."[165]

The SEC has broad jurisdiction over participants in the securities markets, including issuers of securities; investment advisers and investment companies; intermediaries like broker-dealers and securities underwriters; and providers of important information products, such as credit

155 12 U.S.C. § 3308.

156 12 U.S.C. § 3311(a). The FFIEC also has limited additional statutory responsibilities related to data disclosed under the Home Mortgage Disclosure Act of 1975. 12 U.S.C. § 2803(f), (k), (l); 12 U.S.C. § 2809(a).

157 15 U.S.C. § 78a.

158 *See* 15 U.S.C. § 78d *et seq.*

159 *See* 15 U.S.C. § 78o-3; FINRA, 2018 ANNUAL FINANCIAL REPORT 4 (2018).

160 15 U.S.C. § 77aaa *et seq.*

161 15 U.S.C. § 80a-1 *et seq.*

162 15 U.S.C. § 80b-1 *et seq.*

163 15 U.S.C. § 7201 *et seq.*

164 12 U.S.C. § 5301 *et seq.*

165 CONG. RESEARCH SERV., IF10032, INTRODUCTION TO FINANCIAL SERVICES: THE SECURITIES AND EXCHANGE COMMISSION (SEC) 1 (2020), https://fas.org/sgp/crs/misc/IF10032.pdf.

rating agencies and research analysts.[166] In addition, the SEC's jurisdiction includes stock exchanges and market utilities, securities-based swaps and related entities, as well as certain other securities products themselves.[167] The SEC does not, however, have jurisdiction over commodities-based swaps and related entities, which remain under the oversight of the CFTC.[168] Foreign exchange markets, the primary market for Treasury securities, issuers of municipal securities, and private securities are exempt from SEC jurisdiction.[169]

b. Commodity Futures Trading Commission

The Commodity Futures Trading Commission (CFTC) is an independent agency established by the Commodity Future Trading Commission Act of 1974 to administer and enforce the Commodity Exchange Act.[170] In connection with this role, the CFTC "has exclusive jurisdiction over futures, commodity options, and leverage contracts, with certain exceptions" as well as "certain swap contracts and broad-based security index products."[171] As such, the CFTC oversees commodities-based swaps and related entities, such as swap dealers, major swap participants, swap clearing organizations, swap execution facilities, and swap data repositories.[172] The CFTC does not, however, have jurisdiction over securities-based swaps and related entities, which remain under the oversight of the SEC.[173] In addition, the CFTC has taken the position that digital currencies are "commodities," bringing under its jurisdiction certain activities related to digital currencies.[174]

4. State Regulators

State financial regulatory agencies and state attorneys general play an important role in administering state consumer and small business protection laws and, in some cases, enforcing federal laws. States impact the federal regulation of financial services in various ways, including, among other functions, chartering, licensing, supervising, and enforcing. For example, states

166 CONG. RESEARCH SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 18–19 (2020).

167 CONG. RESEARCH SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 17 (2020).

168 *See* 15 U.S.C. §§ 8301–8325. The CFTC must consult with the SEC before commencing any such rulemaking or issuing any order related to commodities-based swaps. 15 U.S.C. § 8302(a).

169 15 U.S.C. §§ 77d, 78o, 78o-4(d), 78o-5.

170 7 U.S.C. § 1 *et seq.*

171 COMMODITIES FUTURE TRADING COMM'N, DIVISION OF ENFORCEMENT–ENFORCEMENT MANUAL (2020), https://www.cftc.gov/media/1966/The%2520CFTC%2520Division%2520of%2520Enforcement%2520-%2520Enforcement%2520Manual/download; *see also* 7 U.S.C. §§ 2, 6.

172 CONG. RESEARCH SERV., R44918, WHO REGULATES WHOM? AN OVERVIEW OF THE U.S. FINANCIAL REGULATORY FRAMEWORK 19–20 (2020).

173 *See* 15 U.S.C. §§ 8341–8344. The CFTC must consult with the SEC before commencing any such rulemaking or issuing any order related to commodities-based swaps. 15 U.S.C. § 8302(a).

174 *See, e.g.*, Coinflip, Inc. d/b/a Derivabit, CFTC No. 15-20 (Sept. 17, 2015); *Commodity Futures Trading Comm'n v. McDonnell*, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018); *Commodity Futures Trading Comm'n v. My Big Coin Pay, Inc. et al.*, 334 F. Supp. 3d 492 (D. Mass. 2018).

are the primary regulator for the insurance industry, have chartering and oversight authority over state banks, and have licensing authority over a wide variety of nondepository financial services companies, such as nondepository lenders, money transmitters, debt settlement and collection companies, and loan brokers, among others.

Some states have also implemented data privacy and security laws and regulations that impact financial data. While pre-emption may prevent application of these laws to some financial services providers and/or some activities, state laws can in some circumstances apply to data not otherwise covered by federal statutes and can also impose more stringent and specific data security requirements on certain financial services companies operating in those states.[175] Additionally, all 50 states and the District of Columbia have passed consumer protection laws prohibiting "unfair or deceptive acts or practices" that correspond to the federal UDA(A)P protections.

In addition to implementing their own regulatory regimes that impact financial data, states have the authority, in some instances, to enforce federal statutes related to financial institutions and financial data matters. For example, states have the authority to bring claims under DFA for "unfair, deceptive, or abusive acts or practices."[176] State attorneys general can sue to enforce a number of federal statutes impacting financial data, including FCRA,[177] COPPA,[178] and CROA.[179]

II. Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act

A. Introduction

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("DFA") was enacted after the 2008 financial crisis with the purpose of "promot[ing] the financial stability of the United

175 *See, e.g.*, California Consumer Privacy Act, CAL. CIV. CODE § 1798.100 *et seq.*; Vermont data broker registry law, VT. STAT. ANN. tit. 9 § 2430 *et seq.*; and Nevada privacy law, NEV. REV. STAT. § 603a *et seq.*

176 See Section VII.D.4. for further discussion of state UDA(A)P authority.

177 15 U.S.C. § 1681s(c) (permitting state enforcement of FCRA).

178 15 U.S.C. § 6504 (permitting state enforcement of COPPA, which regulates personal data of minors potentially including financial data).

179 15 U.S.C. § 1679h(c)(1)–(4) (permitting state enforcement of CROA).

States by improving accountability and transparency in the financial system."[180] DFA implemented widespread changes to the regulation of financial services in the United States, including the creation of the CFPB[181] and the amendment of the supervisory, rulemaking, and enforcement authority for certain federal statutes pertaining to financial data.[182]

In addition, Section 1033 of DFA provides that, subject to rules prescribed by the CFPB, covered persons offering or providing consumer financial products or services and their affiliated service providers must make available to consumers in electronic form upon request certain consumer financial information in their control or possession.[183] The CFPB issued a request for information in 2016,[184] outlined a set of principles for data sharing[185] along with a summary of related stakeholder insights in 2017,[186] and held a symposium on consumer data access in 2020.[187] However, while the CFPB announced[188] plans to issue an Advanced Notice of Proposed Rulemaking in July 2020, as of the date of this paper, the CFPB has not yet issued implementing rules for Section 1033 as required by the terms of the statute.[189] As a result of this lack of formal guidance from the CFPB, the precise scope and current effect of Section 1033 remain uncertain.

Various stakeholders in the financial data ecosystem—e.g., depository institutions, data aggregators, financial technology companies—have expressed different and competing interpretations of their respective rights and obligations under the statute. For example, there remains a lack of consensus regarding what information is subject to the statute's obligations, whether consumers must request such access directly or whether they can authorize third parties to obtain it on their behalf, and what limits covered persons may place on access to this

180 Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*).

181 12 U.S.C. § 5301 *et seq.*

182 Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*).

183 *See* 12 U.S.C. § 5533. As discussed below, the statute specifically requires covered persons to provide to consumers "information relating to any transaction, series of transactions, or to the account including costs, charges and usage data." *Id.*

184 81 Fed. Reg. 83806 (Nov. 22, 2016) (Request for Information Regarding Consumer Access to Financial Records).

185 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

186 CONSUMER FIN. PROT. BUREAU, CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION: STAKEHOLDER INSIGHTS THAT INFORM THE CONSUMER PROTECTION PRINCIPLES (2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

187 Consumer Fin. Prot. Bureau, CFPB Symposium: Consumer Access to Financial Records (Feb. 26, 2020) https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/.

188 Press Release, Consumer Fin. Prot. Bureau, CFPB Announces Plan to Issue ANPR on Consumer-Authorized Access to Financial Data (July 24, 2020), https://www.consumerfinance.gov/about-us/newsroom/cfpb-anpr-consumer-authorized-access-financial-data/.

189 *See* 12 U.S.C. § 5533(a), (d).

information, including whether they can impose information security standards on third-party recipients or mandate that they use particular forms of permissioned electronic access. The combination of a broad pronouncement of consumer data access with a lack of implementing guidance makes Section 1033 one of the most important and contested areas of federal law relating to financial data.

B. Entities Covered

The information-sharing requirements in Section 1033 apply to all "covered persons."[190] A "covered person" is defined as "any person that engages in offering or providing a consumer financial product or service" and any affiliated service provider to such person.[191] The scope of "consumer financial products or services" is broad, and applies to a wide range of financial activities, such as extending credit, servicing loans, deposit-taking activities, funds transmission, and collecting debts that stem from loans or other consumer financial products and services, among others.[192] Although wide-reaching, the requirements of Section 1033 do not apply to certain other kinds of consumer financial transactions, such as insurance and securities products.[193]

C. Data Covered

1. Covered Information

Section 1033 provides that consumers[194] may request from covered persons "information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person."[195] With respect to the scope of covered information, the statute expressly covers "information relating to any transaction, series

190 12 U.S.C. § 5533(a).

191 12 U.S.C. § 5481(6).

192 *See* 12 U.S.C. § 5481(5), (15).

193 *See* 12 U.S.C. §§ 5481(15)(C), 5517, 5519; *see also* U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 31 (2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf. The lack of data sharing requirements for insurance and securities products hinders the ability of personal financial management services applications to present consumers with a complete picture of their financial holdings. The Treasury Department has encouraged institutions within the insurance and securities markets to facilitate such consumer data access even in the absence of a legal obligation as these institutions "play important roles in the retirement savings plans of many Americans." *Id.* at 31–32.

194 DFA defines a "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." 12 U.S.C. § 5481(4). See the Commentary Boxes in Section II.E. for further treatment of the implications of this definition to Section 1033's data access right.

195 12 U.S.C. § 5533(a).

of transactions, or to the account including costs, charges and usage data."[196] The CFPB also mentions the following examples in its Data Principles: "any transaction, series of transactions, or other aspect of consumer usage; the terms of any account, such as a fee schedule; realized consumer costs, such as fees or interest paid; and realized consumer benefits, such as interest earned or rewards."[197] Section 1033 expressly states that it does not impose on covered persons any affirmative obligation to maintain or keep any information about consumers.[198]

Commentary Box 1: Information Subject to Section 1033 Access Requirements

In the absence of formal guidance from the CFPB, there remains a lack of certainty as to what kinds of information are subject to the Section 1033 access requirements. In particular, there is a lack of consensus around whether consumers should be able to access all data about them in the possession of the covered person except any data specifically excluded by statute or rule as discussed further below,[199] or whether access should be limited to specifically enumerated data types, to certain time periods, to certain means of accessing the information, or otherwise to the discretion of the data holder.[200] The written submissions and discussions in connection with the recent CFPB Data Symposium demonstrate the still-unsettled nature of this debate.[201]

The technological means for accessing consumer-permissioned data also impact this debate: Screen-scraping technology permits third-party financial services to access all data available directly to the consumer, while API access may allow data holders to control or restrict the information available to consumer-permissioned

196 12 U.S.C. § 5533(a).

197 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 3 (2017).

198 12 U.S.C. § 5533(c).

199 Section 1033(b) provides a list of four statutory exceptions to the data access right. 12 U.S.C. § 5533(b). For further discussion of these exceptions, please see "Enumerated Exceptions" *infra*.

200 *Compare, e.g.*, Jim Reuter, FirstBank, Submission to the CFPB Data Symposium (2020), at 4–5 (advocating for a model contract that dictates terms on which third-party agents could access consumer financial data from covered persons), https://files.consumerfinance.gov/f/documents/cfpb_reuter-statement_symposium-consumer-access-financial-records.pdf, *with* Jane Barratt, MX, Submission to the CFPB Data Symposium (2020), at 1, https://files.consumerfinance.gov/f/documents/cfpb_barratt-statement_symposium-consumer-access-financial-records.pdf ("Should data be limited, and access denied to data fields that were previously available via scraping - the impact to the consumer will be substantial.").

201 *See generally* Submissions to the CFPB Symposium: Consumer Access to Financial Records (Feb. 26, 2020).

third parties. In practice, many financial institutions do impose temporal limitations on the amount of consumer transactional information they will provide in electronic form, commonly limiting access to transactions that have occurred in the prior year.[202] In addition, some covered persons limit electronic access to certain data fields or categories of information that they maintain related to consumer transactions.[203] Some data aggregators and account data users have raised "concerns that account data holders may restrict or control, in an unreasonable and anti-competitive manner, the type of data that they permit consumers to authorize third parties to access."[204]

2. Enumerated Exceptions

Section 1033 sets forth four express exceptions to consumer data access obligations:

- Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
- Any information required to be kept confidential by any other provision of law;
- Any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct; and

202 *See* Stephen Pedneault, *Need access to historical banking information? Better read the fine print*…, FRAUD MAGAZINE, (Sept. 2014), https://www.fraud-magazine.com/article.aspx?id=4294985046 ("Most financial institutions maintain online access for statements and activity for up to one year.").

203 Jason Gross, Petal, Submission to the CFPB Data Symposium (2020), at 3, https://files.consumerfinance.gov/f/documents/cfpb_gross-statement_symposium-consumer-access-financial-records.pdf ("For this to work successfully, the data must be available at the time of the automated cash flow underwriting process and must be complete, without suppressed data fields or categories of information."); Jane Barratt, MX, Submission to the CFPB Data Symposium (2020), at 2 ("Guidance and rulemaking around what data elements should be accessible is required as the current industry API standard is discretionary as to what data elements a financial institution needs to include in their API.").

204 CONSUMER FIN. PROT. BUREAU, CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION: STAKEHOLDER INSIGHTS THAT INFORM THE CONSUMER PROTECTION PRINCIPLES 3 (2017); *see also* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 51 (2020) https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf ("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.").

- Any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.[205]

Commentary Box 2: Scope of Enumerated Exceptions

Without formal guidance, the scope of these exceptions is uncertain. For example, Section 1033 does not define what information beyond proprietary algorithms constitutes "confidential commercial information." Market participants have claimed that data holders in some cases have suppressed certain data fields or categories of information from the access they provide to consumer-permissioned agents on the basis that the information is confidential or present too significant a liability risk to release.[206] Such claims have included allegations of withholding deposit accounts and routing numbers, which makes it more difficult for consumers to access third-party payment services, even though such information is printed on the bottom of checks.[207]

3. Data Format

Section 1033 requires that covered information "be made available in an electronic form usable by consumers."[208] The statute mandates that the CFPB, by rule, "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."[209] However, the statute directs

205 12 U.S.C. § 5533(b)(1)–(4). In addition to the explicit statutory exclusions, the U.S. Court of Appeals for the Second Circuit has found covered persons are not required to produce "original note[s]" to consumers. *Hariprasad v. Master Holdings Inc.*, 788 F. App'x 783, 787 (2d Cir. 2019).

206 *See* Jason Gross, Petal, Submission to the CFPB Data Symposium (2020), at 2 ("Cash flow underwriting relies on the ability of financial applications like Petal to safely, securely, and reliably access and port, with affirmative consumer authorization, any element of consumers' financial data held by their financial institutions. For this to work successfully, the data must be available at the time of the automated cash flow underwriting process and must be complete, without suppressed data fields or categories of information.").

207 *See* John Pitts, Plaid, Submission to the CFPB Data Symposium (2020), at 5, https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf (arguing for the CFPB to define the minimum scope of financial account information available to consumers and stating that such scope should mandate the inclusion of account and routing numbers); FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 51 *FN* 111, 54 *FN* 121 (2020) ("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.").

208 12 U.S.C. § 5533(a).

209 12 U.S.C. § 5533(d).

the CFPB to consult with other regulators "to ensure, to the extent appropriate, that the rules . . . do not require or promote the use of any particular technology in order to develop systems for compliance." [210]

D. Oversight

Section 1033 assigns rulemaking authority to the CFPB, while mandating that it consult with various other federal regulators.[211] Supervisory and enforcement jurisdiction for Section 1033 is consistent with the general consumer protection authority over covered persons under DFA.[212] Section 1033 provides that the consumer data access rights are "subject to rules prescribed by the [CFPB]," and the CFPB is further required 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, to be made available to consumers under this section."[213] In promulgating rules pursuant to Section 1033, the CFPB is required to consult with the federal banking agencies and the FTC to ensure, to the extent appropriate, that the rules:

- Impose substantively similar requirements on covered persons;
- Take into account conditions under which covered persons do business both in the U.S. and in other countries; and
- Do not require or promote the use of any particular technology in order to develop systems for compliance.[214]

As of September 2020, the CFPB has not yet issued regulations implementing Section 1033. As discussed further below in the Commentary Boxes in Section II.E., there is disagreement regarding whether Section 1033 is self-executing and, therefore, whether covered persons are currently bound by the general obligations set forth in the statute. To date, there has been limited litigation defining the scope of the rights created under Section 1033.[215] The CFPB

210 12 U.S.C. § 5533(e)(3).

211 *See* 12 U.S.C. § 5533(e).

212 See Section I.C. for more information on the supervisory and enforcement powers of the various federal regulators.

213 12 U.S.C. § 5533(a), (d).

214 12 U.S.C. § 5533(e).

215 One court has found that Section 1033 does not create a private right of action to permit consumers to sue for damages when a financial institution withholds information. *Gingras v. Rosette*, No. 5:15-CV-101, 2016 WL 2932163, (D. Vt. May 18, 2016), *aff'd sub nom. Gingras v. Think Fin., Inc.*, 922 F.3d 112 (2d Cir. 2019). Instead, the court opined that the "obvious intent of the provision is to prompt the adoption of a detailed regulatory system for placing information about a financial transaction in the hands of the consumer." *Id.* at 22.

maintains civil penalty authority for noncompliance with Section 1033 by covered persons subject to its enforcement jurisdiction, with penalties ranging from $1,000 to $1,000,000 per day the violation continues, depending upon the tier of the violation.[216] Prudential regulators are authorized to examine and enforce Section 1033 with respect to depository institutions with assets under $10 billion, and state attorneys general may bring civil actions against all entities under their jurisdiction.[217]

As discussed above, in November 2016, the CFPB issued the Data RFI.[218] In October 2017, the CFPB issued the Data Principles, along with a synopsis of stakeholder insights that informed those Data Principles.[219] The Data Principles express the CFPB's "vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[220] The CFPB clarified, however, that the principles do not "themselves establish binding requirements or obligations relevant to the [CFPB]'s exercise of its rulemaking, supervisory, or enforcement authority" and "are not intended as a statement of the [CFPB]'s future enforcement or supervisory priorities."[221] In addition, the CFPB stated that "many consumer protections apply to this market under existing statutes and regulations" and that the principles "may accord with . . . the scope of those existing protections," though they were not intended to "alter, interpret, or otherwise provide guidance" on them.[222]

In February 2020, the CFPB convened a symposium on "Consumer Access to Financial Records."[223] The symposium featured remarks from CFPB Director Kathleen Kraninger and consisted of three panels of experts, addressing: (i) the current landscape of holders of consumer data and the benefits and risks of consumer-authorized data access; (ii) market developments in consumer-authorized data access; and (iii) the future state of the market, as well as considerations for policymakers on how to ensure consumer data is safeguarded while ensuring that consumers have continual access to their data.[224] In July 2020, the CFPB

---

216 *See* 12 U.S.C. § 5565(c). Penalties for recklessly or knowingly continuing to violate Section 1033 impose higher penalties.

217 *See* 12 U.S.C. §§ 5581(c)(1), 5516, 5552.

218 81 Fed. Reg. 83806 (Nov. 22, 2016) (Request for Information Regarding Consumer Access to Financial Records).

219 *See* CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (2017); CONSUMER FIN. PROT. BUREAU, CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION: STAKEHOLDER INSIGHTS THAT INFORM THE CONSUMER PROTECTION PRINCIPLES (2017).

220 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 1 (2017). The Data Principles cover the following topics: (1) access; (2) data scope and usability; (3) control and informed consent; (4) authorizing payments; (5) security; (6) access transparency; (7) accuracy; (8) ability to dispute and resolve unauthorized access; and (9) efficient and effective accountability mechanisms.

221 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 1 (2017).

222 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 1 (2017).

223 *See* Consumer Fin. Prot. Bureau, CFPB Symposium: Consumer Access to Financial Records (Feb. 26, 2020).

224 *See* Consumer Fin. Prot. Bureau, CFPB Symposium: Consumer Access to Financial Records (Feb. 26, 2020).

announced plans to issue an Advanced Notice of Proposed Rulemaking, along with a summary of the symposium earlier in February 2020.[225]

E. Substantive Requirements

As described above, subject to certain enumerated exceptions and to CFPB rulemaking, Section 1033 requires covered persons under CFPB jurisdiction to make available consumer financial information in their possession upon request by a consumer.[226] To date, the CFPB has not issued rules interpreting Section 1033, leaving certain important questions as to the scope and effectiveness of the statute unanswered. Set forth below is a summary of the most significant areas of ambiguity and lack of stakeholder consensus.

Commentary Box 3: Self-Executing Nature of Section 1033

Some statutes are self-executing, which means that they set forth legal rights and obligations that govern as of the statute's effective date with no further action; others are not, and thus require rulemaking by an administrative agency or other official action to give effect to such rights and obligations.[227] DFA presents a mixed model, with some portions announcing clear and immediately applicable standards and other provisions requiring agency rulemaking to take effect.[228]

Section 1033 provides an express obligation on the part of covered persons to provide consumer financial information upon request.[229] That suggests Section 1033

225 Press Release, Consumer Fin. Prot. Bureau, CFPB Announces Plan to Issue ANPR on Consumer-Authorized Access to Financial Data (July 24, 2020); CONSUMER FIN. PROT. BUREAU, BUREAU SYMPOSIUM: CONSUMER ACCESS TO FINANCIAL RECORDS—SUMMARY OF THE PROCEEDINGS (2020), https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

226 *See* 12 U.S.C. § 5533.

227 *See* Adam M. Samaha, *Self-Executing Statutes in the Administrative State*, NYU SCH. OF LAW, Public Law & Legal Theory Research Paper Series, Working Paper No. 15-62 (Jan. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2720309.

228 Adam M. Samaha, *Self-Executing Statutes in the Administrative State*, NYU SCH. OF LAW, Public Law & Legal Theory Research Paper Series, Working Paper No. 15-62 (Jan. 2016), at 8 ("A more recent mixed-model example" is DFA. The statute requires residential mortgage lenders to make "a reasonable and good faith determination . . . that . . . the consumer has a reasonable ability to repay the loan," yet also authorizes the CFPB to "prescribe regulations that revise, add to, or subtract from the criteria that define a qualified mortgage . . . which a lender may presume is enough to satisfy its duty.").

229 12 U.S.C. § 5533(a).

is self-executing and that consumers have an immediate right to data access even in the absence of CFPB rulemaking on the matter. However, the statute begins by stating that this obligation is "[s]ubject to rules promulgated by the [CFPB]."[230] This language holds the possibility that Section 1033 may not be self-executing and that covered persons are under no present legal obligation to provide data access given the CFPB's lack of rulemaking to date. This ambiguity has led to ongoing debate about consumer data access rights.[231]

Some stakeholders argue that the CFPB has already clarified that the statute is binding in its current form.[232] Others take the position that the self-executing conclusion is supported by the statute's broad legislative intent to enhance consumer access to data.[233] That perspective is bolstered by the legislative history. An April 30, 2010, Senate report states that "this section [1033] ensures that consumers are provided with access to their own financial information."[234] The report does not contemplate that additional steps would be required to secure that access. In addition, although the Data Principles do not constitute binding regulatory guidance, they do suggest that consumers are presently "able, upon request, to obtain information about their ownership or use of a financial product or service from their product or service provider."[235] Other stakeholders, however, argue that the "subject to" condition in the statutory text indicates that the statute is not self-executing and that covered persons are under no legal obligation at present.[236]

---

230 12 U.S.C. § 5533(a).

231 *See, e.g.*, Dan Murphy, Fin. Health Network, Submission to the CFPB Data Symposium (2020), at 4, https://files.consumerfinance.gov/f/documents/cfpb_murphy-statement_symposium-consumer-access-financial-records.pdf ("As the financial data ecosystem has grown, the debate over the meaning of Section 1033 has grown with it. Is Section 1033 self-effectuating, or does consumers' right to access only take effect upon rulemaking by the CFPB?").

232 *See* Michael S. Barr, Abigail DeHart & Andrew Kang, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, UNIV. OF MICH. CTR. ON FIN., LAW & POL'Y 4 (2019), http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

233 *See, e.g.*, John Pitts, Plaid, Submission to the CFPB Data Symposium (2020), at 4 ("Confirming that Section 1033 is in effect, and creates a consumer right that financial institutions must satisfy, should not be controversial.").

234 S. REP. No. 111-176, at 173 (2010) (emphasis in the original).

235 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 3 (2017).

236 *See, e.g.*, Rob Morgan, Am. Bankers Ass'n, Comment Letter in Response to the CFPB's RFI Regarding Consumer Access to Financial Records (Feb. 21, 2017), at 3, https://www.aba.com/advocacy/policy-analysis/consumer-financial-protection-bureaus-rfi-consumer-access-financial-records (arguing that "[i]f implemented by rules written by the Bureau, §1033 of the Dodd-Frank Act will require a covered person to 'make available to a consumer, upon request, information . . . concerning the consumer financial product or service that the consumer obtained from such covered person . . . .'").

In 2011, the CFPB itself took the position that another data-related provision of DFA was not self-executing because it employs the language, "in accordance with regulations of the [CFPB],"[237] and that financial institutions' obligations under that section "do not arise until the [CFPB] issues implementing regulations and those regulations take effect."[238]

Even if Section 1033 is self-executing, there is a question as to the enforcement of the obligations set forth therein. In the absence of an express private right of action, as is the case with Section 1033, enforcement would fall to the regulatory bodies granted authority under the statute: in this case, the CFPB, the prudential regulators, and the states.

Commentary Box 4: Consumer-Authorized Third-Party Data Access

Section 1033 grants data access rights to "consumers," which is defined by DFA to include both an individual consumer, as well as "an agent, trustee, or representative acting on behalf of an individual."[239] The statute leaves it to the CFPB to determine what entities may qualify as agents or representatives, however.[240] The inclusion of consumer agents and representatives into the definition of "consumer" is supported by the Data Principles[241] and a 2018 U.S. Department of Treasury report that reviewed the regulatory framework for fintech companies and made

237 15 U.S.C. § 1691c-2(e).

238 Consumer Fin. Prot. Bureau, Letter to Chief Executive Officers of Financial Institutions Regarding Section 1071 of the Dodd-Frank Act (Apr. 11, 2011), at 1–2, https://files.consumerfinance.gov/f/2011/04/gc-letter-re-1071.pdf.

239 12 U.S.C. § 5481(4).

240 In the absence of agency action, a court could potentially interpret Section 1033 and issue a holding as to the scope of the agent or representative designation.

241 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 3 (2017), (stating that "[c]onsumers [should be] generally able to authorize trusted third parties to obtain such information from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner.").

recommendations,[242] as well as by former executive branch officials who assisted in drafting the provision.[243] The Treasury Fintech Report urges the CFPB to affirm this understanding, suggesting that the Treasury Department does not view this interpretation as beyond doubt.[244]

Notwithstanding these sources, some commentators have noted that "there is disagreement as to whether the law extends that obligation to customers' agents, such as firms that seek to serve customers by giving them a consolidated picture of their financial lives across all of their accounts, or by possibly allowing customers to transact with multiple financial services firms through a common platform."[245] For example, some have questioned whether Section 1033 applies to data aggregators, with whom consumers may not have a direct relationship, or only the companies that have a relationship with, and data-access authorization from, the consumer.[246]

Commentary Box 5: Conditioning Third-Party Access

Another open question is the extent to which Section 1033 permits the conditioning of third-party access to consumer financial data. Under its rulemaking authority, the

242 U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 31 (2018), (stating that "[t]his definition 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 to access their financial account and transaction data from financial services companies").

243 *See* Michael S. Barr, Abigail DeHart & Andrew Kang, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, UNIV. OF MICH. CTR. ON FIN., LAW & POL'Y 4 (2019) ("As a drafter of the provision that become § 1033, I can state that the scope of the provision was intended to be broad—providing a framework for customer access that would encourage competition and innovation, including through the use of third-party providers and aggregators.").

244 U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 31 (2018).

245 Brian Knight, George Mason Univ. Mercatus Ctr., Submission to the CFPB Data Symposium (2020), at 1–2, https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf ("Because of advances in technology, changing consumer expectations, and legal ambiguity, Section 1033 presents a significant question because it may require banks and other covered financial firms to provide access to records to not only their customers, but to the agents of those customers.").

246 *See* Brian Knight, George Mason Univ. Mercatus Ctr., Submission to the CFPB Data Symposium (2020), at 2 ("Are aggregators (who generally do not have a direct relationship with the consumer) covered by Section 1033, or is it only those firms who have a direct relationship and receive specific authorization from a covered firm's customer?").

CFPB has the ability to define the conditions and activities that give rise to an authorized third-party agent relationship for purposes of Section 1033. In addition, private data holders have argued that they too may condition third-party access to consumer data—a subject on which the text of Section 1033 is silent. Access conditions could conceivably include, among others, the technological capabilities of the third party, the nature and timing of consumer consent, liability-sharing agreements or insurance and indemnification standards, information security standards, or fraud or money laundering considerations.

At the CFPB Data Symposium, some data holders advocated for data holders' ability to restrict data access by consumer-permissioned third parties on the basis of information security and data privacy standards that the covered persons themselves have set (and which they assert are based, at least in part, on data holders' own regulatory obligations to protect consumer data and manage service provider relationships as discussed further below).[247] Data holders expressed concerns about their ability to protect proprietary data, their customers, and their own information security networks, and to prevent fraudulent transactions.[248] Stakeholders from data aggregators and consumer-facing fintech companies—the likely recipients of consumer permission as data access agents—expressed concerns that data holders' unilateral discretion to condition access on standards

247 A significant point of contention is whether covered persons may block credentials-based account access and "screen scraping" technology by consumer-permissioned third parties and instead require them to access consumer financial information through tokenized credentials and API technology. *See, e.g.*, Becky Heironimus, Capital One, Submission to the CFPB Data Symposium (2020), at 5–7, https://files.consumerfinance.gov/f/documents/cfpb_heironimus-statement_symposium-consumer-access-financial-records.pdf ("[W]e urge the CFPB to require aggregators and fintechs seeking consumer-permissioned access to data from financial institutions to use API-based connections when they are available."); *see also* Dan Murphy, Fin. Health Network, Submission to the CFPB Data Symposium (2020), at 3 ("The security challenges brought about by screen scraping are well known, and have recently been cited by the Financial Crimes Enforcement Network (FinCEN) as an emerging source of fraud. Data aggregators largely acknowledge the shortcomings of screen scraping in the long run, but point out that regulatory uncertainty and disagreements with banks over the scope of data access make it difficult to move beyond screen scraping at present.").

248 *See* Meredith Fuchs & Andres L. Navarette, Capital One, Submission to the CFPB Data Symposium (2020), at 5–7; Lila Fakhraie, Wells Fargo, Submission to the CFPB Data Symposium (2020), at 2–3, https://files.consumerfinance.gov/f/documents/cfpb_fakhraie-statement_symposium-consumer-access-financial-records.pdf (noting Wells Fargo's use of bilateral agreements that condition third-party data access on terms related to security, consumer consent, transparency, and liability allocation); Jim Reuter, FirstBank, Submission to the CFPB Data Symposium (2020), at 4–5 (advocating for a model contract that dictates terms on which third-party agents could access consumer financial data from covered persons).

they create may mask anticompetitive motives and undermine Section 1033's fundamental purpose of empowering consumers.[249]

Absent more specific CFPB guidance on this matter, data holders have already started imposing conditions on consumer-permissioned third-party access to financial data in the course of shifting from screen scraping to API transfers. Covered persons have required consumer-permissioned third-party agents to enter into bilateral agreements that mandate certain terms in exchange for data access.[250] For example, in 2019, one large bank instituted heightened security standards that limited access for a consumer-authorized peer-to-peer payments provider and its third-party data aggregator service and suggested its users instead use a competing service owned by banks.[251] In January 2020, another bank announced that it will begin conditioning access to consumer financial data by consumer-permissioned third-party agents on the agents' agreement to use specific and proprietary technology.[252]

249 *See* John Pitts, Plaid, Submission to the CFPB Data Symposium (2020), at 2 ("Financial institutions have announced plans to block data access for any company that will not sign a data access agreement."); Jane Barratt, MX, Submission to the CFPB Data Symposium (2020), at 1 ("Should data be limited, and access denied to data fields that were previously available via scraping - the impact to the consumer will be substantial."); Steven Boms, Fin. Data and Tech. Ass'n of N. Am., Submission to the CFPB Data Symposium (2020), at 3–4, https://files.consumerfinance.gov/f/documents/cfpb_boms-statement_symposium-consumer-access-financial-records.pdf ("But any rational assessment of the ecosystem must also conclude that commercial interests can factor into decisions that financial institutions make with regard to what data to include in their APIs or how onerous the terms of the bilateral agreements they offer to third parties will be.").

250 Steven Boms, Fin. Data and Tech. Ass'n of N. Am., Submission to the CFPB Data Symposium (2020), at 3–4 ("The only tool available to the industry to address data access currently is individual bilateral agreements between financial institutions and aggregators, each with differing requirements on the fintech ecosystem and different provisions to consumers.").

251 *See* Kate Rooney, *PNC's fight with Venmo highlights bigger issue over who owns your banking data*, CNBC (Dec. 16, 2019), https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html; *see also* Thomas Brown, Paul Hastings LLP, Submission to the CFPB Data Symposium (2020), at 6, https://files.consumerfinance.gov/f/documents/cfpb_brown-statement_symposium-consumer-access-financial-records.pdf ("The recent decision by PNC to deny consumer requests to share information with Venmo received considerable attention in the press, but it is not the only instance of a financial institution denying a consumer request to share information. At least one dispute has resulted in a lawsuit by a consumer-facing financial services provider to prevent a third party from making a bill payment on a consumer's behalf."); Dan Murphy, Fin. Health Network, Submission to the CFPB Data Symposium (2020), at 2 ("Persistent disputes between banks and data aggregators have resulted in banks cutting off access altogether in some cases, resulting in service interruptions to consumers using third-party applications.").

252 *See* Penny Crosman, *JPMorgan Chase moves to block fintechs from screen scraping*, AM. BANKER (Jan. 2, 2020), https://www.americanbanker.com/news/jpmorgan-chase-moves-to-block-fintechs-from-screen-scraping.

Commentary Box 6: Disclosure and Consent

Assuming individual consumers may authorize third parties to access their financial data under Section 1033, there is an open question as to the limits of what the CFPB can require with regard to specific types of consumer disclosure and consent, whether data holders can require certain processes in the absence of CFPB action, and what constitutes best practices for disclosure and consent with respect to financial data access by consumers. The Data Principles advise that "[a]uthorized terms of access, storage, use, and disposal [should be] fully and effectively disclosed to the consumer, understood by the consumer, not overly broad, and consistent with the consumer's reasonable expectations in light of the product(s) or service(s) selected by the consumer."[253] These suggestions are principles-based, and do not list any specific information that agents must disclose or any specific form of consent that consumers must provide in order to designate an agent.[254] Some stakeholders have expressed concern, however, that consumers do not understand the terms of the consent that they provide agents.[255] In November 2019, The Clearing House published the results of a survey among fintech application users that found that 80% of respondents were not fully aware that fintech apps or third parties may store their bank account username and password, less than 25% of respondents knew that financial apps often continue to have ongoing access to their data until consumers revoke their bank account credentials, and 26% incorrectly believe that financial apps continue to have access to their data after users revoke their bank account credentials.[256] The Treasury Department has warned that the lack of standards regarding disclosure and consent leaves "consumers unable to clearly understand and weigh the risks and benefits of using

253 CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 3 (2017).

254 *See* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 74 (2020) ("The statute does not provide standards with regard to what type of request or consent is required to trigger data access . . ."). The CFPB has broad-based authority to require disclosures relating to consumer financial products and services under Section 1032 of DFA. 12 U.S.C. § 5532.

255 *See* Chi Chi Wu, Nat'l Consumer Law Ctr., Submission to the CFPB Data Symposium (2020), at 7–8, https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf; Becky Heironimus, Capital One, Submission to the CFPB Data Symposium (2020), at 3–5 ("[C]onsumers continue to lack a sufficient understanding of aggregator and fintech data sharing practices and are not offered a meaningful opportunity to consent or object to the privacy and data sharing practices of these services.").

256 THE CLEARING HOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY 3–6 (Nov. 2019), https://www.theclearinghouse.org/payment-systems/articles/2019/11/-/media/ec23413b9f98467ea7bdf55e93854278.ashx.

fintech applications and letting third parties access and use their personal and financial data."[257]

Additional questions concern processes for revocation of consent and the ability of consumers to direct that financial services providers or other previous data recipients delete their information. These topics are not expressly addressed in Section 1033 and have not been a primary focus of earlier federal consumer financial protection laws, though revocation is briefly mentioned in GLBA's privacy regulations.[258] Other data protection regimes, such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act, address these issues in greater detail, including a "right to be forgotten" in certain circumstances.[259]

257 U.S. DEP'T OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION 32 (2018); *see also* Lael Brainard, Governor of the Fed. Reserve Bd., Speech at the Univ. of Mich., *Where Do Consumers Fit in the Fintech Stack?* (Nov. 16, 2017), https://www.federalreserve.gov/newsevents/speech/brainard20171116a.pdf ("It is often hard for the consumer to know what is actually happening under the hood of the financial app they are accessing. In most cases, the log in process does not do much to educate the consumer on the precise nature of the data relationship . . . In reviewing many apps, it appears that the name of the data aggregator is frequently not disclosed in the fintech app's terms and conditions, and a consumer generally would not easily see what data is held by a data aggregator or how it is used. The apps, websites, and terms and conditions of fintech advisors and data aggregators often do not explain how frequently data aggregators will access a consumer's data or how long they will store that data.").

258 Specifically, 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." 12 C.F.R. § 1016.15(a)(1). The Fair Credit Reporting Act requires consumer consent to sharing consumer reports for certain employment-related activities, but informal guidance from FTC staff does not appear to contemplate that consent could subsequently be revoked. FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 51 (2011), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf ("A valid disclosure and consent remain effective throughout the duration of employment."). FCRA regulations address information security requirements when disposing of consumer report information, but those do not address whether and when consumers can direct that their information be deleted. 15 U.S.C. § 1681w; 16 U.S.C. pt. 682 (Federal Trade Commission version).

259 California Consumer Privacy Act, Cal. Civ. Code § 1798.105; *see also* CONG. RESEARCH SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 38–39, 45–46 (2019), https://crsreports.congress.gov/product/pdf/R/R45631.

Commentary Box 7: Liability and Data Accuracy

Section 1033 is silent as to how consumer-authorized financial access intersects with other existing statutes and regulations that relate to financial data and more broadly as to how liability and responsibilities for data accuracy, data security, and account security should be allocated among the various stakeholders in the market. In addition, current statutory regimes that focus specifically on data accuracy (FCRA), unauthorized transactions (EFTA), and data privacy/security (GLBA) do not necessarily have the same scope of coverage as 1033 and were not written in contemplation of the breadth of consumer data sharing that could occur under Section 1033 or the modern financial ecosystem more generally. Thus, there are a number of questions under multiple federal consumer financial laws about accuracy and liability issues in connection with financial data sharing, particularly when data is shared between entities at the direction of a consumer.

For example, some commentators have raised questions regarding whether FCRA applies to financial data shared pursuant to Section 1033 and which entities, if any, involved in such sharing are subject to FCRA accuracy requirements as "furnishers" or "consumer reporting agencies."[260] Further, in instances in which a financial institution does transmit inaccurate consumer financial information, it is often unclear as to whether federal law provides consumers with correction rights and other protections.

Data sharing increasingly underpins the entire fintech industry. As the volume of data sharing continues to grow and companies become increasingly dependent on consumer data access, the risks to consumers and market participants may also

260 *See* Dan Murphy, Financial Health Network, Submission to the CFPB Data Symposium (2020), at 4; Chi Chi Wu, Nat'l Consumer Law Ctr., Submission to the CFPB Data Symposium (2020), at 6–9; FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 74 (2020) ("The statute does not provide standards with regard to . . . processes for correcting any errors in the data that is obtained."), https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf; Sam Adriance, *The Future of Interconnected Banking is Now, and It's Brought to You by APIs*, AM. BAR ASS'N CONSUMER FIN. SERVS. COMMITTEE NEWSLETTER (Dec. 5, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/consumer/2019/201911/banking/. See Section IV.B.2. for more detailed information on "furnishers" under FCRA.

grow to the extent that the application of existing laws and regulations to data sharing remain unclear and important implications are left unaddressed.[261]

III. Gramm-Leach-Bliley Act (GLBA)

A. Introduction

The Gramm-Leach-Bliley Act ("GLBA")[262] was signed into law in 1999. The purpose of GLBA was to "enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers."[263] In so doing, GLBA repealed the provisions of the Glass-Steagall Act[264] restricting the commingling of commercial banking, investment banking, and insurance activities within or among affiliated financial institutions.[265]

In the decade leading up to GLBA's passage, the public was growing concerned about financial data privacy—a concern that was thought to be exacerbated by data sharing among financial institutions with the removal of Glass-Steagall provisions. In response to these anxieties, Congress included in GLBA new obligations pertaining to the privacy and security of consumer data in the possession of financial institutions.[266] Congress authored GLBA to require institutions to safeguard data, establish privacy policies, disclose these policies to customers, and prohibit

261 *See* Melissa Koide & Kelly Cochran, FinRegLab, Submission to the CFPB Data Symposium (2020), at 2, https://files.consumerfinance.gov/f/documents/cfpb_cochran-statement_symposium-consumer-access-financial-records.pdf ("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.").

262 Pub. L. No. 106-102, 113 Stat. 1338 (1999).

263 Pub. L. No. 106-102, 113 Stat. 1338 (1999).

264 Banking Act of 1933 (Glass-Steagall), Pub. L. No. 73-66, 48 Stat. 162, 184–85 (codified as amended at 12 U.S.C. § 227).

265 Pub. L. No. 106-102, 113 Stat. 1338 (1999).

266 Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 500–04 (2002), https://lawcat.berkeley.edu/record/1118180?ln=en; *see also Financial Privacy And Consumer Protection: Oversight Hearing on the Gramm-Leach-Bliley Act Before the S. Comm. of Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group) https://privacyrights.org/resources/oversight-hearing-financial-privacy-and-gramm-leach-bliley-financial-services.

the disclosure of certain customer information to non-affiliated third parties except under certain circumstances.[267]

Although legislators appeared in general agreement on the need to protect private financial information, they met the GLBA privacy provisions with varying degrees of support and skepticism.[268] Some legislators claimed that these provisions would "provide the strongest privacy protection ever for Americans."[269] Others were more skeptical, citing the "explosive growth of the Internet" and resultant ease of collecting and sharing information, insufficiency of disclosure requirements and opt-out provisions, absence of rules governing the sharing of information amongst affiliates, and exceptions to providing information to non-affiliated third-parties as evidence that GLBA fell short of providing adequate consumer protection.[270]

The two substantive areas of GLBA addressing financial data have become known as the Privacy Rule[271] and the Safeguards Rule.[272] The applicable subchapter of GLBA opens with a broad statement that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[273]

The Privacy Rule, Safeguards Rule, and their implementing regulations, as amended over the years since their passage, represent the current interpretation and application of that policy to the day-to-day practices of financial institutions. The term "financial institution" under GLBA is defined more broadly than in normal parlance; exactly which entities qualify depends on an often-complex analysis of the types of activities in which they engage and, in some cases, the frequency with which they engage in them.[274] As a result, there may be uncertainty as to which

---

267 Prior to GLBA's enactment, NationsBank (now Bank of America) was fined $7 million in penalties for sharing its customers financial information to an affiliated securities firm which led to customers with conservative holdings being moved to riskier products and losing large portions of their savings. Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 503–04 (2002).

268 *See generally* 145 CONG. REC. S13783-01 (daily ed. Nov. 3, 1999); 145 CONG. REC. S13871-07 (daily ed. Nov. 4, 1999); 145 CONG. REC. S13883-01 (daily ed. Nov. 4, 1999); 145 CONG. REC. H11513-08 (daily ed. Nov 4, 1999); 145 CONG. REC. E2302-01 (daily ed. Nov. 8, 1999) (statement of Rep. Dingell); 145 CONG. REC. E2302-02 (daily ed. Nov. 8, 1999) (statement of Rep. Kilpatrick); 145 CONG. REC. E2291-04 (daily ed. Nov. 5, 1999) (statement of Rep. Stark); 145 CONG. REC. S14533-02 (daily ed. Nov. 10, 1999) (statement of Sen. Shelby).

269 145 CONG. REC. S13871-07 (daily ed. Nov. 4, 1999) (statement of Sen. Enzi).

270 145 CONG. REC. S13871-07 (daily ed. Nov. 4, 1999) (statement of Sen. Johnson); 145 CONG. REC. E2291-04 (daily ed. Nov. 5, 1999) (statement of Rep. Stark); 145 CONG. REC. E2296-02 (daily ed. Nov. 8, 1999) (statement of Rep. Stark).

271 15 U.S.C. §§ 6801–6809 ("Privacy Rule"). The implementing regulations for the Privacy Rule are contained in the CFPB's Regulation P (12 C.F.R. Part 1016) and the FTC's regulations at 16 C.F.R. Part 313. Given Regulation P's broader scope of applicability than the FTC's implementing regulation, this paper will primarily reference Regulation P except where discussing differences between the CFPB's and FTC's regulations.

272 15 U.S.C. §§ 6801(b), 6805(b)(2) ("Safeguards Rule"). The implementing regulations for the Safeguards Rule are contained in the FTC's regulations at 16 C.F.R. Part 314. As discussed below in Section III.C.3., the prudential banking regulators, SEC, and CFTC have also issued their own guidelines for compliance with the Safeguards Rule.

273 15 U.S.C. § 6801(a).

274 15 U.S.C. § 6809(3).

entities are subject to GLBA's information sharing and data security requirements, especially as companies that focus primarily on general commercial activities start offering financial products and services to their customers.

The Privacy Rule regulates the circumstances under which financial institutions are permitted to disclose consumer nonpublic personal information ("NPI") and related notice requirements. The Safeguards Rule requires financial institutions to take steps to protect the confidentiality and security of customer information from unauthorized access. As discussed below, the two rules differ in important ways with respect to regulatory jurisdiction, the types of data covered, and the entities subject to oversight.

B. Privacy Rule

The Privacy Rule, comprised of the applicable portions of GLBA along with the implementing regulations, sets forth federal law governing the privacy of financial data. In particular, the Privacy Rule prohibits financial institutions from sharing consumers' NPI with non-affiliated entities, subject to certain exceptions. It also provides guidance on the required privacy policies and notices for consumers and customers of financial institutions. As discussed further below, companies must carefully consider whether the activities in which they engage subject them to GLBA's Privacy Rule.

1. Entities Covered

The Privacy Rule applies to financial institutions, affiliates of financial institutions, and non-affiliated third parties that receive nonpublic personal information from a financial institution or its affiliate, although the specific applicable requirements vary in some cases by entity type. For example, financial institutions with a customer relationship receiving NPI directly from a consumer may have different requirements under the Privacy Rule than non-affiliated third parties receiving that same NPI from a financial institution.

a. Financial Institutions and Affiliates

GLBA applies to any entity that is a "financial institution" and to any entity that is an "affiliate" of a financial institution.[275] GLBA defines a "financial institution" as any "institution the business of

275 "Affiliate" means "any company that controls, is controlled by, or is under common control with another company." 15 U.S.C. § 6809(6); 12 C.F.R. § 1016.3(a); 16 C.F.R. § 313(a). "Control" is defined in the implementing regulations. *See* 12 C.F.R. § 1016.3(g).

which is engaging in financial activities" as described in section 4(k) of the Bank Holding Company Act ("BHCA").[276]

Section 4(k) of BHCA sets forth the types of activities that a "financial holding company" may engage in, which under the statute include those that are "financial in nature or incidental to such financial activity" or "complementary to a financial activity."[277] Permitted activities under Section 4(k) include those specifically enumerated in BHCA;[278] activities that the FRB has determined by regulation[279] and order[280] to be "closely related to banking"; activities determined by the FRB "to be usual in connection with the transaction of banking abroad";[281] and activities determined by the FRB to be "financial in nature or incidental to financial activities."[282]

The prudential bank regulators and the FTC historically interpreted the statutory language of GLBA differently in their implementing regulations. Prudential regulators defined "financial institution" broadly to include any entity conducting activities that are "financial in nature or incidental thereto."[283] The FTC, on the other hand, included in the definition of "financial institutions" only entities that are "significantly engaged" in financial activities and excluded those companies conducting activities merely incidental to financial activities.[284] The FTC's rule also limited the definition of "financial institution" to entities engaged in those activities determined by the FRB as of the effective date of the rule to be financial in nature, excluding any activities determined by the FRB to be financial activities or incidental activities after the date thereof.[285] When the CFPB assumed rulemaking authority for the Privacy Rule, the CFPB incorporated both definitions into Regulation P.[286]

In April 2019, the FTC issued a proposed rule that would expand the definition of "financial institution" primarily for purposes of the Safeguards Rule, but also for the Privacy Rule to the extent that certain entities are not subject to CFPB jurisdiction. Specifically, the proposed

276 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k).

277 12 U.S.C. § 1843(k)(1).

278 12 U.S.C. § 1843(k)(4).

279 12 C.F.R. § 225.28.

280 12 C.F.R. § 225.86(a)(2).

281 12 C.F.R. § 225.86(b).

282 12 C.F.R. § 225.86(d).

283 *See* FED. RESERVE BD., SMALL ENTITY COMPLIANCE GUIDE, REGULATION P: PRIVACY OF CONSUMER FINANCIAL INFORMATION 2 (2002), https://www.federalreserve.gov/regulations/cg/reg_p_cg.pdf.

284 16 C.F.R. § 313.3(k)(1).

285 65 Fed. Reg. 33646, 33654 n.23 (May 24, 2000) (codified at 16 C.F.R. Part 313) ("Section 4(k) of the Bank Holding Company Act established procedures whereby the Board can add activities to the list of activities that it is permissible for financial holding companies to engage in. To the extent these later added activities are financial activities, and not incidental activities, the rule will not be effective as to those new financial institutions until the Commission so determines.").

286 12 C.F.R. § 1016.3(l).

expanded definition would include entities engaged in activities that are "incidental to" financial activities—including those later determined by the FRB to be financial activities—but would preserve the "significantly engaged" standard.[287] As of the date of this paper, the proposed rule has not yet been finalized and the historical differences remain.[288]

Commentary Box 8: Broad Reach of 'Financial Activities'

GLBA's incorporation of the definition of financial activities in BHCA and related regulations is significant. In the BHCA context, the purpose of the definition is to enumerate the permissible activities in which a bank holding company or financial holding company and its affiliates may engage. As such, the list of activities is intended to be quite expansive and, indeed, has grown over the years. Under GLBA and related regulations, the same list of activities is used to determine which entities are "financial institutions" subject to GLBA's requirements.[289] The list of financial activities includes, among others, lending, transferring or safeguarding money or securities, providing financial or investment advisory services, brokering loans, servicing loans, debt collecting, providing real estate settlement services, and career counseling in the financial services industry.[290]

As noted above, the pre-existing differences in interpretation of the statute by the FTC and the prudential regulators were preserved by the CFPB when it issued Regulation P. As a result, the activities that trigger coverage of nonbank entities subject to joint FTC and CFPB jurisdiction are somewhat narrower than for banks and their affiliates. For nonbanks, the list of qualifying financial activities is shorter as it includes only activities that are "financial in nature" (as opposed to activities that are incidental or complementary to financial activities).[291] In addition, the person

287 *See* 84 Fed. Reg. 13150 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. Part 313). The FTC's version of the Privacy Rule applies to entities that are excluded from CFPB jurisdiction, most notably certain auto dealers.

288 On July 13, 2020, the FTC held a public workshop regarding its 2019 proposed rule. Virtual Workshop, Information Security and Financial Institutions: FTC Workshop to Examine Safeguards Rule, Fed. Trade Comm'n (July 13, 2020), https://www.ftc.gov/news-events/events-calendar/information-security-financial-institutions-ftc-workshop-examine.

289 15 U.S.C. § 6809(3)(A).

290 12 U.S.C. § 1843(k)(1); *see also* FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT: A GUIDE FOR SMALL BUSINESS (2002), https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf.

291 *See* 65 Fed. Reg. 33646, 33654 n.23, 33673 (May 24, 2000) (codified at 16 C.F.R. Part 313).

must be "significantly engaged" in such activities in order to trigger application of GLBA.[292] The FTC has noted in guidance that whether an entity is "significantly engaged" in financial activities depends on all the facts and circumstances surrounding those activities and highlighted two factors as most important to that analysis: whether there is a "formal arrangement" between the entity and its customers and the frequency of the activity.[293] The CFPB's Regulation P provides a few examples of entities not "significantly engaged" in financial activities, in each case because the activities are either occasional or informal. [294]

Unlike nonbank financial institutions subject to joint CFPB and FTC jurisdiction, banks and their affiliates are not subject to the "significantly engaged" threshold in determining whether they qualify as a "financial institution."[295] In addition, the scope of qualifying financial activities is broader insofar as it includes, in addition to financial activities, activities determined by the FRB to be "incidental or complementary" thereto.[296] Thus, nonbank entities that engage in some "financial activities" may have doubts as to whether they meet the definition of a "financial institution" under the CFPB's Regulation P.[297]

292 12 C.F.R. § 1016.3(l)(3).

293 FED. TRADE COMM'N, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT: A GUIDE FOR SMALL BUSINESS (2002).

294 12 C.F.R. § 1016.3(l)(3)(iv). These examples include the following: (i) a retailer "if its only means of extending credit are occasional 'lay away' and deferred payment plans or accepting payment by means of credit cards issued by others"; (ii) a retailer "merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue"; (iii) a merchant "merely because it allows an individual to 'run a tab'"; and (iv) a grocery store "merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return." *Id.*

295 12 C.F.R. § 1016.3(l)(1).

296 12 C.F.R. § 1016.3(l)(1).

297 These activities include, among others: lending, servicing of loans, and activities related to extending credit; insurance and annuities; financial, investment, or economic advisory services; issuing or selling instruments representing interests in pools of assets permissible for bank to hold directly; underwriting, dealing in, or making a market in securities; providing management consulting services; operating a travel agency in connection with offering financial services; and acting as a finder. *See* 12 C.F.R. § 225.86.

Commentary Box 9: Applying GLBA in a Changing Business Landscape

The application of the Privacy Rule has grown more complex with the increasing diversity of business models in the financial services marketplace. The first step for nonbanks subject to FTC enforcement jurisdiction is to evaluate whether they are "significantly engaged" in financial activities as discussed above. The next step is to determine the nature of the relationship between the entity and consumers. Even if a company is engaged in a "financial activity" under BHCA, application of most Privacy Rule requirements depends on whether the entity has a direct relationship with a consumer. Where a company is acting solely as an agent for, or provides processing or other services on behalf of, another financial institution that is providing financial products or services to a consumer, the agent company is not regulated as a financial institution for purposes of Regulation P, even if it would otherwise meet Regulation P's definition of a "financial institution."[298] As discussed further below, this means that the agent company is likely subject only to limitations on the reuse and redisclosure of information received from its principal.

This analysis must be revisited as business models and relationships continue to evolve within the financial services ecosystem. Two examples of relatively recently emerged business models can help illustrate the point: personal financial management companies and data aggregators. First, depending on the nature of the services, companies offering personal financial management services directly to consumers may be engaged in "financial advisory services" and/or "data processing" within the scope of BHCA.[299] Assuming that activity levels are high enough and that the company has direct customer relationships with consumers, a personal financial management company would likely be deemed to be a "financial institution" under GLBA. Indeed, the FTC's preamble to its GLBA implementing regulations noted that "data processing" had specifically been designated as a permissible banking activity under Regulation Y and, therefore, brought "into the definition of financial institution an Internet company that compiles or aggregates an individual's online accounts (such as credit cards, mortgages, and loans) at that company's web site as a

298 12 C.F.R. § 1016.3(e)(2)(v).

299 12 U.S.C. § 5481(15)(A)(viii).

service to the individual, who then may access all of its account information through that Internet site."[300]

Data aggregators perform similar data processing and transmission activities in the course of compiling consumer data. However, because data aggregators typically function as service providers to financial institutions that are the end users of the data, rather than providing services directly to consumers, data aggregators would likely be subject only to the reuse and redisclosure requirements under the Privacy Rule, rather than the requirements to provide privacy notices and administer the opt-out process.[301] At least one prominent data aggregator has publicly stated that it considers itself governed by GLBA, commenting that "[e]cosystem participants—both traditional institutions and new digital players—should abide by this framework, including provisions that limit the use of permissioned data to the scope of the consumer's consent."[302] Comments submitted to the CFPB from other industry participants have emphasized the need for the CFPB to officially clarify that data aggregators are "financial institutions" subject to the Privacy Rule and Regulation P more broadly.[303]

b. Non-affiliated Third Parties

Although the primary focus of the Privacy Rule is on financial institutions and their affiliates, as discussed further below the statute and regulations also impose some downstream limitations on information sharing by non-affiliated third parties that receive NPI from a financial institution. For purposes of the Privacy Rule, a "non-affiliated third party" means "any entity that is not an

300 65 Fed. Reg. 33646, 33655 (May 2000) (codified at 16 C.F.R. Part 313).

301 In the preamble to its implementing regulations the FTC stated that "[t]he Commission agrees that the purposes of the G-L-B Act will be met provided the activities of the agent are the responsibility of the financial institution, and, therefore, the financial institution fulfills the obligations regarding the agent's handling of consumer information that would otherwise fall on the agents. Of course, those providing services to a financial institution will also be subject to the limitations on reuse of information." 65 Fed. Reg. 33646, 33651 (May 24, 2000) (codified at 16 C.F.R. Part 313). See Section III.B.4. for a discussion of the substantive requirements under the Privacy Rule.

302 Plaid, Comment Letter in Response to the CFPB's RFI Regarding Consumer Access to Financial Records (Feb. 21, 2017), at 17, https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf.

303 *See* The Clearing House, Comment Letter in Response to the CFPB's RFI Regarding Consumer Access to Financial Records (Feb. 21, 2017), at 3–4, https://beta.regulations.gov/comment/CFPB-2016-0048-0066 (noting "guiding principal" to address CFPB rulemaking on consumer access to data that data aggregators are "financial institutions" under GLBA); Meredith Fuchs, Capital One, Comment Letter in Response to the CFPB's RFI Regarding Consumer Access to Financial Records (Feb. 21, 2017), at 5–8, https://beta.regulations.gov/comment/CFPB-2016-0048-0042 (arguing data aggregators are "financial institutions" under GLBA).

affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution."[304]

Depending on the circumstances, non-affiliated third parties can include both vendors who are providing services to a financial institution as well as entities that are not acting on behalf of a financial institution or otherwise facilitating the financial institution's provision of products and services to a customer.[305] The statute applies the same limitations to non-affiliated third parties regardless of whether they may meet the definition of a "financial institution" in their own right.[306] As discussed further below, neither the statute nor Regulation P directly addresses requirements for downstream entities that receive NPI from a non-affiliated third party.[307]

c. Application to Consumers and Customers

GLBA defines a "consumer" as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[308] Regulation P provides several examples of the types of consumers covered by the rule, including individuals that apply for credit from a financial institution; individuals that provide information to a financial institution in order to obtain financial, investment, or economic advisory services; and individuals whose loans are owned or serviced by a financial institution.[309]

A "customer" is defined as "a consumer who has a customer relationship with a financial institution." A customer relationship means "a continuing relationship between a consumer and a financial institution."[310] Examples of a customer relationship include, among others, opening a deposit or investment account, obtaining or servicing a loan, and purchasing an insurance product.[311] A continuing relationship is not present when a consumer obtains a financial product or service only in isolated transactions.[312] The distinction between consumer and customer is

304 15 U.S.C. § 6809(5); 12 C.F.R. § 1016.3(o).

305 See Section III.B.4.d. for more information on the exceptions to opt-out and notice requirements for third-party service providers.

306 15 U.S.C. § 6802(c). The CFPB's 2018 rulemaking altered Regulation P's definition of "you," limiting it to only financial institutions for which the Bureau has rulemaking authority" over under GLBA. 12 C.F.R. § 1016.3(s)(1). The prior definition of "you" had included other entities in addition to financial institutions. This change may inadvertently have given rise to confusion as to whether non-financial institutions that receive NPI are subject to certain regulations. See Commentary Box 13 more information.

307 By contrast, the FTC's implementing regulations for the Safeguards Rule directly addresses the oversight required of service providers and downstream data sharing. See Section III.C.4.a. for more information.

308 15 U.S.C. § 6809(9).

309 12 C.F.R. § 1016.1(e)(2). Unlike the Privacy Rule, which applies to consumers even if they are not customers (e.g., if they submit an application for a financial product or service but do not end up becoming a customer), the Safeguards Rule applies only to *customer* data. See Section III.C.2. for additional detail.

310 12 C.F.R. § 1016.3(i).

311 12 C.F.R. § 1016.3(j)(2)(i).

312 12 C.F.R. § 1016.3(j)(2)(ii).

relevant as notice and other obligations that financial institutions have under the Privacy Rule vary based on the nature of the relationship with the individual, as well as from whom the nonpublic personal information is acquired.

2. Data Covered

The Privacy Rule covers "nonpublic personal information" ("NPI"), which includes "personally identifiable financial information" and "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."[313] NPI does not cover "publicly available information" or lists, descriptions, or groupings derived without using any personally identifiable financial information that is not publicly available.[314]

"Personally identifiable financial information means any information (i) a consumer provides to [a financial institution] to obtain a financial product or service from [a financial institution]; (ii) about a consumer resulting from any transaction involving a financial product or service between [a financial institution] and a consumer; or (iii) [a financial institution] otherwise obtain[s] about a consumer in connection with providing a financial product or service to that consumer."[315] Examples of personally identifiable financial information include:

- information consumers provide on application forms for financial products or services;
- information pertaining to account balance, payment, overdraft, or purchase history;
- information indicating that an individual is or has been a customer;
- information obtained through loan collections or servicing;
- information obtained through internet "cookies"; and
- information from consumer reports.[316]

Information "that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses" is not covered by the Privacy Rule.[317] Neither is "publicly available information," which encompasses

313 12 C.F.R. § 1016.3(p)(1); *see also* 15 U.S.C. §6809(4).

314 12 C.F.R. § 1016.3(p)(2).

315 12 C.F.R. § 1016.3(q)(1). The statutory language of GLBA defines the term similarly to include information "(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." 15 U.S.C. §6809(4)(A).

316 12 C.F.R. § 1016.3(q)(2)(i)(A)–(G).

317 12 C.F.R. § 1016.3(q)(2)(ii)(A)–(B).

"information that [a financial institution has] a reasonable basis[318] to believe is lawfully made available to the general public" from government records, widely distributed media, or legally required disclosures to the general public.[319] The Privacy Rule also only applies to NPI about individuals who obtain financial products or services "primarily for personal, family, or household purposes" and, therefore, does not cover "information about companies or individuals who obtain financial products or services for business, commercial, or agricultural purposes."[320]

Commentary Box 10: How Anonymous is Anonymized Data?

The Privacy Rule's implementing regulations exclude "aggregate information" and "blind data" from the definition of "personally identifiable financial information," effectively carving out such data from the scope of the NPI data covered under the Privacy Rule.[321] As such, companies need not comply with the notice and opt-out requirements under the Privacy Rule as it relates to anonymized data before selling or sharing it. At a conceptual level, this approach is consistent with GLBA's goal of protecting consumer privacy. In practice, however, the implementation of this exception is more challenging. Regulation P does not specify what level of anonymization is sufficient for compliance. For example, research has shown that, at least for certain datasets, reidentification can be achieved by "using background knowledge and cross-correlation with other databases to re-identify individual data records."[322] As new technology becomes available, de-identification practices that were once considered sound may no longer be effective. Whether or not aggregate data provides the privacy protections worthy of being excluded from the substantive requirement is a topic of debate among privacy experts.[323] Additional clarity may be

318 The "reasonable basis" provision requires financial institutions to take steps to determine that "the information is of the type that is available to the general public," whether the individual "can direct that the information not be made available to general public," and "if so, that the consumer has not done so." 12 C.F.R. § 1016.3(r)(2).

319 12 C.F.R. § 1016.3(r)(1).

320 12 C.F.R. § 1016.1(b).

321 12 C.F.R. § 1016.3(q)(2)(ii).

322 Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2008), http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (demonstrating that deanonymization technology can be used to identify Netflix records of known users and uncover apparent political preferences and other potentially sensitive information).

323 *See e.g.* Luk Arbuckle, *Aggregate Data Provides a False Sense of Security*, INT'L ASS'N OF PRIVACY PROF'LS, (Apr. 27, 2020), https://iapp.org/news/a/aggregated-data-provides-a-false-sense-of-security/.

beneficial here, as well as in other areas where anonymized data is exempted from coverage, such as the definition of "consumer reports" under FCRA.[324]

3. Oversight

Federal rulemaking authority to implement GLBA's Privacy Rule was originally allocated among the federal prudential bank regulators, the NCUA, the FTC, the SEC, and the CFTC. The federal prudential bank regulators—the FRB, the OCC, the FDIC, and the former Office of Thrift Supervision ("OTS")—jointly adopted final rules in 2000.[325] The NCUA, FTC, SEC, and CFTC, which had rulemaking authority with respect to their respective regulated entities, each issued separate rules implementing the Privacy Rule.[326] In 2009, the agencies collectively issued a joint final rule establishing the model form for financial institutions to utilize when providing initial, annual, and revised privacy notices.[327]

In 2011, DFA transferred GLBA rulemaking authority from the FRB, NCUA, OCC, FDIC, and the FTC (in part) to the CFPB.[328] The CFPB restated the implementing regulations in Regulation P [329] in late 2011 through an interim final rule[330] that was finalized as amended in 2014.[331]

Currently, the CFPB has authority to promulgate regulations under the Privacy Rule for depository institutions and most non-depository institutions. The FTC, SEC, CFTC, and state insurance authorities, however, retain rulemaking authority over most motor vehicle dealers, securities firms, futures-related companies, and insurance-related companies, respectively.[332] The federal agencies are required by statute to consult with each other and with representatives

324 See Section IV.C. for additional information about aggregate data as it relates to FCRA requirements.

325 65 Fed. Reg. 35161 (June 1, 2000) (codified at 12 C.F.R. Parts 40, 216, 332, 573).

326 65 Fed. Reg. 31721 (May 18, 2000) (NCUA final rule codified at 12 C.F.R. Parts 716, 741); 65 Fed. Reg. 33645 (May 24, 2000) (FTC final rule codified at 16 C.F.R. Part 313); 65 Fed. Reg. 40333 (June 29, 2000) (SEC final rule codified at 17 C.F.R. Part 248); 66 Fed. Reg. 21235 (Apr. 27, 2001) (CFTC final rule codified at 17 C.F.R. Part 160).

327 74 Fed. Reg. 62889 (Dec. 1, 2009) (codified at 12 C.F.R. Parts 40, 216, 332, 573, 716; 16 C.F.R. Part 313; 17 C.F.R. Parts 160, 248).

328 *See* 12 U.S.C. §§ 5481(12), 5581. The OTS was disbanded with the passage of DFA. Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*).

329 12 C.F.R. § 1016 *et seq.*

330 76 Fed. Reg. 79025 (Dec. 21, 2011) (codified at 12 C.F.R. Part 1016).

331 79 Fed. Reg. 64057 (Oct. 28, 2014) (codified at 12 C.F.R. Part 1016).

332 *See* 16 C.F.R. Part 313 (FTC), 17 C.F.R. Part 248 (SEC), and 17 C.F.R. Part 160 (CFTC). This paper refers to the applicable provisions of the rules promulgated by the CFPB in Regulation P, where applicable, and does not reference the FTC's corresponding provisions of these regulations unless specifically relevant.

of state insurance authorities to ensure consistency and comparability among the respective regulations implementing the Privacy Rule.[333] Although significant portions of the rulemaking authority for the Privacy Rule were shifted to the CFPB by DFA, supervisory and enforcement authority remains split between the CFPB and the other applicable federal regulators discussed above with respect to the persons under their jurisdiction.[334] Although depository institutions have historically been subject to supervision by the prudential regulators, DFA provided the CFPB with supervision authority for over a large array of non-bank institutions that were previously not subject to supervision for compliance with consumer protections laws like GLBA, except in limited third-party service provider situations.[335]

Despite the fact that no private right of action exists under GLBA, civil monetary penalties are available to regulators, in certain circumstances, as a mechanism to punish and deter violations. The availability and size of civil penalties vary by the authorizing statute of the agency bringing an enforcement action. For example, the FTC Act limits the FTC's authority to disgorgement and injunctive relief for initial violations of GLBA,[336] whereas the FDI Act permits prudential regulators to seek civil penalties for entities under their supervision.[337]

4. Substantive Requirements

a. Summary

The Privacy Rule obligates each financial institution to comply with three primary requirements: (i) to provide notice to both consumers and customers about its privacy policies and practices; (ii) to describe the conditions under which the financial institution may disclose NPI about consumers to non-affiliated third parties; and (iii) to provide a method for consumers to prevent the institution from disclosing NPI to most non-affiliated third parties by opting out, subject to certain exceptions explained below. The Privacy Rule also limits the redisclosure and reuse of NPI by financial institutions and non-affiliated third parties that receive information directly from financial institutions, though it is less clear about restricting further downstream parties. The Privacy Rule does not impose privacy notice and opt-out requirements on companies when they are not providing financial services directly to consumers or customers in their own right, even if

333 15 U.S.C. § 6804(a)(2).

334 15 U.S.C. § 6805(a).

335 12 U.S.C. § 5514(a).

336 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-196, CONSUMER DATA PROTECTION: ACTIONS NEEDED TO STRENGTHEN OVERSIGHT OF CONSUMER REPORTING AGENCIES 18–20 (2019), https://www.gao.gov/assets/700/697026.pdf.

337 *See* 12 U.S.C. § 1818(i)(2).

such companies are performing financial activities that would otherwise qualify them as "financial institutions."[338]

b. Requirements Relating to Opt-Out Rights

As outlined above, the Privacy Rule requires financial institutions to provide notice to consumers of their right to opt out from certain data sharing with non-affiliated third parties. Although financial institutions can provide consumers with a separate notice explaining any required opt-out rights, the model privacy form for initial, annual and revised privacy notices meets the notice requirements for opt-out rights.[339] As a result, financial institutions typically satisfy the opt-out notice requirements by utilizing the model form. Opt-out notices must at a minimum provide the following information to consumers:

- that the financial institution discloses or reserves the right to disclose NPI about the consumer to a non-affiliated third party;
- that the consumer has the right to opt out of that disclosure; and
- a reasonable means by which the consumer may exercise the opt-out right.[340]

The regulations also specify what constitutes "reasonable opt-out means," such as:

- designating check-off boxes in a prominent position on the relevant forms with the opt-out notice;
- including a reply form together with the opt-out notice that includes the address to which the form should be mailed;
- providing an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the institution's website, if the consumer agrees to the electronic delivery of information; or
- providing a toll-free telephone number that consumers may call to opt out.[341]

338 *See* 12 C.F.R. § 1016.11.

339 12 C.F.R. § 1016.7(k).

340 12 C.F.R. § 1016.7(a)(1).

341 12 C.F.R. § 1016.7(a)(2)(i).

When dealing with joint relationships, a financial institution may provide a single opt-out notice, but the notice must explain how the institution will handle opt-out directions by consumers in a joint relationship. The following limitations are placed on financial institutions regarding opt outs for joint relationships:

- If a consumer in a joint relationship chooses to opt out, a financial institution can treat that as opting all consumers out, or permit each consumer to opt out separately;
- If the financial institution allows consumers to opt out separately, the institution must permit one consumer to opt out on behalf of all joint consumers;
- The financial institution may not require all consumers to opt out before honoring an individual opt-out request.[342]

c. Limits on Disclosure – General Rule

Subject to multiple exceptions explained below, a financial institution[343] is prohibited from disclosing NPI about a consumer to a non-affiliated third party[344] unless the financial institution provides the consumer with (i) an initial notice containing the substantive requirements discussed below; (ii) an opt-out notice; and (iii) a reasonable opportunity to opt out prior to the disclosure of any NPI.[345] For example, if a financial institution decided to sell its customer list to an unaffiliated company so that the company could use the list for marketing purposes, the financial institution would have to first provide notice and an opportunity to opt out of the sale. With limited exceptions, financial institutions are also specifically not permitted to disclose consumer account numbers to non-affiliated third parties for marketing purposes.[346]

In addition to limiting financial institutions' disclosure of NPI in the first instance, the Privacy Rule also restricts the subsequent redisclosure and reuse of NPI once received by non-affiliated third parties.[347] As discussed below, the scope of permitted activities by a financial institution or

342 12 C.F.R. § 1016.7(d).

343 As discussed above in Section III.B.1., the Privacy Rule also applies to service providers and other nonaffiliated third parties that receive NPI from financial institutions with whom they are not affiliated. *See* 12 C.F.R. § 1016.1(b).

344 GLBA does not impose data sharing restrictions among affiliated entities.

345 12 C.F.R. § 1016.10(a).

346 12 C.F.R. § 1016.12. This restriction does not apply to disclosures of such information to consumer reporting agencies, to agents or service providers solely in order to perform marketing for the financial institution's own products or services, or to participants in a private label credit card program or an affinity or similar program where the participants in the program are identified to the customer when the customer enters the program. *Id.* at § 1016.12(a)–(b).

347 *See* 15 U.S.C § 6802(c); 12 C.F.R. § 1016.11.

a covered third party with respect to such NPI depends on the source of the information and the circumstances of its disclosure.

d. Limits on Disclosure – Exceptions

The Privacy Rule sets forth three categories of exceptions pursuant to which financial institutions are permitted to provide NPI to non-affiliated third parties without complying with the applicable notice and/or opt-out requirements.[348] These exceptions apply when financial institutions are engaged with (i) joint marketing and other service providers;[349] (ii) processing and servicing transactions;[350] and (iii) certain other circumstances.[351]

Exception 1 – Joint Marketing and Other Service Providers

The first exception covers the disclosure of information by a financial institution to a non-affiliated third party to perform services for, or on behalf of, the financial institution where the activities are not otherwise covered by Exception 2 or 3. Joint marketing agreements between financial institutions are an example of such activity.[352] Where the exception applies, financial institutions are not required to provide consumers with an opportunity to opt out of the information sharing, provided that the following conditions are met:

- The financial institution provided an initial privacy notice to the consumer; and
- The financial institution entered into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.[353]

The FRB issued guidance on GLBA in 2001 that addressed various questions related to this exception.[354] In this guidance, the FRB clarified that (i) the joint marketing exception specifically applies to disclosures made between two financial institutions; (ii) the arrangement must offer, endorse, or sponsor financial products or services; and (iii) the joint marketing arrangements must be described in the initial, annual, or revised privacy notices.[355]

---

348 *See* 15 U.S.C §6802; 12 C.F.R. §§ 1016.13, 1016.14, 1016.15.

349 12 C.F.R. § 1016.13.

350 12 C.F.R. § 1016.14.

351 12 C.F.R. § 1016.15.

352 A "joint agreement" is defined under Regulation P as a "written contract pursuant to which you and one or more financial institutions jointly offer, endorse, or sponsor a financial product or service." 12 C.F.R. § 1016.13(c).

353 12 C.F.R. § 1016.13(a).

354 FED. RESERVE BD., FREQUENTLY ASKED QUESTIONS FOR THE PRIVACY REGULATION (2001), https://www.federalreserve.gov/boarddocs/press/general/2001/200112122/attachment.pdf.

355 FED. RESERVE BD., FREQUENTLY ASKED QUESTIONS FOR THE PRIVACY REGULATION 28–32 (2001).

Although service providers are specifically called out in this exception, Exceptions 2 and 3 also encompass activities—such as legal services, account servicing, and others—that involve information sharing with service providers. Due to the less stringent requirements regarding notice and opt-out, as well as the impact on which reuse and disclosure requirements are applicable, financial institutions may choose to rely more heavily on Exceptions 2 and 3 where possible.

Exception 2 – Processing and Servicing Transactions

A financial institution is not required to comply with either notice or opt-out requirements if the financial institution discloses NPI "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with" any of the following:

- servicing or processing a financial product or service that a consumer requests or authorizes;
- maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or
- a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.[356]

Exception 3 – Certain Other Circumstances

Regulation P also contains several other exceptions to the notice and opt-out requirements covering disclosure by a financial institution of NPI under a variety of scenarios, including, among others:

- with consumer consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;[357]
- to protect confidentiality or security;

356 12 C.F.R. § 1016.14(a)(1)–(3).

357 The implementing regulations to the Privacy Rule provide little detail concerning the means and timing by which a consumer can provide consent. The Rule provides only that a consumer "may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information" as permitted under the Privacy Rule. 12 C.F.R. § 1016.15(b)(2).

- to protect against fraud, unauthorized transactions, claims, or other liabilities;
- to persons holding a legal or beneficial interest relating to the consumer;
- to persons acting in a fiduciary or representative capacity on behalf of the consumer;
- to law enforcement agencies and applicable regulators;
- to consumer reporting agencies in accordance with FCRA;
- in connection with a proposed or actual sale or similar transaction involving all or a portion of a business or operating unit; and
- to comply with applicable law.[358]

Commentary Box 11: Scope and Processes Concerning Consumer Consent

The Privacy Rule actually relies on two different consumer consent mechanisms, since it is primarily structured to rely on notice and opt-out but also contains an exception to that regime for sharing with the consent or at the direction of the consumer.[359] Both forms of consent raise potential policy issues, particularly as a growing body of research suggests that choice architecture can affect the ways that consumers make decisions.[360] Critics have argued since the law was originally proposed that reliance on an opt-out structure is insufficient to protect consumer

358 12 C.F.R. § 1016.15.

359 The exceptions to the Privacy Rule also treat information sharing for certain purposes to be inherently permissible regardless of consumer consent. As discussed in Commentary Box 17, there is a growing debate about the tradeoffs between using permissible purposes as compared to consumer consent to manage privacy and other policy concerns, separate from the primary focus in this commentary box about particular structure of the consent process.

360 *See* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008); Jon M. Jachimowicz et al., *When and Why Defaults Influence Decisions: A Meta-Analysis of Default Effects*, 3:2 BEHAVIORAL PUB. POL'Y 159 (2019), https://www.cambridge.org/core/journals/behavioural-public-policy/article/when-and-why-defaults-influence-decisions-a-metaanalysis-of-default-effects/67AF6972CFB52698A60B6BD94B70C2C0; Alessandro Acquisti et al., *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online*, 50:3 ACM COMPUTING SURVEYS #44 (2017), https://dl.acm.org/doi/10.1145/3054926; James J. Choi et al., *Defined Contribution Pensions: Plan Rules, Participant Decisions, and the Path of Least Resistance*, NAT'L BUREAU OF ECON. RESEARCH, Working Paper 8655 (Dec. 2001), https://www.nber.org/papers/w8655.pdf.

privacy interests, while proponents argue that it is more efficient than requiring each consumer to transmit an affirmative opt-in.[361]

The impact of the exception for affirmative consumer consent is also growing as consumer-permissioned data aggregation is becoming more common, though it was not a major point of focus in the original rulemakings. For instance, the implementing regulations specify only that the consent or direction must not be revoked to be valid, but otherwise provide no additional detail concerning the breadth or duration of the consent, the means by which such consent is captured, or how the consent may be revoked.[362] They also do not address whether consumers have the right to direct that their data be deleted after consent revocation. Thus, the exception raises similar policy questions to the consent issues that are raised under Section 1033 and an affirmative consent exception in FCRA.[363]

Although no formal guidance on these topics has been issued pursuant to GLBA by the applicable regulatory agencies, at least one regulator briefly acknowledged some of the potential process issues. In issuing its initial rules under the Privacy Rule, the FTC noted that, "[s]everal commenters responded to the request for comment on whether the consent exception should include consumer safeguards, such as a requirement that the consent be written, be indicated by a signature on a separate line, or automatically terminate after a certain period of time."[364] The FTC declined to issue further guidance despite these comments, noting that "the resolution of this issue is appropriately left to the particular circumstances of a given transaction[,]" and the covered entity should take steps to ensure "the limits of the consent are well understood by both the institution and the consumer."[365] In the absence of federal guidance, financial institutions must thus make their own

361 *See, e.g., Financial Privacy and Consumer Protection: Hearing Before the S. Comm. on Banking, Housing, & Urban Affairs*, 107th Cong. 107-990 (2002); 45 CONG. REC. E2363, E2364 (Daily Ed. Nov. 11,1999) (statement of Rep. Melvin Watt); 145 CONG. REC. S13, 783, 789 (Daily Ed. Nov. 3, 1999) (statement of Sen. Paul Sarbanes); 145 CONG. REC. H11539 (daily ed. Nov. 4, 1999) (statement of Rep. Davis); 145 CONG. REC. S13785 (daily ed. Nov. 3, 1999) (statement of Chairman Sen. Phil Gramm); 145 CONG. REC. S13, 876 (daily ed. Nov. 4, 1999) (statement of Sen. Chuck Hagel).

362 There is a similar lack of clarity and guidance under FCRA and related regulations regarding various consent-related issues where a CRA provides a consumer report to a third party at the consumer's direction under 15 U.S.C. § 1681b(a)(2).

363 See Commentary Box 6 and Commentary Box 17 for more information.

364 65 Fed. Reg. 33646, 33671 (May 24, 2000) (codified at 16 C.F.R. Part 313).

365 65 Fed. Reg. 33646, 33671 (May 24, 2000) (codified at 16 C.F.R. Part 313).

determinations as to what kind of consent is sufficient, how long such consent is valid, and how to offer and document revocation.

e. Limits on Redisclosure and Reuse of NPI

In addition to the requirements placed on financial institutions with respect to their own data, the Privacy Rule and its implementing regulations also impose limitations on the redisclosure and reuse of NPI when that information is transferred from a financial institution to a non-affiliated third party.[366] These provisions are extremely important in light of the rapidly changing financial services ecosystem, in which financial data frequently moves between financial institutions and non-affiliated parties. The efficacy of the data privacy protections afforded by the Privacy Rule is thus significantly impacted by the extent to which data privacy limitations follow the data as it moves among various parties.

GLBA provides that:

> [A] non-affiliated third party that receives from a financial institution nonpublic personal information under this section shall not, directly or through an affiliate of such receiving third party, disclose such information to any other person that is a non-affiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution.[367]

Although the statute itself mentions disclosure limitations, Regulation P expands further and imposes usage limitations on non-affiliated third parties as well.[368] Regulation P details the redisclosure and reuse requirements under a complicated matrix of rules that depend on whether the NPI is being received or disclosed and whether any particular exception applies.[369]

366 *See* 15 U.S.C. § 6802(c); 12 C.F.R. § 1016.11.

367 15 U.S.C. § 6802(c).

368 *See* 12 C.F.R. § 1016.11.

369 It is important to note that the statutory language of the Privacy Rule only contemplates the situation in which information from a financial institution is received by a nonaffiliated financial institution. Neither law nor regulation directly addresses the circumstance in which a nonaffiliated third party discloses NPI to, or receives NPI from, a nonaffiliated third party that is not a financial institution. Recent changes to Regulation P have given rise to further uncertainty into this area. See Commentary Box 13 for additional detail.

For example, a non-affiliated third party that receives NPI from a financial institution under Exception 2 in order to provide account processing services, could disclose or use that information for any reason listed in Exception 2 and 3, such as providing such information to law enforcement agencies, but it could not use the NPI for its own marketing purposes.[370] If that same non-affiliated third party receives NPI not subject to an exception (because a consumer has not exercised their opportunity to opt out of a type of information sharing disclosed in a privacy notice for which no exception applies), the scope of permissible use and disclosure is more expansive, including for its own purposes.[371] See Appendix A for a summary of the redisclosure and reuse rules. In some circumstances, recipients of financial data are sometimes bound by the privacy policies of, and contractual confidentiality provisions with, the original data holders in addition to regulatory limitations.

Commentary Box 12: Information Sharing Among Affiliates

Although drafters ultimately decided to focus GLBA privacy restrictions primarily on financial institutions' sharing customer information with nonaffiliated parties, the run up to the legislation had included controversies about sharing between affiliated companies as well.[372] Some members of Congress specifically criticized the legislation as weak for not addressing affiliate sharing in more depth, particularly given that the law encouraged mergers between different types of financial institutions.[373] Concerns about affiliate sharing continue to come up today. For instance, some stakeholders have raised concerns about payment networks' acquisitions of data aggregators on those grounds.[374]

370 12 C.F.R. § 1016.11(a)(2).

371 *See* 12 C.F.R. § 1016.11(b)(2).

372 Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L. J. 497, 500–04 (2002); *see also Financial Privacy And Consumer Protection: Oversight Hearing on the Gramm-Leach-Bliley Act Before the S. Comm. of Banking, Housing and Urban Affairs*, 107th Cong. (2002) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group, discussing a $7 million penalty imposed on a bank that shared financial statements, account balances, and other confidential information with an affiliated securities firm) *available at* https://privacyrights.org/resources/oversight-hearing-financial-privacy-and-gramm-leach-bliley-financial-services. Although GLBA is not focused on information sharing among affiliates, model forms issued under the statute do include potential language on affiliate sharing that is required under certain circumstances by FCRA. See Section IV.E.1.c. for a discussion of FCRA's treatment of affiliate sharing.

373 145 CONG. REC. S13871-07 (daily ed. Nov. 4, 1999) (statement of Sen. Johnson); 145 CONG. REC. E2291-04 (daily ed. Nov. 5, 1999) (statement of Rep. Stark); 145 CONG. REC. E2296-02 (daily ed. Nov. 8, 1999) (statement of Rep. Stark).

374 *See, e.g.*, Penny Crosman, *What the Visa-Plaid Merger Means for Banks, Fintechs*, AM. BANKER (Jan. 16, 2020), https://www.americanbanker.com/news/what-the-visa-plaid-merger-means-for-banks-fintechs; Rey Mashayekhi, With Plaid Acquisition, *Visa Makes a Big Play for the 'Plumbing' That Connects the Fintech World*, FORTUNE (Jan. 14, 2020), https://fortune.com/2020/01/14/visa-plaid-acquisition-fintech/.

Commentary Box 13: Application of Reuse and Redisclosure Provisions

As discussed above and in Appendix A, application of the reuse and redisclosure limitations imposed by Regulation P are extremely complex even as to initial information sharing between financial institutions and nonaffiliated third parties. Treatment of downstream parties who in turn receive financial data from an initial nonaffiliated third-party recipient are even less clear.

The situation is complicated by the fact that some regulations are phrased as applying to entities covered under the definition of "you,"[375] while others focus on "third-party" information recipients.[376] The term "you" is defined under Regulation P as "a financial institution for which the [CFPB] has rulemaking authority" under GLBA.[377] Previously, this definition included "financial institutions and other entities" for which the CFPB had rulemaking authority. In 2018, however, the CFPB amended this definition to refer only to financial institutions to align the definition with those entities required to provide a privacy notice under the statute.[378]

This 2018 change created some uncertainty as to exactly which parts of the regulation apply to nonfinancial institution recipients that receive information directly from a financial institution and whether or how downstream recipients are also subject to the Privacy Rule. Although it could be argued that the updated definition of "you," considered in isolation, excludes those "other entities," the section of Regulation P describing its general scope continues to state that the rule "applies to any financial institution and other covered person or service provider that is subject to Subtitle A of Title V of the GLBA, including third parties that are not financial institutions but that receive nonpublic personal information from financial institutions with whom they are not affiliated."[379]

375 *See* 12 C.F.R. § 1016.11.

376 12 C.F.R. § 1016.11(c).

377 12 C.F.R. § 1016.3(s)(1). Other implementing regulations contain similar language with respect to their covered entities. *See, e.g.*, 16 C.F.R. § 313.3(q).

378 *See* 83 Fed. Reg. 40945 (Aug. 17, 2018) (codified at 12 C.F.R. Part 1016).

379 12 C.F.R. § 1016.1(b)(1).

f. Initial and Periodic Privacy Notices – Content Requirements

The Privacy Rule specifies three types of notices that are required for financial institutions to provide to their consumers and customers, as applicable: (i) initial notice; (ii) annual notice; and (iii) revised notice. Each notice must contain the following information, in addition to any other information that the financial institution wishes to provide:

- the categories of NPI that a financial institution collects;
- the categories of NPI that a financial institution discloses;
- the categories of affiliates and non-affiliated third parties to whom a financial institution discloses NPI, other than those covered by Exceptions 2 and 3;
- the categories of NPI about a financial institution's former customers that it discloses and the categories of affiliates and non-affiliated third parties to whom it discloses NPI about its former customers, other than those covered by Exceptions 2 and 3;
- if a financial institution discloses NPI to a non-affiliated third party under Exception 1 (and Exceptions 2 and 3 do not apply to that disclosure), a separate statement of the categories of information it discloses and the categories of third parties with whom the financial institution has contracted;
- an explanation of the consumer's right to opt out of the disclosure of NPI to non-affiliated third parties, including the method(s) by which the consumer may exercise that right at that time (discussed further below);
- any disclosures that a financial institution makes under the opt-out requirements for affiliate sharing pursuant to FCRA;[380]
- the financial institution's policies and practices with respect to protecting the confidentiality and security of NPI; and

380 The affiliate sharing notice and opt-out requirements are detailed in Section 603(d)(2)(A)(iii) of FCRA (16 U.S.C. § 1681a(d)(2)(A)(iii)). See Section IV.E.1.c. for more information on the affiliate-sharing requirements under FCRA.

- disclosures that inform consumers that a financial institution may disclose NPI for everyday business purposes and as permitted by law.[381]

Regulation P provides financial institutions with examples of sufficient disclosures for many of these notice categories, as well as a model privacy form that, if utilized consistent with the instructions, constitutes compliance with the notice content requirements under GLBA.[382]

g. Initial and Periodic Privacy Notices – Timing Requirements

Initial Notice

Financial institutions must provide an initial privacy notice to both customers and consumers. Customers must receive the notice before or at the time a customer relationship is established except in certain specified circumstances.[383] Consumers must receive the notice prior to the financial institution disclosing any NPI about the consumer to any non-affiliated third party.[384]

Annual Notice

Annual notices are required for the duration of the customer relationship, with the first annual notice due in the year following the year in which the financial institution provided the initial notice.[385] However, in 2015 Congress exempted a financial institution from providing an annual notice if the institution only discloses NPI to non-affiliated third parties under the three exceptions set forth above, and the institution has not changed its policies and practices regarding disclosure of NPI since the last time it provided a notice to the customer.[386]

381 12 C.F.R. § 1016.6(a)(1)–(9).

382 12 C.F.R. § 1016.2. Model privacy forms are available in the Appendix to 12 C.F.R. Part 1016.

383 12 C.F.R. § 1016.4(a)(1). Financial institutions are not required to provide initial privacy notices before or at the time the customer relationship is established if establishing the customer relationship is not at the customer's election (e.g., a transfer of servicing rights) or providing such notice "would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time." 12 C.F.R. § 1016.4(e). A financial institution is not required to provide initial privacy notices to an existing customer if the prior notice to the customer was accurate with respect to the new financial product or service or if the financial institution provides a revised privacy notice to the customer that covers the customer's new financial product or service. *See* 12 C.F.R. § 1016.4(d).

384 12 C.F.R. § 1016.4(a)(2). A financial institution is not required to provide an initial privacy notice to a consumer if the financial institution does not disclose any NPI about a consumer to a nonaffiliated third party or if the financial institution does not have a customer relationship with the consumer. *See* 12 C.F.R. § 1016.4(b).

385 12 C.F.R. § 1016.5(a). "Annual" is defined as at least once in any period of 12 consecutive months during which that relationship exists. *See* 12 C.F.R. 1016.5(a)(1). Financial institutions are permitted to define the 12-consecutive-month period, but it must be applied to the customer consistently. *See* 12 C.F.R. 1016.4(a)(2).

386 *See* 12 C.F.R. § 1016.5(e)(1). This exemption was included in the Fixing America's Surface Transportation Act (FAST Act), which was passed December 4, 2015. The CFPB issued a proposed rule implementing the FAST Act statutory amendment to GLBA on July 15, 2016, which was later adopted on August 17, 2018. *See* 83 Fed. Reg. 40945 (Aug. 17, 2018) (codified at 12 C.F.R. Part 1016).

Revised Notice

Unless otherwise permitted pursuant to the exceptions outlined above, a financial institution is not permitted to disclose any NPI about a consumer to a non-affiliated third party other than as described in the initial notice, unless the financial institution has provided to the consumer a clear, conspicuous, and accurate revised privacy notice and a new opt-out notice, and the consumer has not opted out after being given a reasonable opportunity to do so.[387] For example, a revised privacy notice is required if a financial institution wishes to disclose (i) a new category of NPI to a non-affiliated third party; (ii) NPI to a new category of non-affiliated third party; or (iii) NPI about a former customer to a non-affiliated third party, if the former customer did not have the opportunity to exercise an opt-out right regarding that disclosure.[388]

h. Initial and Periodic Privacy Notices – Means of Delivery

Financial institutions are required to provide initial and periodic privacy notices "so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically."[389] Financial institutions are explicitly precluded from providing an oral description of the notice in lieu of a written notice.[390]

Regulation P states it is reasonable for a financial institution to expect that the consumer will receive actual notice in writing if it does any of the following:

- hand-deliver a printed copy of the notice to the consumer;
- mail a printed copy of the notice to the last known address of the consumer;
- for the consumer who conducts transactions electronically, post the notice on the electronic site and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service;
- for an isolated transaction with the consumer, such as an ATM transaction, post the notice on the ATM screen and require the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.[391]

387 12 C.F.R. § 1016.8(a).

388 12 C.F.R. § 1016.8(b).

389 12 C.F.R. § 1016.9(a).

390 12 C.F.R. § 1016.9(d).

391 12 C.F.R. § 1016.9(b)(1)(i)–(iv).

In addition, Regulation P states that it is reasonable for a financial institution to expect that a customer would receive actual notice of an annual privacy notice if (i) the customer uses the financial institution's website to access financial products and services electronically and agrees to receive notices at the website, and the financial institution posts its current privacy notice on the website in a clear and conspicuous manner; or (ii) if the customer has requested that the financial institution refrain from sending any information about the customer relationship and the current privacy notice remains available upon request.[392]

In some cases, financial institutions are permitted to provide a single notice that covers multiple financial institutions or multiple consumers. Financial institutions may provide a single notice from an institution and its affiliated third parties so long as the notice is accurate with respect to all the institutions.[393] When dealing with joint relationships,[394] financial institutions may provide a single notice to all consumers jointly, subject to certain limitations dependent on the type of financial institution providing the notice.[395]

C. Safeguards Rule

GLBA's Safeguards Rule establishes standards and requirements for the storage, security, and protection of NPI by financial institutions. The implementing regulations and related regulatory guidance provide financial institutions with elements of information security programs ("ISP") that should be tailored to the size and complexity of the specific company. Unlike the Privacy Rule, the CFPB does not have authority to write regulations and enforce requirements under the Safeguards Rule with regard to non-banks; that authority resides with the FTC.

1. Entities Covered

The Safeguards Rule applies to financial institutions as defined under GLBA and its implementing regulations.[396] The Safeguards Rule also applies to customer information that is "handled or maintained" by or on behalf of affiliates of financial institutions. In contrast to the Privacy Rule, which applies only limited provisions to financial institutions in situations in which

392 12 C.F.R. § 1016.9(c).

393 12 C.F.R. § 1016.9(f).

394 A joint relationship occurs when two or more consumers jointly obtain a financial product or service from a financial institution. *See* 12 C.F.R. § 1016.7(d).

395 *See* 12 C.F.R. § 1016.9(g)–(i). Credit unions providing a loan jointly to two or more consumers must provide an initial notice to each borrower or guarantor but may thereafter provide a single annual notice to all borrowers or guarantor jointly. *See* 12 C.F.R. § 1016.9(i)(2). Covered entities subject to FTC enforcement jurisdiction may provide a single notice to consumers jointly "unless one or more of the consumers requests separate notices." 12 C.F.R. § 1016.9(h).

396 15 U.S.C. § 6801(b).

they are acting as an agent on behalf of another financial institution rather than maintaining a direct customer relationship in their own right, the FTC's implementing regulations applies safeguards requirements to all financial institutions that hold customer information, regardless of whether they have such a direct relationship with a customer.[397] For a discussion of the definitions of "financial institution" and "affiliate" and the FTC's proposal to expand the definition of "financial institution," please see Section III.B.1.a. above.

In addition to safeguards requirements relating to financial institutions' protection of customer data they hold, the FTC's implementing regulations require financial institutions to oversee service providers by "[t]aking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards" for customer information and requiring service providers "by contract to implement and maintain such safeguards."[398] A "service provider" means "any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution."[399]

2. Data Covered

In contrast to the Privacy Rule, which applies to both consumer and customer information, the Safeguards Rule covers only customer information (e.g., where there is a continuing relationship between the consumer and financial institution). As a practical matter, however, the fact that the Safeguards Rule's coverage is somewhat narrower than the Privacy Rule's coverage may have little impact on the operational practices of financial institutions, as it is likely easier in most situations to apply consistent data security measures across all collected data rather than differentiating based on factors that may change over time. The implementing regulations define "customer information" as any record containing NPI about a customer "whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates." [400] The regulations use the same definition of "nonpublic personal information" as is used for purposes of the Privacy Rule.[401] Similarly, the interagency FFIEC's Safeguards Rule guidance references Regulation P's definition.[402] For a discussion of the meaning of NPI, please see Section III.B.2.

397 16 C.F.R. § 314.1(b).

398 16 C.F.R. § 314.4(d).

399 16 C.F.R. § 314.2(d).

400 16 C.F.R. § 314.2(b).

401 16 C.F.R. § 313.3(n).

402 *See, e.g.*, 12 C.F.R. § 225(I)(C)(2)(c), Appendix F.

3. Oversight

Rulemaking and enforcement authority for the Safeguards Rule is delegated to the FTC, OCC, FDIC, NCUA, CFTC, SEC, FRB, and state insurance authorities, with respect to the financial institutions under their jurisdiction.[403] The Safeguards Rule requires the prudential regulators to implement the applicable security standards through the interagency guidance process, whereas it instructs the FTC and SEC to proceed by rulemaking.[404] The Commodity Exchange Act separately requires the CFTC to prescribe regulations under GLBA and provides that persons subject to CFTC jurisdiction shall be treated as financial institutions under GLBA.[405] The prudential regulators through the FFIEC have issued guidelines for safeguarding customer information,[406] and the FTC, SEC, and CFTC have promulgated their respective rules.[407]

Unlike the Privacy Rule, for which significant rulemaking, supervision, and enforcement authority is vested in the CFPB, the CFPB has no role with respect to the Safeguards Rule.[408] Although the FTC has rulemaking and enforcement authority over the Safeguards Rule, the FTC does not have examination authority over the financial institutions under its jurisdiction. In effect, therefore, non-bank financial institutions will not receive supervisory scrutiny under the Safeguards Rule unless they are subject to a third-party service provider examination by the prudential banking regulators. Like the Privacy Rule, there is no private right of action under the Safeguards Rule, and civil penalties can vary depending on the agency bringing the enforcement action.[409]

403 15 U.S.C. § 6801(a)–(b). Although the FTC has broad authority to enforce the Safeguards Rule, it does not share the examination authority of its prudential regulators which limits its oversight capabilities.

404 *See* 15 U.S.C. § 6805(b); 66 Fed. Reg. 41162 (Aug. 7, 2001) (codified at 16 C.F.R. Part 314).

405 7 U.S.C. § 7b-2.

406 *See* 12 C.F.R. § 208, Appendix D-2; 12 C.F.R. § 30, Appendix B; 12 C.F.R. § 364, Appendix B; 12 C.F.R. § 225, Appendix F; and 12 C.F.R. § 748, Appendix A.

407 *See* 16 C.F.R. § 314; 17 C.F.R. § 248.30; 17 C.F.R. § 160.30.

408 Although the CFPB does not have authority to enforce the data security provisions of the Safeguards Rule, it has broad authority under UDAAP that can be, and has been, used to supervise and enforce data security issues. See Section VII.E.2. for additional information.

409 The availability and size of civil penalties vary by the authorizing statute of the agency bringing an enforcement action. For example, the FTC Act limits the FTC's authority to disgorgement and injunctive relief for initial violations of GLBA, whereas the FDI Act permits prudential regulators to seek civil penalties for entities under their supervision. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-19-196, CONSUMER DATA PROTECTION: ACTIONS NEEDED TO STRENGTHEN OVERSIGHT OF CONSUMER REPORTING AGENCIES 18–20 (2019), https://www.gao.gov/assets/700/697026.pdf; *see also* 12 U.S.C. § 1818(i)(2).

Commentary Box 14: Supervision and Enforcement Concerning Data Security

Although GLBA's safeguards provisions were designed to create a common baseline for data security requirements, nonbank financial institutions are not subject to ongoing supervision for compliance with GLBA standards unless they also act as third-party service providers to banks. Although the FTC can take enforcement action for GLBA safeguards violations, it has limited resources and generally focuses its investigations on situations in which data breaches or other problems have already come to light. As of 2019, the FTC had litigated or settled less than 70 information security cases involving both financial and nonfinancial companies under all sources of authority.[410]

As noted above, the CFPB has neither examination nor enforcement authority under the Safeguards Rule, even where it conducts examinations or enforcement activity in connection with Privacy Rule compliance. After the 2017 Equifax breach affecting almost 150 million consumers, the CFPB began conducting some information security-related examinations of nonbanks under its UDAAP authority. However, a 2019 Government Accountability Office report indicates that the CFPB is not routinely focusing on cybersecurity risks when prioritizing its supervision activities and may not be examining all companies that are subject to its authority as "larger participants" in the consumer reporting market. In particular, the GAO reported that the CFPB did not "routinely consider data security risks during their examination prioritization process and [has] not reassessed the process to determine how to incorporate such risks going forward."[411] In responding to the GAO's recommendation to focus more consistently on cybersecurity issues during the examination prioritization process, the CFPB "expressed concern with the scope of

410 *See Improving Data Security at Consumer Reporting Agencies: Hearing Before the Subcomm. on Economic and Consumer Policy of the H. Comm. On Oversight and Reform*, 116th Cong. (2019) (prepared testimony of Andrew Smith, Director of the Bureau of Consumer Protection, Federal Trade Commission), https://www.ftc.gov/system/files/documents/public_statements/1508935/p180101_ftc_testimony_re_oversight_house_12262019.pdf.

411 GOV'T ACCOUNTABILITY OFFICE, GAO-19-196, CONSUMER DATA PROTECTION: ACTIONS NEEDED TO STRENGTHEN OVERSIGHT OF CONSUMER REPORTING AGENCIES 26–27 (2019).

its statutory authority, such as its lack of authority to supervise for compliance with GLBA safeguard provisions."[412]

Prudential regulators have the power to examine third-party service providers, including with respect to data security.[413] Statistics are not available on how many or how frequently nonbank companies have been subjected to third-party service provider examinations by federal prudential regulators, although some agency leaders have expressed interest in providing more transparency about their third-party supervision programs as a way of lowering burden on smaller banks.[414] After the Equifax breach, the prudential regulators reportedly indicated that they did not have authority to subject consumer reporting agencies to third-party service provider examinations under the Bank Service Company Act (BSCA), although they have exercised such jurisdiction over at least one data aggregator for purposes of cybersecurity.[415]

4. Substantive Requirements

GLBA states that it is the policy of Congress that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[416] In furtherance of that policy, the Safeguards Rule requires each of the federal financial regulators other than the CFPB to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—(1) to insure the security and

412 GOV'T ACCOUNTABILITY OFFICE, GAO-19-196, CONSUMER DATA PROTECTION: ACTIONS NEEDED TO STRENGTHEN OVERSIGHT OF CONSUMER REPORTING AGENCIES 23–29, 33–34 (2019); GOV'T ACCOUNTABILITY OFFICE, GAO-18-559, DATA PROTECTION: ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 8–9, 25–27 (2018).

413 See Section V.B.2. for additional information on prudential oversight of third-party service providers.

414 Michelle Bowman, Governor of the Fed. Reserve Bd., Speech at the Conf. for Community Bankers, *Empowering Community Banks* (Feb. 10, 2020), https://www.federalreserve.gov/newsevents/speech/bowman20200210a.htm.

415 Kate Berry, *Is CFPB Punting on Equifax? It's Complicated*, Am. Banker (Feb. 5, 2018), https://www.americanbanker.com/news/is-cfpb-punting-on-equifax-its-complicated; Envestnet/Yodlee, Comment Letter in Response to the OCC/FDIC/FRB NPRM Regarding Enhanced Cyber Risk Management Standards, (Feb. 17, 2017), https://www.federalreserve.gov/SECRS/2017/February/20170227/R-1550/R-1550_022117_131738_464167618786_1.pdf.

416 15 U.S.C. § 6801(a).

confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[417]

a. FTC Regulations and Guidance

Consistent with GLBA, the FTC's implementing regulations require financial institutions to develop, implement, and maintain security measures to protect their customers' NPI.[418] The primary requirement under the FTC's implementing regulations is the development of an ISP. Each financial institution's ISP should be tailored to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of customer information—allowing for a variety of different programs to be developed based on a variety of company-specific factors.[419]

Although the Safeguards Rule allows financial institutions some flexibility to tailor an ISP based on the aforementioned factors, the FTC prescribes certain actions by a financial institution as fundamental to any successful ISP:

- Designate an employee or employees to coordinate the ISP;[420]
- Identify reasonable and foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.[421] The ISP's risk assessment must include the following considerations:
    - employee training and management;
    - information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

417 15 U.S.C §§ 6801(b), 6805(a).

418 16 C.F.R. § 314.1.

419 16 C.F.R. § 314.3(a). The main objectives of any ISP should be the following, which track the statutory objectives of the Safeguards Rule: (1) ensure the security and confidentiality of customer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. 16 C.F.R. § 314.3(b).

420 16 C.F.R. § 314.4(a).

421 16 C.F.R. § 314.4(b).

- detecting, preventing and responding to attacks, intrusions, or other system failures.

- Design and implement a safeguards program that controls any identified risks, as well as regularly tests and monitors the effectiveness of key controls, systems, and procedures; [422]

- Select service providers that can maintain appropriate safeguards and contractually obligate them to maintain those safeguards, and oversee their handling of customer information;[423]

- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[424]

The FTC's website also lists a variety of measures that can be included in an ISP, depending on the nature of the business.[425] The FTC's regulations are intended to permit flexibility to minimize the compliance burden on companies.[426] However in March 2019, the FTC sought comment on proposed amendments to the Safeguards Rule, which would add more specific requirements that financial institutions must include in an ISP, including the following:

- designating a single qualified individual to serve as the Chief Information Security Officer;

- conducting information security risk assessments;

- conducting periodic risk-based assessments of service providers;

- initiating multi-factor authentication for any individual accessing customer information or internal networks that contain customer information;

- encrypting all customer information in transit and at rest; and

422 16 C.F.R. § 314.4(c).

423 16 C.F.R. § 314.4(d).

424 16 C.F.R. § 314.4(e).

425 Fed. Trade Comm'n, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

426 67 Fed. Reg. 36483, 36490 (May 23, 2002) (codified at 16 C.F.R. Part 314).

- creating an incident response plan for potential breaches.[427]

Commentary Box 15: Strengthening Nonbank Safeguards Standards

Although banks have long complained that the FTC's Safeguards Rule is not as detailed or rigorous as the prudential agencies' cumulative information security guidance,[428] the FTC's 2019 proposals draw on the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies and the National Association of Insurance Commissioners Insurance Data Security Model Law, rather than FFIEC materials.[429] Two commissioners dissented from the decision to issue the proposal, arguing that it was premature in light of congressional discussions about data legislation and flawed in various respects.[430]

Many bank stakeholders and consumer advocates have urged the FTC to further harmonize the proposal with FFIEC guidance, at least for nationwide consumer reporting agencies and/or large fintechs.[431] Many nonbank financial institution commenters have argued that various aspects of the proposal are too rigid and burdensome, particularly for smaller companies.[432]

427 84 Fed. Reg. 13158 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. Part 314). As of the publication date of this paper, no final rule had been issued. Financial institutions that maintain customer information on fewer than 5,000 consumers would be exempt from certain proposed requirements. These proposed regulations adopt some of the "concrete and specific requirements" from the New York Department of Financial Services' cybersecurity regulations and the National Association of Insurance Commissioners' Model Data Security Law. *See* Nat'l Consumer Law Ctr., Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (Aug. 5, 2019), https://www.regulations.gov/document?D=FTC-2019-0019-0058.

428 *See, e.g.*, THE CLEARING HOUSE, ENSURING CONSISTENT CONSUMER PROTECTION FOR DATA SECURITY: MAJOR BANKS VS. ALTERNATIVE PAYMENT PROVIDERS (2015), https://bpi.com/wp-content/uploads/2018/07/tchconsumer-protection-for-data-security-august-2015-final.pdf.

429 84 Fed. Reg. 13158, 13163 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. Part 314).

430 84 Fed. Reg. 13158, 13176–77 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. Part 314).

431 *See, e.g.*, Bank Pol'y Inst., Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (Aug. 2, 2019), https://www.regulations.gov/document?D=FTC-2019-0019-0039; The Clearing House, Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (Aug. 5, 2019), https://www.regulations.gov/document?D=FTC-2019-0019-0049; Nat'l Consumer Law Ctr., Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (Aug. 2, 2019).

432 See, e.g., Nat'l Automobile Dealers Ass'n, Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (Aug. 2, 2019), https://www.regulations.gov/document?D=FTC-2019-0019-0046; Elec. Transactions Ass'n, Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (July 31, 2019), https://www.regulations.gov/document?D=FTC-2019-0019-0027; Consumer Data Info. Ass'n, Comment Letter in Response to FTC's NPRM Regarding the Safeguards Rule (Aug. 2, 2019), https://www.regulations.gov/document?D=FTC-2019-0019-0036.

The FTC held a daylong virtual hearing on the proposal in July 2020, with a particular focus on gathering more information about the cost and benefits of particular elements and their scalability for smaller firms.[433]

b. FFIEC Guidance

The FFIEC's interagency guidance requires financial institutions overseen by the prudential banking regulators to develop standards for safeguarding customer information and develop and to implement an ISP to protect customer NPI. The FFIEC's original guidance largely mirrored the FTC's rules, with a few differences such as the FFIEC's more specific requirements regarding the ongoing monitoring by financial institutions of service providers' security practices and board-level responsibilities. Under FFIEC guidance, the required components of an ISP include:

- Involvement of the Board of Directors – to approve, oversee the development, implementation, and maintenance of the ISP;

- Assessment of Risk – (i) identify reasonable and foreseeable threats, (ii) assess the likelihood of potential damage, and (iii) assess the sufficiency of policies, procedures, customers information systems, and other controls;

- Management and Control of Risk – (i) design an ISP to control identified risks commensurate with the sensitivity of information and complexity and scope of the bank holding company's activities, (ii) train staff to implement the ISP, and (iii) regularly test the key controls, systems and procedures from the ISP.[434]

- Oversight of Service Provider Arrangements – (i) exercise due diligence in selecting service providers, (ii) require service providers to implement appropriate measures

433 Transcript, Fed. Trade Comm'n, GLBA Safeguards Workshop (July 13, 2020), https://www.ftc.gov/system/files/documents/public_events/1567141/transcript-glb-safeguards-workshop-full.pdf.

434 The FFIEC guidance provides a list of measures that may or may not be appropriate to include in an ISP depending on the company's size and complexity. These include measures such as "[a]ccess restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals." 12 C.F.R. § 225, Appendix F (III)(C)(b). *See* 12 C.F.R. § 225, Appendix F (III)(C) for a complete list of all recommended measures.

designed to meet the FFIEC guidelines, and (iii) if indicated by a risk assessment, monitor its service providers to confirm they have satisfied their obligations

- Adjustment of the Program – monitor, evaluate, and adjust its ISP in light of any relevant changes in technology, sensitivity of customer information, internal/external threats, and changes in its business structure;

- Reports to the Board – report to the institution's Board of Directors or an appropriate committee of the Board of Directors at least annually, describing overall status of the ISP as well as any issues or recommendations.[435]

The FFIEC has issued a supplement to the Security Guidelines that sets forth additional interagency guidance on response programs for handling unauthorized access to customer information and customer notice.[436] That supplementary guidance requires that the response program must include the following actions:

- assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;

- notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;

- consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;

- taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence;

435 12 C.F.R. § 225, Appendix F (III).

436 12 C.F.R. § 225, Supplement A to Appendix F.

- notifying customers when warranted.[437]

c. SEC and CFTC Regulations and Guidance

The SEC and CFTC regulations are significantly abridged compared to the FTC's regulations and the FFIEC's interagency guidance. The SEC and CFTC regulations mirror the statutory language of the Safeguards Rule and require the entities under their jurisdiction to adopt "policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."[438]

The SEC has issued various guidance related to the Safeguards Rule, noting in risk alerts certain concerns raising Safeguards Rule compliance risks.[439] The CFTC also issued "best practices" guidance for complying with the Safeguards Rule in 2014.[440] This guidance is generally consistent with the guidance contained in regulations promulgated by the FTC. One notable difference requires that, at least once every two years, the covered entity arranges for an independent party to test and monitor the controls, systems, policies, and procedures.[441] The CFTC, similar to the FFIEC, also recommends financial institutions within its jurisdiction design and implement policies and procedures for incidents involving unauthorized access and disclosure of personal information.[442]

IV. Fair Credit Reporting Act (FCRA)

437 12 C.F.R. § 225, Supplement A(II)(A) to Appendix F. The guidelines note that it is the responsibility of a financial institution, or a service provider on its behalf, to contact customers if the unauthorized access involves customers information system maintained by an institution's service provider. See the interagency guidelines at 12 C.F.R. § 225, Supplement A(III) to Appendix F for additional details on the content and timeline of any required notice.

438 17 C.F.R. §§ 248.30(a), 160.30(a).

439 *See, e.g.*, Securities & Exchange Comm'n, Risk Alert on Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies (Apr. 16, 2019), https://www.sec.gov/ocie/announcement/ocie-risk-alert-regulation-s-p; Securities & Exchange Comm'n, Risk Alert on Safeguarding Customer Records and Information in Network Storage—Use of Third-party Security Features (May 23, 2019), https://www.sec.gov/ocie/announcement/risk-alert-network-storage.

440 COMMODITIES FUTURES TRADING COMM'N, STAFF ADVISORY NO. 14-21, GRAMM-LEACH-BLILEY ACT SECURITY SAFEGUARDS (2014), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

441 COMMODITIES FUTURES TRADING COMM'N, STAFF ADVISORY NO. 14-21, GRAMM-LEACH-BLILEY ACT SECURITY SAFEGUARDS 3 (2014).

442 COMMODITIES FUTURES TRADING COMM'N, STAFF ADVISORY NO. 14-21, GRAMM-LEACH-BLILEY ACT SECURITY SAFEGUARDS 4 (2014).

A. Introduction

Enacted in 1970, the Fair Credit Reporting Act ("FCRA") was established to promote fairness and accuracy in the information held by consumer reporting agencies ("CRAs") and entities contributing to and using information received from CRAs. FCRA is best known for its regulation of consumer reports, which are typically composed from aggregated data pertaining to consumers' credit history, payment patterns, and public records. This information is frequently used to assess whether, and at what cost, a consumer will be able to obtain credit or to qualify for insurance or employment. FCRA is also an important consumer tool that "provides consumers with the right to access their own data that has been used to make such decisions, and if it is erroneous, to correct it."[443]

FCRA was originally enacted in response to the increasing availability of credit records and complaints surrounding investigations into consumers' financial histories when applying for financial products.[444] FCRA has been amended on several occasions since its passage, including in 1996 to relax information sharing restrictions among affiliated entities and place new duties on users of consumers reports and furnishers of information to CRAs;[445] in 2003 to add provisions intended to reduce identity theft and require nationwide CRAs to provide consumers with free annual access to consumer reports;[446] and in 2010 to amend jurisdiction of FCRA as discussed below.[447]

443 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 66 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

444 *See Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System: Hearing Before the H. Comm. on Fin. Servs.*, 116th Cong. (2019) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group), https://www.congress.gov/116/meeting/house/108945/witnesses/HHRG-116-BA00-Wstate-MierzwinskiE-20190226.pdf; *see also Fair Credit Reporting: Hearing on H.R. 16340 Before the H. Subcomm. on Consumer Affairs*, 91st Cong. (1970) (statement of Rep. Leonor Sullivan, Chairman, H. Subcomm. on Consumer Affairs) (leading up to FCRA's passage stating that "we cannot continue to countenance the slipshod practices in credit reporting which destroy the reputations of innocent people seeking credit, insurance, or employment").

445 Consumer Credit Reporting Reform Act of 1996, *adopted* as Subtitle D, Chapter 1, Omnibus Consolidated Appropriations Act, Pub. L. No. 104-208, 110 Stat. 3009 (1996) (codified at 15 U.S.C. § 1681s-2).

446 Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, 77 Stat. 1952 (2003) (codified at 15 U.S.C. § 1601 *et seq.*); 15 U.S.C. §§ 1681c-1, 1681c-2, 1681j.

447 Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*); *see* 12 U.S.C. §§ 5481(12)(F), 5581.

B. Entities Covered

FCRA and its implementing regulation, Regulation V,[448] applies to entities involved in the creation, transmission, and use of consumer reports.[449] In particular, the following types of entities are governed by FCRA: (i) CRAs, including nationwide CRAs; (ii) furnishers and transmitters of information; and (iii) users of consumer reports, such as providers and marketers [450] of financial products, employers, and landlords.[451] A single entity may fall into more than one of these categories depending on how it uses consumer reports and whether it provides such data to third parties and for what purposes. Given the expansive set of use cases of consumer reports, FCRA has an extremely broad reach and covers a wide range of entities, including many entities not typically associated with financial services.

1. CRAs and Nationwide CRAs

One of the primary purposes of FCRA is to regulate the activities of CRAs, which are defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling[452] or evaluating[453] consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."[454]

Nationwide CRAs are defined under FCRA as CRAs that "regularly engage[] in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each

448 Codified at 12 C.F.R. Part 1022.

449 See Section IV.C. for further information on what constitutes a consumer report.

450 As discussed below in Section IV.E.1.a., marketing is generally not considered a permissible purpose for obtaining a consumer report; however, FCRA does permit the use of consumer reports in limited cases, such as marketing by affiliates and prescreened, firm offers of credit.

451 This list is not comprehensive of all entities that are subject to FCRA. This paper focuses on the types of entities most relevant to issues relating to financial data; however, FCRA regulates the use of consumer information in a broad range of commercial activities, such as employment and rental screenings.

452 FTC guidance provides that "assembling" means "gathering, collecting, or bringing together consumer information such as data obtained from CRAs or other third parties, or items provided by the consumer in an application." FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 29 (2011) (emphasis added), https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting-act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

453 FTC guidance provides that "evaluating" means "appraising, assessing, determining or making a judgment on such information." FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 29 (2011) (emphasis added).

454 15 U.S.C. § 1681a(f). The term "person" is defined broadly as "any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity." 15 U.S.C. § 1681a(b).

of the following regarding consumers residing nationwide: (i) Public record information; and (ii) Credit account information from persons who furnish that information regularly and in the ordinary course of business."[455] There are three primary nationwide CRAs: Equifax, TransUnion, and Experian. The distinction between CRAs and nationwide CRAs is important as nationwide CRAs are subject to additional requirements, such as the obligation to provide free credit reports to consumers on an annual basis.[456]

2. Data Furnishers

A furnisher is "an entity that furnishes information relating to consumers to one or more consumer reporting agencies for inclusion in a consumer report."[457] However, there are some important exclusions from that definition; for example, a consumer is not a furnisher when the consumer shares information about himself or herself.[458] The same financial institutions that use information may also act as furnishers by providing information to CRAs, e.g., credit line amounts, account closures, and payment history.[459] In an effort to ensure the information provided to CRAs is accurate and current, FCRA and its implementing regulations place certain responsibilities on furnishers, such as the duty to investigate and correct potential inaccuracies.[460]

3. Data Users

Data users are entities that obtain consumer reports from CRAs. Due to FCRA's broad application to both financial services as well as other general commerce such as employment and rental screening, the types of data users covered by the statute are varied. Financial institutions and other financial services firms become data users when they obtain consumer reports for use in determining whether to approve an application for a checking account, credit extension, or insurance policy.[461] Employers also use consumer reports—which can include criminal and other public records such as bankruptcy filings, and records of civil court procedures and judgments—to assist in the hiring process.[462] Entities, including financial

455 15 U.S.C. § 1681a(p).

456 See Section IV.E.2.b. for a further discussion of the free credit report requirement.

457 12 C.F.R. § 1022.41(c).

458 The definition of "furnisher" excludes entities that (i) provide information to CRAs solely to obtain consumer reports; (ii) are acting as CRAs; (iii) are consumers to whom the furnished information pertains; or (iv) are individuals that provide information about the consumer upon a request from a CRA. 12 C.F.R. § 1022.41(c).

459 *See* 15 U.S.C. § 1681s-2.

460 *See* 15 U.S.C. § 1681s-2; 12 C.F.R. § 1022.43.

461 The term "financial institution" under FCRA means "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer." 15 U.S.C § 1681a(t).

462 15 U.S.C. §§ 1681b(a)(3)(B), 1681b(b).

institutions, may also utilize information in credit reports to engage in certain marketing activities, subject to certain limitations discussed below.[463] FCRA's list of permissible purposes attempts to safeguard the sensitive information contained in consumer reports by limiting when data users can obtain reports and resell consumer report information.[464]

Commentary Box 16: Application of CRA and Furnisher Definitions to New Business Models

The increasing diversity of new participants in the financial services ecosystem raises questions about the applicability of FCRA and its implementing regulations to different types of market actors. For example, there is a lack of consensus around whether and when newer types of intermediaries, such as data aggregators and data brokers, should be deemed to be CRAs and when data holders, such as banks, should be viewed as furnishers by providing data to such intermediaries. Whether data transmitted by a data source constitutes a "consumer report" also has implications for users of that data in terms of adverse action notice requirements.[465] Some data aggregators have embraced their role as CRAs,[466] while others have taken the position that they are not CRAs and that the data they transmit are not consumer reports.[467] The latter argue that merely acting as the "pipes" to transmit data at the direction of a consumer without taking a more active role in analyzing and repackaging the data should not itself make the data aggregator a consumer reporting agency.[468] In addition, some stakeholders have argued that consumer-initiated sharing of the consumer's own data through a third-party data aggregator should not subject the original data source to the obligations of a

463 *See* 15 U.S.C. §§ 1681a, 1681b for more information on permissible uses of consumer reports in marketing.

464 *See* 15 U.S.C. §§ 1681b, 1681e(e). In order to procure a consumer report for resale, a person must disclose the identity of the report's end-user and each permissible purpose to the CRA. 15 U.S.C. § 1681e(e)(1). Additionally, FCRA specifies certain compliance procedures required for reselling. 15 U.S.C. § 1681e(e)(2). See Section IV.E.1.a. for information on permissible purposes.

465 *See* 15 U.S.C. § 1681m.

466 *See e.g.* Finicity, Consumer Reporting Agency, https://www.finicity.com/consumer-reporting-agency/ (last visited June 25, 2020).

467 *See, e.g.*, Plaid, Developer Terms of Use, https://plaid.com/legal/terms-of-use/ (last visited June 25, 2020).

468 *See* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 87 (2020) (referencing informal guidance by FTC staff on a related point), https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf.

furnisher.[469] Consumer advocate groups, on the other hand, have argued that data aggregators should be considered CRAs when they transmit data to be used for one of the designated permissible purposes under FCRA and Regulation V, even if the original data holder—such as the account-holding financial institution—is not furnishing data to the intermediary.[470]

C. Data Covered

FCRA generally focuses on the creation, use, disclosure, and accuracy of consumer reports. "Consumer reports" are defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under" FCRA's list of permissible purposes.[471] Given the broad definition, whether data constitutes a "consumer report"—and is therefore subject to regulation under FCRA—depends on whether the data bears on one of the characteristics listed above, the purposes for which the data is collected and expected to be used, and whether the data is transferred via an intermediary meeting the definition of a CRA as described above to the end user.[472]

469 *See* Kwamina Williford and Brian Goodrich, *Why Data Sources Aren't Furnishers Under Credit Report Regs*, Law360 (Sept. 25, 2019), https://www.law360.com/articles/1202240/why-data-sources-aren-t-furnishers-under-credit-report-regs; *see also* Chi Chi Wu, Nat'l Consumer Law Ctr., Submission to the CFPB Data Symposium (2020), at 7–8, https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf (noting stakeholder arguments and gathering sources).

470 Chi Chi Wu, Nat'l Consumer Law Ctr., Submission to the CFPB Data Symposium (2020), at 7–8.

471 U.S.C. § 1681a(d)(1). FCRA outlines a different definition for investigative consumer reports, which are outside the scope of this paper. 15 U.S.C. § 1681a(e).

472 FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 21 (2011). Certain data is not covered under the definition of a "consumer report" where it did not pass from a CRA to a creditor, even if the data otherwise meets the definition and is in fact used for credit decisioning. For example, experiential data compiled by a creditor that is used to re-underwrite a previous customer or passed directly to another creditor without going through a third party is not a consumer report.

A consumer report obtained from a CRA can include personally identifiable information (e.g., social security numbers, name, address), credit account information (e.g., date of account opening, credit limit or loan amount, payment history, current status), credit inquiry information (e.g., a list of every person who accessed an individual's credit report within the last two years), collections information (e.g., accounts that have been referred to a third-party debt collector or sold to a debt buyer) and public records (e.g., information from federal, state and county courts, including bankruptcies). FCRA also applies in commercial transactions when a consumer report is obtained if the consumer will be personally liable for a debt, such as when a sole proprietor or other business principal guarantees an extension of credit to the company.[473]

Anonymized data has generally been considered to fall outside the definition of a "consumer report," though regulatory guidance suggests that information about a particular person or group of persons that is compiled and used for the purpose of evaluating their creditworthiness is not exempted from the definition simply because it does not contain direct identifiers.[474] Conversely, a list of names and contact information will be treated as a series of consumer reports even if it does not contain other data if the list is compiled based on specific eligibility criteria, for instance "that every name on the list has at least one active trade line [and] updated within six months . . . ."[475] As noted elsewhere in this paper, the extent to which aggregated and anonymized data may be traced to individual consumers is an evolving area and presents challenges to exclusions related to de-identification in the FCRA and GLBA contexts.[476]

FCRA excludes from the definition of "consumer reports" the following specific types of data and sharing practices [477]:

- a report that only contains information related to transactions or experiences between the consumer and the person making the report;[478]

473 *See* FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 10 (2011). A consumer report obtained from a CRA remains a consumer report even if used for purposes of a commercial transaction. *See id*. at 21 (citing to Fed. Trade Comm'n, Advisory Opinion Letter 07-26-00 (July 26, 2000), https://www.ftc.gov/policy/advisory-opinions/advisory-opinion-tatelbaum-07-26-00).

474 FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? UNDERSTANDING THE ISSUES 16–17 *FN* 85 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 20 (2011); *see also* CHET WIERMANSKI & STEPHANIE M. WILSHUSEN, FED. RESERVE BANK OF PHILADELPHIA—PAYMENTS CARD CTR., EXPLORING THE USE OF ANONYMIZED CONSUMER CREDIT INFORMATION TO ESTIMATE ECONOMIC CONDITIONS: AN APPLICATION OF BIG DATA 12 (2015), https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2015/d-2015_big-data.pdf?la=en.

475 FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 10 (2011).

476 See Commentary Box 10 for a discussion of considerations related to de-identification of consumer data.

477 An exception pertaining to investigative reports has been excluded from this list as it does not bear on financial data matters.

478 15 U.S.C. § 1681a(d)(2)(A)(i).

- a report containing transactional or experience information shared between persons with common ownership or affiliated by common control;[479]

- a report shared among affiliates that includes other information (such as information about accounts held at different institutions included in an application), if notice and opt-out rights were provided to the consumer before sharing with an affiliate;[480]

- any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device;[481] and

- any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the required disclosures to the consumer.[482]

Although certain information is not considered a "consumer report" under FCRA, the statute may still regulate activities related to that data, such as adverse action notices. For example, if an affiliate receives transactional information specifically excluded from the definition of a consumer report, that affiliate may still be required to provide an adverse action notice if relying on that information to make a credit decision.[483]

D. Oversight

Rulemaking authority under FCRA was limited historically and divided among the FTC, the prudential bank regulators, and the NCUA.[484] In 2010, DFA vested the CFPB with rulemaking authority to implement nearly all provisions of the statute, except for limited provisions related to information security that remained with the FTC and prudential regulators.[485] The CFPB is also

479 15 U.S.C. § 1681a(d)(2)(A)(ii). See Section IV.E.1.c. for further discussion of affiliate transactional data sharing.

480 15 U.S.C. § 1681a(d)(2)(A)(ii). This disclosure and opt out is contemplated in GLBA model form found in Regulation P. 12 C.F.R. § 1016. Any entity not subject to GLBA compliance obligations needs to provide consumers with a separate disclosure and opt-out prior to communicating this type of information to an affiliate.

481 15 U.S.C. § 1681a(d)(2)(B).

482 15 U.S.C. § 1681a(d)(2)(C).

483 15 U.S.C. § 1681m(b)(2).

484 *See* 76 Fed. Reg. 79307 (Dec. 21, 2011) (codified at 12 C.F.R. Part 1022).

485 *See* Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified at 12 U.S.C. § 5301 *et seq.* and 15 U.S.C. § 1601 *et seq.*). The CFPB's authority also does not cover the disposal and red flag regulations, for which the CFPB does not have rulemaking, supervision, or enforcement authority under FCRA. See 15 U.S.C. §§ 1681m(e), 1681w.

able to use its supervisory and enforcement authorities to examine "covered persons" for compliance with all provisions subject to its rulemaking jurisdiction.[486] The changes enacted by DFA represented an important shift with respect to the supervision of FCRA compliance across the financial services ecosystem. Unlike banks, which can be supervised for compliance with FCRA as data furnishers and data users by the prudential banking regulators, prior to the enactment of DFA and the creation of the CFPB, CRAs and non-bank furnishers and credit-report users had generally not been subject to federal regulatory supervision.[487]

In 2011 the CFPB republished previously-issued FCRA regulations under its new rulemaking authority as Regulation V.[488] The FTC retains its FCRA enforcement authority and shares such authority with the CFPB with respect to non-bank covered persons under CFPB jurisdiction.[489] The prudential bank regulators maintain their FCRA supervisory and enforcement authority for depository institutions with $10 billion or less in total assets.[490] States are also entitled to bring actions to enforce FCRA for actual or suspected violations in their states.[491]

Civil liability, including through a private cause of action, is available for noncompliance with certain provisions of FCRA.[492] For willful noncompliance, liability per individual is available up to $1,000 for actual damages, with punitive damages permitted.[493] Liability for negligent noncompliance is limited to actual damages incurred by an individual.[494]

E. Substantive Requirements

FCRA imposes a variety of responsibilities on CRAs, nationwide CRAs, data furnishers, and data users. These requirements fall into three primary categories: (i) privacy

---

486 See 15 U.S.C. §§ 5514, 5516.

487 *See Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System: Hearing Before the H. Comm. on Fin. Servs.*, 116th Cong. (2019) (statement of Edmund Mierzwinski, Consumer Program Director, U.S. Public Interest Research Group).

488 12 C.F.R. § 1022.

489 15 U.S.C. §§ 1681s(a), 1681s(b)(1)(H). Although the FTC no longer has rulemaking authority over the majority of FCRA, it retained rulemaking authority over red flag guidelines and the disposal of records. The FTC's red flag guidelines, found at 16 C.F.R. § 681.1, require specific businesses and organizations to "implement a written identity theft program designed to detect 'red flags' of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage." *See* Fed. Trade Comm'n, *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*, https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business (last visited April 26, 2020).

490 15 U.S.C. § 1681s(b). As noted above, prudential regulators and the FTC retained rulemaking and enforcement authority over FCRA's disposal and red flags rules. *See* 15 U.S.C. §§ 1681m(e), 1681w.

491 15 U.S.C. § 1681s(c).

492 *See* 15 U.S.C. §§ 1681n, 1681o.

493 *See* 15 U.S.C. § 1681n(a).

494 15 U.S.C. § 1681o(a).

protections—covering the information contained in consumer reports and the conditions under which they can be obtained; (ii) accuracy protections—addressing consumer rights to notice in the event of adverse actions and data accuracy requirements for CRAs and furnishers; and (iii) security protections—concerning compliance requirements, consumer alerts, and identity theft protections.

1. Privacy

FCRA imposes a variety of privacy obligations on CRAs and data users by regulating the permissible purposes for which consumer reports can be obtained, the kinds of information that can be contained in a consumer report, and the circumstances under which consumer report information can be used for marketing.

a. Permissible Purposes for Obtaining Consumer Reports

CRAs compile and maintain a significant amount of sensitive information about consumers. This information is used to determine creditworthiness for a variety of products, such as deposit accounts, insurance, utilities, and loans. FCRA governs access to this information to ensure users obtain information only for permissible purposes. FCRA provides that CRAs may furnish consumer reports under the following circumstances and no others.[495]

Specific Types of Financial Transactions

The statute specifically identifies the following types of financial transactions, in addition to providing broader language that may also be invoked by financial services providers as discussed further below:

- credit transactions involving the consumer and involving the extension of credit to, or review or collection of an account of, the consumer;[496]
- underwriting of insurance;[497]
- valuation of, or assessments of credit or prepayment risks associated with, existing credit obligations by a potential investor or servicer or current insurer.[498]

495 15 U.S.C. § 1681b(a).

496 15 U.S.C. § 1681b(a)(3)(A).

497 15 U.S.C. § 1681b(a)(3)(C).

498 15 U.S.C. § 1681b(a)(3)(E).

Other Enumerated Uses

Consumer reports may also be provided by CRAs under the following circumstances:

- for employment purposes;[499]
- in response to a court order or subpoena;[500]
- in connection with a determination of a consumer's eligibility for a license or other benefit where applicant's financial responsibility or status is a required factor;[501]
- executive departments or agencies in connection with the issuance of government-sponsored individually billed travel charge cards;[502]
- specific circumstances related to child support;[503]
- to the FDIC or NCUA if related to their roles as conservator, receiver, or liquidating agent for distressed depository institutions or credit unions.[504]

Other Business Transactions

Consumer reports can be provided by a CRA to a person the CRA has reason to believe "otherwise has a legitimate business need for the information (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an account to determine whether the consumer continues to meet the terms of the account."[505] This provision is frequently invoked in connection with checking account and tenant screening activities.[506] Given its broad language, this provision affords CRAs and data users significant latitude to expand the potential use cases for consumer reports.

499 15 U.S.C. § 1681b(a)(3)(B).

500 15 U.S.C. § 1681b(a)(1).

501 15 U.S.C. § 1681b(a)(3)(D).

502 15 U.S.C. § 1681b(a)(3)(G).

503 15 U.S.C. § 1681b(a)(4)–(5).

504 15 U.S.C. § 1681b(a)(6).

505 15 U.S.C. § 1681b(a)(3)(F).

506 *See* FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 48 (2011).

Consumer Consent

Consumer reports can be provided by a CRA "in accordance with the written instructions of the consumer to whom it relates."[507] This provision acknowledges the consumer's ability to consent to the release of information about themselves, but also allows for a significant expansion in the scope of circumstances under which consumer reports may be furnished. Although FCRA provides some guidance related to consent in an employment context,[508] both the statute and implementing regulations are silent with respect to what requirements are necessary to adequately capture consumer consent for sharing of consumer reports. As noted elsewhere in this paper, issues surrounding the lack of clarity on the consent parameters can lead to inconsistent practices throughout the industry.[509]

The statute lists permissible purposes but does not require CRAs to provide consumer reports. Because the statute precedes the list of permissible purposes with "and no other," CRAs may not provide, and data users may not use, a consumer report for any reason outside of those listed. For example, CRAs cannot provide access to consumer financial data for reasons such as curiosity, acceptance of a free trial, or general law enforcement requests.[510] FCRA and related regulations require that CRAs and data users employ procedures, controls, and other safeguards to ensure that regulated entities provide, obtain, and use consumer reports for permissible purposes only.[511]

Commentary Box 17: Purpose Restrictions vs. Notice and Consent

Both in the U.S. and other jurisdictions, data protection laws frequently rely on a combination of purpose restrictions and notice and consent to define what types of data collection, sharing, and/or usage are permissible. But as evidence is mounting that consumers may be overwhelmed by the volume of privacy notices, consent forms, and related material that they are receiving—particularly in online

507 15 U.S.C. § 1681b(a)(2).

508 *See* 15 U.S.C. § 1681b(b)(2).

509 See Commentary Box 11 for a discussion of considerations related to the scope of consumer consent.

510 There are certain exceptions for disclosure to governmental agencies for counterterrorism purposes. *See* 15 U.S.C. § 1681v.

511 FCRA sets forth compliance procedures for covered entities. *See* 15 U.S.C. § 1681e.

settings—there is increasing debate over how these mechanisms interact with each other and how to strike an optimal balance between them.[512]

For example, FCRA relies primarily on permissible purpose restrictions, but contains a catchall permitting other uses of consumer reports with consumer consent.[513] GLBA creates a notice and opt-out consent structure to govern financial institutions' sharing of consumer data with nonaffiliated companies, but also provides a long list of sharing activities for which notice and/or consent are not required and a further exception for sharing with the affirmative authorization of a consumer.[514] The European Union's General Data Protection Regulation also uses both mechanisms; for instance, by permitting collection and use of data with consumer consent or pursuant to other enumerated purposes.[515]

Using both approaches in the same statute provides flexibility as data activities evolve, but can create effectiveness concerns where particular elements are not built out in sufficient detail and contribute more generally to risks of information overload and "consent fatigue." For example, if permissible purpose standards are vague, companies may decide to seek consent simply to provide a backstop against liability. And where standards for obtaining meaningful consent are vague, they may create opportunities to evade purpose restrictions. For these and other reasons,

512 *See, e.g.*, FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 108–13 (2020); Aleecia M. McDonald & Lorrie Faith Cranor, *The Costs of Reading Privacy Policies*, 4:3 J. OF L. & POL'Y FOR THE INFO. SOC'Y 543 (2008), https://kb.osu.edu/handle/1811/72839 (calculating that U.S. residents encounter an average of 1462 privacy policies per year, representing costs in time of approximately 244 hours and $3,534 per internet user).

513 15 U.S.C. § 1681b. Similar to the exception for data sharing under the GLBA Privacy Rule with the consent or at the direction of consumers, the FCRA exception does not specify particular process requirements for obtaining consumer consent. See Commentary Box 6 and Commentary Box 11 for further discussion of consent process issues under Section 1033 and GLBA, respectively. FCRA also requires affirmative consent in the employment context. The law and regulatory guidance do address some procedural issues in that context, but are silent as to whether employers can take negative actions against an applicant or employee who refuses to authorize access. While informal guidance materials also emphasize that the statute does not specifically authorize such actions, the law has been generally interpreted to permit employers to condition job offers on credit report checks. *Id.* § 1681b(b); FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 51–52 (2011).

514 15 U.S.C. §§ 6802, 6803.

515 European Union General Data Protection Regulation, Art. 6(1) (2016). The purposes include processing that is necessary for the performance of certain contracts, for compliance with legal obligations, or for the legitimate interests of the organization, so long as those interests are not overridden by the interests or fundamental rights of the data subject.

some regulators and private stakeholders are expressing growing concern about over-reliance on notice and consent relative to purpose restrictions.[516]

b. Limitations on Information Contained in Consumer Reports

FCRA limits the type of information that CRAs can include in consumer reports transmitted to data users to safeguard sensitive information and ensure transmitted information is accurate and current. Except in limited circumstances, the following information cannot be included in consumer reports provided to data users:

- Chapter 11 bankruptcies that occurred at least ten years ago;
- civil suits, civil judgments, and records of arrest that occurred at least seven years ago;
- paid tax liens that were paid seven years before the report;
- accounts placed for collection or charged off that occurred at least seven years ago;
- any other adverse item of information, other than records of convictions of crimes that occurred at least seven years ago;[517]

516 Kaitlin Asrow, Fed. Reserve Bank of San Francisco, *The Role of Individuals in the Data Ecosystem: Current Debates and Considerations for Individual Data Protection and Data Rights in the U.S.,* FINTECH EDGE 58 (June 3, 2020), https://www.frbsf.org/banking/publications/fintech-edge/2020/june/role-individuals-data-ecosystem/; DAVID MEDINE & GAYATRI MURTHY, CONSULTATIVE GRP. TO ASSIST THE POOR, MAKING DATA WORK FOR THE POOR: NEW APPROACHES TO DATA PROTECTION AND PRIVACY (2020), https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor.pdf; *Banking on Your Data: The Role of Big Data in Financial Services, Hearing Before H. Comm. On Fin. Servs., Task Force on Financial Technology*, 116th Cong. (Nov. 21, 2019) (testimony of Lauren Saunders, Associate Director of the National Consumer Law Center) at 12–13, https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf; Caitlin Chin & Maria Odell, *Highlights: Commissioners Discuss the Future of the FTC's Role in Privacy*, BROOKINGS INSTITUTION: TECHTANK (Nov. 5, 2019), https://www.brookings.edu/blog/techtank/2019/11/05/highlights-commissioners-discuss-the-future-of-the-ftcs-role-in-privacy/; Luis Alberto Montezuma & Tara Taubman-Bassirian, *How to Avoid Consent Fatigue*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 29, 2019), https://iapp.org/news/a/how-to-avoid-consent-fatigue/; United Kingdom Info. Comm'r's Office, *Legitimate Interests: When Can We Rely on Legitimate Interests?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (last visited Sept. 15, 2020).

517 An exception to the first five items is permitted if the consumer report is related to (a) a credit transaction likely to involve $150,000 or more in principal; (b) underwriting life insurance with a likely face value of $150,000 or more; and (c) the employment of any individual at an annual salary which equals, or which may reasonably be expected to equal, $75,000 or more. *See* 15 U.S.C. § 1681c(b).

- the name, address, and telephone number of any medical information furnisher that has notified the agency of its status;[518] and

- with respect to a nationwide CRA, certain limitations related to veterans' medical debts.[519]

c. Marketing

Although marketing is generally not a permissible purpose for obtaining a consumer report, FCRA permits information sharing with affiliates under certain circumstances and marketing of firm offers of credit or insurance using prescreened consumer reports.

Affiliate Sharing

FCRA excludes certain types of affiliate[520] data sharing from the definition of a "consumer report." The first type of excluded sharing occurs when a regulated entity shares information with an affiliate that specifically relates to a transaction or experience between a consumer and such entity.[521] The second category of excluded sharing occurs when a data holder shares non-transactional information in circumstances where the consumer has been provided notice and an opportunity to opt out of the sharing.[522]

Notice and opportunity to opt out from affiliate data sharing under FCRA must be included in any initial, annual, or revised notices that financial institutions are required to provide to consumers or customers under GLBA.[523] Although GLBA's model form provides the necessary language related to this FCRA opt-out requirement, FCRA itself does not provide additional detail regarding the substance, timing, and duration of opt-out requirements.

Affiliate Use

Once an affiliate receives information that would otherwise be considered a consumer report but for the exception for affiliate use, there are specific guidelines the affiliate must follow with respect to subsequent solicitations for marketing purposes ("marketing solicitation"). A person

518 There are a limited number of specific circumstances in which this information can be included in a consumer report. *See* 15 U.S.C. § 1681c(a)(6).

519 These limitations are described at 15 U.S.C. § 1681c(a)(7)–(8).

520 "Affiliate" means any company that is related by common ownership or common corporate control with another company. 12 C.F.R. § 1022.3(b).

521 15 U.S.C. § 1681a(d)(2)(A)(i)–(ii).

522 15 U.S.C. § 1681a(d)(2)(A)(iii).

523 *See* 12 C.F.R. § 1016.6(a)(7).

engages in a marketing solicitation covered under Regulation V if (i) based on "eligibility information"[524] communicated to that person by its affiliate; (ii) the person uses the eligibility information to identify the consumer or type of consumer, establish criteria to select the consumer, or decide which product or service to market to the consumer; and (iii) as a result, the person provides the consumer with a solicitation.[525]

Subject to certain limited exceptions,[526] FCRA restricts affiliates from using shared information for marketing solicitation unless the consumer is provided a clear and conspicuous disclosure and an opportunity to opt out of receiving the solicitation.[527] This solicitation notice and opt-out opportunity is separate from the affiliate-sharing opt-out notice and may, but is not required to, be included in any GLBA disclosures. The affiliate-use disclosure must provide consumers with the ability to prohibit all marketing solicitation and delivery efforts and also may allow a consumer to select which types of marketing solicitations and delivery options are acceptable, including the types of entities permitted to send them.[528]

FCRA regulations provide model forms for opt-out notices.[529] Any opt-out rights exercised by individuals are effective for at least five years, beginning on the date the person receives the election from the consumer.[530] Once the opt-out period expires, the affiliate may not engage in marketing solicitations until the consumer receives notice and an opportunity to renew the opt-out for a period of five years or more.[531] This renewal notice may also, but is not required to, be included with the annual GLBA privacy notices.[532]

---

524 "Eligibility information" includes both transaction and experience information as well as other data typically found in credit reports, such as information from third-party sources and credit scores. 12 C.F.R. § 1022.20(b)(3). Eligibility information does not include "aggregate or blind data that does not contain personal identifiers such as account numbers, names, or addresses." *Id.* FCRA regulations also provide specific rules relating to eligibility information use by a service provider. *See* 12 C.F.R. § 1022.21(b)(5).

525 12 C.F.R. § 1022.21(b)(1).

526 Notice and opt-out to consumers are not required under the following circumstances: (i) there is a pre-existing business relationship between the consumer and the affiliate; (ii) the affiliate uses the information to communicate with an individual who receives employee benefits or other services pursuant to a contract with an employer; (iii) performing marketing services on behalf of an affiliate; (iv) using information in response to a communication initiated by the consumer; (v) using information in response to solicitations authorized or requested by the consumer; and (vi) compliance with this prohibition would prevent the affiliate from complying with state insurance laws pertaining to unfair discrimination. 15 U.S.C. § 1681s-3(a)(4).

527 15 U.S.C. § 1681s-3(a)(1). Whether or not the relationship between a person and/or affiliate and consumer is ongoing will determine whether an opt-out notice applies to eligibility information received in the future. 12 C.F.R. § 1022.21(a)(2)–(3).

528 15 U.S.C. § 1681s-3(a)(2).

529 12 C.F.R. § 1022, Appendix C.

530 15 U.S.C. § 1681s-3(3).

531 15 U.S.C. § 1681s-3(3).

532 12 C.F.R. § 1022.23.

Prescreened Consumer Reports

CRAs generally cannot provide consumer reports to persons in connection with a credit or insurance transaction unless such transaction is initiated by the consumer, such as a consumer applying for a loan.[533] A notable exception to this rule is that CRAs can provide consumer reports for "a firm offer of credit or insurance."[534] A "firm offer" is defined as "any offer of credit or insurance to a consumer that will be honored if the consumer is determined, based on information in a consumer report on the consumer, to meet the specific criteria used to select the consumer for the offer."[535] A firm offer of credit or insurance can only be conditioned on certain parameters, such as verification that the consumer continues to meet certain criteria contained in the prescreened report.[536]

FCRA allows data users to obtain and use consumer reports to provide consumers with firm offers of credit or insurance through a process called prescreening.[537] Prescreening occurs when a data user requests from a CRA a list of customers that meet certain criteria in order to offer them products or services. FCRA limits the type of information that may be included on these lists to (i) the name and address of a consumer; (ii) an identifier that is not unique to the consumer used exclusively to verify his/her identity; and (iii) other information about the consumer that does not identify a relationship between a particular creditor and the consumer.[538] FCRA places separate notice and opt-out requirements on persons who provide prescreened firm offers of credit or insurance.[539]

2. Accuracy

Both the enactment of FCRA and its amendments since inception have placed important emphasis on the accuracy of the information contained in consumer reports. In its initial form, FCRA placed accuracy obligations only on CRAs. However, the 1996 amendments to the statute expanded its scope to place accuracy obligations on furnishers.[540] The primary accuracy-related provisions of FCRA include adverse action notice requirements, the right of

533 *See* 15 U.S.C. § 1681b(c)(3).

534 15 U.S.C. § 1681b(c)(1)(B)(i).

535 15 U.S.C. § 1681a(l).

536 *See* 15 U.S.C. § 1681a(l). Some courts have held that the firm offer of credit need not contain all material terms, such as the interest rate or the term of the loan. *See Sullivan v. Greenwood Credit Union*, 520 F.3d 70 (1st Cir. 2008) and *Dixon v. Shamrock Fin. Corp.*, 522 F.3d 76 (1st Cir. 2008).

537 *See* 15 U.S.C. § 1681b(c).

538 *See* 15 U.S.C. § 1681b(c)(2).

539 *See* 12 C.F.R. § 1022.54.

540 *See* Consumer Credit Reporting Reform Act of 1996, *adopted* as Subtitle D, Chapter 1, Omnibus Consolidated Appropriations Act, Pub. L 104-208, 110 Stat. 3009 (1996) codified at 15 U.S.C. § 1681s-2.

consumers to request credit reports on an annual basis and upon receipt of an adverse action notice, and the requirements that CRAs and furnishers institute policies and procedures to promote data accuracy.[541]

a. Adverse Actions

Financial Services

FCRA requires users of consumer reports to make certain disclosures when they take adverse action[542] against a consumer based in whole or part on information contained in a consumer report.[543] The information contained in consumer reports is not limited to data provided by traditional creditors or lenders and can include information related to child support payments, medical debt, etc.[544] When a data user obtains a consumer report from a CRA and takes an adverse action, the data user is required to:

- provide a consumer with oral, written, or electronic notice of the adverse action to the consumer;[545]

- provide a consumer with written or electronic disclosures of a numerical credit score[546] used by such person in taking any adverse action based in whole or in part on any information in a consumer report and the following information[547]:
    - the range of possible credit scores under the model used;
    - key factors[548] that adversely affected the credit score, limited to four;
    - the date on which the credit score was created;
    - the name of the person or entity that provided the credit score or credit file upon which the credit score was created;

541 *See* 15 U.S.C. § 1681a.

542 "Adverse action" includes a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested. See 15 U.S.C. §§ 1681a(k)(1)(A), 1691(d)(6). Adverse action also includes "an action taken or determination that is adverse to the interest of the customer and made in connection with an application that was made by, or transaction initiated by, any consumer, or in connection with a review of an account." *See* 15 U.S.C. § 1681a(k)(1)(B)(iv). Other activities within this definition are related to employment, insurance, and license or benefits. *See* 15 U.S.C. § 1681a(k)(1)(B)(i)–(iii).

543 *See* 15 U.S.C. § 1681m(a).

544 *See* 15 U.S.C. §§ 1681s-1, 1681b(g).

545 15 U.S.C. § 1681m(a)(1).

546 "Credit score" is defined as a "numerical value or a categorization derived from a statistical tool or modeling system used by a person who makes or arranges a loan to predict the likelihood of certain credit behaviors, including default (and the numerical value or the categorization derived from such analysis may also be referred to as a 'risk predictor' or 'risk score')." 15 U.S.C. § 1681g(f)(2)(A).

547 15 U.S.C. § 1681m(a)(2)(A)–(B).

548 The term "key factors" means all relevant elements or reasons adversely affecting the credit score for the particular individual, listed in the order of their importance based on their effect on the credit score. *See* 15 U.S.C. § 1681g(f)(2)(B).

- provide a consumer, orally or in writing, contact information about the CRA from which it received the report (including a toll-free number if it is a nationwide CRA), and a statement that the CRA did not make the decision and cannot answer questions about why the decision was made;[549] and

- provide the consumer information on how to obtain a free copy of the report, and his/her right to dispute any perceived inaccuracies.[550]

If the information used to take an adverse action was not obtained by way of a consumer report from a CRA, the statute provides abridged guidelines for notice to the consumer.[551]

Like the adverse-action notice, FCRA requires users of consumer reports to provide a risk-based pricing notice when a user, based on a consumer report, extends credit on terms "materially less favorable" than extended to other consumers.[552] The contents of the risk-based pricing notice are substantially similar to the adverse-action notice.[553]

Other Commercial Uses

CRAs often provide consumer reports in connection with other commercial uses, such as to employers in evaluating candidates for employment or landlords in connection with the rental of properties. For example, in the employment context, a potential employer must provide the consumer with a clear and conspicuous notice that a report will be procured, and the consumer must authorize this request in writing.[554] If the employer takes an adverse action against the consumer after obtaining a consumer report, the employer is required to provide the consumer with an adverse-action notice.[555]

b. Consumer Access to Consumer Reports

Nationwide CRAs are required to make available one free consumer report to consumers in a twelve-month period.[556] After receiving a request for such a report, nationwide CRAs must provide it within fifteen days.[557] Consumers are separately entitled to receive a free consumer

549 15 U.S.C. § 1681m(a)(3)(A)–(B).

550 15 U.S.C. § 1681m(a)(4)(A)–(B).

551 *See* 15 U.S.C. § 1681m(b).

552 *See* 12 C.F.R. § 1022.71.

553 For additional information about the content, form, and timing of the risk-based pricing notice, see 12 C.F.R. § 1022.73.

554 15 U.S.C. § 1681b(b).

555 For additional information about the information FCRA requires in an adverse action notice related to employment, see 15 U.S.C. § 1681b(b)(3).

556 15 U.S.C. § 1681j(a)(1)(A). Nationwide CRAs are not required to provide these reports during the first twelve months of operation. 15 U.S.C. § 1681j(a)(4).

557 15 U.S.C. § 1681j(a)(2).

report from any CRA after receiving an adverse-action notice.[558] Absent qualifying for a free consumer report, CRAs are permitted to impose a reasonable charge to consumers for the procurement of a report.[559]

c. Accuracy Requirements for CRAs and Furnishers

Accuracy and Dispute Requirements for CRAs

CRAs are required to put in place policies and procedures to ensure the maximum possible accuracy for information contained in consumer reports.[560] In a 2015 settlement, the CFPB noted a CRA's deficiencies in this area due to (i) the absence of written procedures for researching public records for consumers with common names; (ii) the failure to require employers to provide middle names; (iii) the failure to track consumer disputes in a manner that would allow for the identification and remedy of reporting error trends; and (iv) the failure of the CRA to conduct sufficient testing of non-disputed records.[561]

If a consumer believes that a consumer report contains inaccuracies, the consumer may dispute the accuracy of information directly to a CRA or indirectly through a reseller.[562] The CRA must then conduct a reasonable investigation into the claim and either record the current status of the disputed information or delete the information within 30 days of receiving notice of the dispute.[563] CRAs have obligations to (i) promptly notify the furnisher about the dispute;[564] (ii) notify the consumer if the CRA determines the dispute is frivolous or irrelevant;[565] (iii) review and consider all information submitted by the consumer related to the dispute;[566] (iv) promptly delete or modify any information found to be inaccurate or unverifiable;[567] (v) notify the consumer about

558 15 U.S.C. § 1681j(b). There are other circumstances where a free consumer report may be available. *See* 15 U.S.C. § 1681j(c)–(d).

559 15 U.S.C. § 1681j(f).

560 15 U.S.C § 1681e(b). One requirement under FCRA aimed at ensuring consumer reports contain accurate information is the requirement that CRAs provide a free credit report to consumers after receiving an adverse action notice. 15 U.S.C. § 1681j(b).

561 *See* In re General Information Services, Inc., and e-Backgroundchecks.com, Inc., 2015-CFPB-0028 (Oct. 29, 2015) (consent order).

562 *See* 15 U.S.C. § 1681i. The term "reseller" means a consumer reporting agency that (i) assembles and merges information contained in the database of another consumer reporting agency or multiple consumer reporting agencies concerning any consumer for purposes of furnishing such information to any third party, to the extent of such activities; and (ii) does not maintain a database of the assembled or merged information from which new consumer reports are produced. 15 U.S.C. § 1681a(u).

563 15 U.S.C. § 1681i(a)(1)(A). The CRA may extend the investigation timeline no more than fifteen days if the information that is the subject of the investigation is found to be inaccurate or incomplete, or the CRA determines it cannot be verified. 15 U.S.C. § 1681i(a)(1)(B)–(C).

564 *See* 15 U.S.C. § 1681i(a)(2).

565 *See* 15 U.S.C. § 1681i(a)(3).

566 *See* 15 U.S.C. § 1681i(a)(4).

567 *See* 15 U.S.C. § 1681(a)(5)(A). CRAs are additionally required to follow guidelines under FCRA related to any reinsertion of previously deleted information, and procedures and reinvestigations to prevent future recurrences and support consistently accurate data. *See* 15 U.S.C. § 1681(a)(2)(B)–(D).

the results of the dispute;[568] and (vi) describe the investigation procedure to the consumer upon request.[569]

Accuracy Requirements for Furnishers

CRAs can only generate reliable consumer reports if the information received from data furnishers is accurate. FCRA and its implementing regulations "prohibit reporting information with knowledge of actual errors"[570] and require furnishers to "establish and implement reasonable written policies and procedures regarding the accuracy and integrity of the information" provided to CRAs.[571] In particular, Regulation V requires that furnishers develop policies and procedures to ensure that furnishers[572]:

- establish and implement an information-furnishing system that is appropriate to the nature, size, complexity, and scope of the furnisher's business operations;
- use standard data reporting formats and standard procedures for compiling and furnishing data, to the extent feasible;
- maintain records for a reasonable period of time in order to substantiate the accuracy of any information about consumers it furnishes that is subject to a direct dispute;
- establish and implement appropriate internal controls regarding the accuracy and integrity of information about consumers furnished to CRAs;
- train staff that participates in activities related to the furnishing of information about consumers to CRAs;
- provide for appropriate and effective oversight of relevant service providers whose activities may affect the accuracy or integrity of information about consumers furnished to consumer reporting agencies to ensure compliance with the policies and procedures;
- furnish information about consumers to CRAs following mergers, portfolio acquisitions or sales, or other acquisitions or transfers of accounts or other obligations in a manner that

568 *See* 15 U.S.C. § 1681(a)(6).

569 *See* 15 U.S.C. § 1681(a)(7). For additional information relating to CRA responsibilities related to consumer disputes, please see 15 U.S.C. § 1681i.

570 15 U.S.C. § 1681s-2(a)(1)(A).

571 12 C.F.R. § 1022.42(a).

572 *See* 12 C.F.R. § 1022.42, Appendix E.

prevents re-aging of information, duplicative reporting, or other problems that may similarly affect the accuracy or integrity of the information furnished;

- delete, update, and correct information in the furnisher's records, as appropriate, to avoid furnishing inaccurate information;
- conduct reasonable investigations of disputes;
- design technological and other means of communication with CRAs to prevent duplicative or erroneous reporting;
- provide CRAs with sufficient identifying information so the CRA is able to properly match the information with the correct consumer record; and
- conduct a periodic evaluation of its own practices and CRA practices to identify any areas for improvement.

Failures to maintain reasonable policies and procedures are subject only to administrative enforcement, rather than private litigation by individual consumers.[573]

Dispute Requirements for Furnishers

FCRA requires certain steps be taken in the event a furnisher receives notice from a CRA or consumer questioning the accuracy or completeness of information contained in a consumer report. Furnishers are required to take certain steps to investigate and review a dispute and fix any inaccuracies in the underlying data, unless they reasonably determine that the dispute is frivolous or irrelevant.[574] Although the specific requirements vary slightly depending on whether the dispute was received from a CRA[575] or directly from a consumer,[576] furnishers generally have an obligation to (i) conduct a timely investigation with respect to the disputed information; (ii) review the relevant information provided with the notice; (iii) report the results back to the CRA or consumer; (iv) report inaccuracies to all nationwide CRAs to which the furnisher previously provided the information; and (v) if applicable, amend the underlying information held

573 15 U.S.C. §§ 1681s, 1681s-2(c)–(d).

574 *See* 12 C.F.R. § 1022.43(f).

575 *See* 15 U.S.C. § 1681s-2(b).

576 *See* 12 C.F.R. § 1022.43(e).

by the furnisher and block future reporting of such information. If a consumer is dissatisfied with the outcome, there are limited private rights of actions available.[577]

Commentary Box 18: Accuracy and Dispute Requirements for Data Aggregators and Sources

Compliance with the accuracy, policy and procedure documentation, and dispute requirements would likely pose novel challenges for data aggregators determined to be CRAs and the companies that provide data to them. For example, the volume and variety of data obtained by data aggregators would require that they develop procedures to promote the accuracy of the data they obtain from third parties and to limit disputed data from appearing in future consumer reports.[578] Aggregators may have limited formal communication channels set up with data providers, particularly if they rely on screen scraping to acquire the data. Complying with the CRA accuracy and dispute requirements would thus require establishing new communication channels and ongoing monitoring with a large volume of data sources. Similarly, in the absence of regulatory guidance, companies that provide information to data aggregator CRAs must interpret for themselves whether providing such data makes them furnishers, and if so, how to investigate disputes, remove incorrect records that often stem from time periods well prior to the date of the consumer report, and avoid retransmission of erroneous records.[579] Some commentators suggest that data sources should not be considered furnishers under the CRA solely by having their data accessed—regardless of whether the process involves an API or screen scraping—because the data source does not take sufficient affirmative action to justify them being deemed furnishers.[580] The

577 *See* Catherine Bourque, *Can Consumers Bring State Claims For Furnisher Errors on Their Credit Reports*, 6:1 LEGIS. AND POL'Y BRIEF 11 (2014), https://digitalcommons.wcl.american.edu/lpb/vol6/iss1/1/; *see also* CHI CHI WU ET AL., FAIR CREDIT REPORTING 401–02 (Nat'l Consumer Law Ctr., 7th ed. 2010) (stating that private rights of action are not available for most furnisher violations of FCRA except when furnishers fail to properly reinvestigate disputed information).

578 *See* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 88 (2020) ("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.").

579 Chi Chi Wu, Nat'l Consumer Law Ctr., Submission to the CFPB Data Symposium (2020), at 8–9 (noting the uncertainty around whether banks would be considered furnishers under certain scenarios involving data sharing with consumer consent).

580 *See* Kwamina Thomas Williford & Brian J. Goodrich, *Why Data Sources Aren't Furnishers Under Credit Report Regs*, LAW360 (Sept. 25, 2019), https://www.law360.com/articles/1202240/why-data-sources-aren-t-furnishers-under-credit-report-regs ("It does not follow that the act of a consumer or her representative accessing their data converts that data source into a furnisher. If it were so, all entities subject to Section 1033 would be furnishers.").

uncertainties of whether and how to apply accuracy requirements to these evolving business models impact both the practices of data aggregators, the companies from which they obtain data, and the consumers that seek to correct errors in their records.

Commentary Box 19: Relationship Between Industry Data Standards and FCRA Requirements

Although furnishers have been required since implementing rules went into effect in 2010 to maintain reasonable policies and procedures regarding the accuracy and integrity of their information, neither FCRA nor its implementing regulations generally define what information must be provided to CRAs or specify standards for data consistency.[581] The federal guidelines that furnishers must consider in developing their policies and procedures simply state that furnishers should "address . . . using standard data reporting formats and standard procedures for compiling and furnishing data, where feasible."[582]

And while regulators can bring actions against furnishers for failing to maintain reasonable policies and procedures, consumers can only sue furnishers for failing to take certain actions in response to a specific accuracy dispute.[583] Failures to follow industry standards have not generally been treated by regulators or courts as FCRA

581 12 C.F.R. § 1022.42, Appendix E. Federal regulators have defined accuracy as focusing on whether the reported information correctly identifies the appropriate consumer, reflects the account's terms and liability, and reflects the consumer's performance with respect to the account. 12 C.F.R. § 1022.41(a). Integrity focuses on whether the information is substantiated by the furnisher's records, is in a form that minimizes the chance that it will be reflected inaccurately in a consumer report, and contains information in the furnisher's possession that federal regulators have determined would be "materially misleading" for purposes of evaluating creditworthiness and other specified traits if it was omitted from the consumer's report. 12 C.F.R. § 1022.41(d). To date, the only specific item that has been identified by regulators as materially misleading if it is omitted is the consumer's credit limit, which is critical for determining consumers' credit utilization rates. 12 C.F.R. § 1022, Appendix E (I)(b)(2)(iii).

582 12 C.F.R. § 1022, Appendix E (III)(b).

583 15 U.S.C. §§ 1681s, 1681s-2(c)–(d).

violations in their own right, although they are sometimes cited as bearing on accuracy and integrity issues.[584]

This system complicates the relationship between industry data standards that are used to report to the three nationwide consumer reporting agencies and compliance with FCRA requirements. Where industry standards are unclear or not followed consistently, data discrepancies may cause consumers who are in fact similarly situated to be treated differently under credit scoring models or by individual consumer report users. But federal regulators may feel constrained in providing guidance that hinges upon the interpretation of private industry standards across a wide variety of factual scenarios, and accuracy litigation fears may similarly complicate the issuance of intra-industry guidance on complex topics.[585]

More broadly, the fact that furnishing is a voluntary activity complicates administration of the traditional credit reporting system for both policymakers and industry actors. Proposals to impose new burdens on furnishers, through either industry or regulatory standards, often trigger concerns that some companies will simply choose to stop providing information, which would hurt the system as a whole and affect consumers individually. For instance, the original industry standard for reporting to nationwide CRAs was not formally retired for almost two decades after a successor standard was rolled out because of concerns about imposing burdens on smaller furnishers.[586]

584 *See, e.g.*, Complaint, *C.F.P.B. v. Navient Corp.*, No. 3:17-cv-00101, 80–83 (M.D. Pa. Jan. 18, 2017); Conditionally Redacted First Amended Complaint, *People v. Navient Corp.*, No. CGC-18-567732 (Cal. Super. Ct. Oct. 16, 2018); In re First Investors, 2014-CFPB-0012, 3.h (Aug. 20, 2014) (consent order); In re Security Group, Inc., 2018-BCFP-0002 (C.F.P.B. June 12, 2018) (consent order).

585 For illustrations of some of the complicated interactions that can occur between industry standards and FCRA compliance, see FINREGLAB, RESEARCH BRIEF: COVID-19 CREDIT REPORTING & SCORING UPDATE (2020), https://finreglab.org/wp-content/uploads/2020/07/FinRegLab-Research-Brief-Covid-19-Credit-Reporting-Scoring-Update.pdf; FINREGLAB, RESEARCH BRIEF: DISASTER-RELATED CREDIT REPORTING OPTIONS (2020), https://finreglab.org/wp-content/uploads/2020/05/FinRegLab-Disaster-Related-Credit-Reporting.pdf.

586 FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 10 (2020).

3. Security

Certain provisions of FCRA relate to the security of information maintained by CRAs and the controls in place to reduce the risks of damage to consumers from identity theft and fraud.[587]

a. Security Compliance Requirements for CRAs

To ensure information compiled and maintained by CRAs is secure, FCRA requires CRAs to maintain reasonable policies and procedures to avoid providing consumer reports for reasons other than those listed as permissible purposes.[588] Commentary issued by the FTC on this point states that CRAs must adopt reasonable security procedures to minimize the possibility that computerized consumer information can be altered by either authorized or unauthorized users of the information system.[589] Additionally, CRAs are not permitted to provide consumer reports to a person for purposes of reselling the report (or information contained therein) unless the identity of the end user of the report is disclosed along with each permissible purpose which the reseller intends to rely on for furnishing to the end user.[590]

b. Consumer Alerts and Identity Theft Protections

FCRA also contains obligations designed to assist victims of identity theft. For example, a consumer may request nationwide CRAs place initial fraud alerts in their consumer reports, which must remain active for no less than one year.[591] Additionally, members of the armed services called to active duty can request an active duty alert be placed in their consumer reports for no less than a year.[592] If a data user receives a consumer report with these alerts on

587 In addition to the provisions discussed in the body of the paper, FCRA contains two additional sets of requirements for which implementation authority remained with the FTC rather than transferred to the CFPB. FCRA regulations called the "red flags" rule require that financial institutions and creditors must "develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft[.]" 16 C.F.R. § 681.1(d)(1). Moreover, FCRA regulations also require any person who maintains or possesses consumer reports or information derived therefrom that identifies individuals to take the necessary, reasonable measures to dispose of such consumer information in order to prevent unauthorized access. 16 C.F.R. § 682.3(a).

588 15 U.S.C § 1681e(a). Recent court decisions indicate that these requirements do not cover data breaches, but rather are limited to furnishing information. See *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295 (N.D. Ga. 2019) (holding that consumers failed to state a claim under FCRA because, even if agency's conduct was egregious, the data at issue was stolen by cyberhackers and not furnished to them).

589 FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 68 (2011).

590 *See* 15 U.S.C § 1681e(e).

591 *See* 15 U.S.C. § 1681c-1(a)(1). Prior to September 21, 2018, the alert period was limited to 90 days; this alert period was extended by amendments to FCRA contained within the Economic Growth, Regulatory Relief, and Consumer Protection Act. This bill also added provisions to FCRA allowing parents to freeze, for free, the credit of their children under the age of sixteen. Additionally, a CRA is required to block the reporting of any information in the consumer's file that a consumer identifies as information resulting from identity theft, provided the consumer provides sufficient documentation. *See* 15 U.S.C. § 1681c-2.

592 *See* 15 U.S.C. § 1681c-1(c)(1). In addition, CRAs are required to exclude active duty military consumers from any credit or insurance firm offer lists for a period of two years. *See id.*

them, the data user must take steps to verify the consumer's identity.[593] Unless the data user has reasonable policies and procedures[594] "to form a reasonable belief that the user knows the identity of the person making the request," the user may not establish a new credit plan or extension of credit for the consumer, issue an additional card on a consumer's existing credit account, or increase a credit limit.[595]

Consumers are also entitled to receive a copy of the records of fraudulent transactions within thirty days of submitting a request.[596] This entitlement applies whether the records are maintained by the institution itself or by a service provider.[597] After taking reasonable steps to positively identify the requestor, the institution can choose to provide these records to the victim, a law enforcement agency specified by the victim, or a law enforcement agency investigating an identity theft authorized by the victim.[598]

V. Third-Party Risk Management Authority

A. Introduction

Third-party risk management refers generally to the body of law, regulation, and guidance governing the relationships between regulated entities and the third parties with whom they interact (typically through commercial relationships). Guidance on third-party relationships arises in the context of broader statutes addressing financial data issues, such as GLBA and FCRA, as well as in discrete bodies of law and guidance more specific to third-party risk management. This section focuses on the latter, while the former is addressed in the other sections of this paper explaining those broader statutes.[599]

593 *See* 15 U.S.C. § 1681c-1(h)(1)(B)(ii).

594 This identity verification process is not required to open an "open-end credit plan" as defined at 15 U.S.C. § 1602. *See* 15 U.S.C. § 1681c-1(h)(1)(A).

595 *See* 15 U.S.C. § 1681c-1(h)(1)(B)(ii).

596 *See* 15 U.S.C. § 1681g(e)(1).

597 *See* 15 U.S.C. § 1681g(e)(1).

598 *See* 15 U.S.C. § 1681g(e)(1)(A)–(C). This statutory provision also includes information on what steps a covered person must take to verify the identity and claim prior to providing the requested information.

599 See Section III.B.1., Section III.C.1., and Section IV.B. for broader discussions of the entities covered under GLBA and FCRA, respectively.

The latter body of federal guidance focused on third-party risk management includes the Bank Service Company Act ("BSCA"),[600] the broad safety and soundness powers of the prudential banking regulators, and DFA.[601] BSCA, among other things, empowers federal agencies to extend their regulatory and examination authorities to any "bank service companies" that act as third parties to regulated persons under their jurisdiction.[602] BSCA also gives prudential regulators the authority to regulate and examine bank service providers "to the same extent as if such services were being performed by the depository institution itself on its own premises."[603] In addition, prudential banking regulators' broad safety and soundness powers permit the examination of service providers of regulated financial institutions. Finally, DFA authorizes the CFPB to exercise regulatory oversight over service providers of covered persons that are subject to its supervisory jurisdiction, as well as service providers that support a number of smaller depository institutions.[604]

In addition to establishing jurisdiction for federal regulators to examine third-party service providers themselves, the agencies have used BSCA, DFA, and related authorities to issue guidance that articulates due diligence expectations for supervised entities when selecting, working with, and monitoring third parties. Thus, supervised entities themselves perform oversight activities in addition to the supervision performed by federal regulators.

The purpose of third-party risk management and regulatory oversight is to ensure that the agencies' regulatory objectives—such as safety and soundness and consumer protection—are not compromised by regulated entities' interactions with third parties, many of which may otherwise be unregulated. Third-party risk management plays a significant role in the regulation of financial data in particular. A substantial portion of financial data is created in the first instance by financial institutions and financial services companies. These regulated entities are increasingly reliant on unaffiliated third parties to provide critical functions and technologies and, as a result, sensitive financial data is often transferred among the parties.[605] Third-party risk

600 *See* Bank Service Company Act, 12 U.S.C. §§ 1661–1867(c).

601 *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. §§ 5514–5565. The Homeowners Loan Act applies substantially similar service provider regulatory provisions as BSCA on service providers of federal savings associations. *See* 12 U.S.C. § 1464(d)(7).

602 12 U.S.C. § 1867(a).

603 12 U.S.C. § 1867(c)(1).

604 DFA defines "service provider" as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service." 12 U.S.C. § 5481(26). This definition includes the following: service providers to large insured banks, credit unions, and their affiliates; service providers to certain non-depository consumer financial service companies; and service providers to a number of small insured depository institutions or insured credit unions. *See* 12 U.S.C. §§ 5514–5516; *see also* CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 2 (2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceServiceProviderBulletin.pdf.

605 *See* MAJ. STAFF OF H. COMM. ON FIN. SERVS., 116TH CONG., MEMORANDUM ON AI AND THE EVOLUTION OF CLOUD COMPUTING: EVALUATING HOW FINANCIAL DATA IS STORED, PROTECTED, AND MAINTAINED BY CLOUD PROVIDERS 3 (2019),

guidance provides a mechanism through which regulators can promote information security, data privacy, and overall legal and regulatory compliance through direct and indirect oversight of third parties, which in many cases may not otherwise be subject to financial data restrictions.

B. Entities Covered

Service providers to depository institutions and non-bank financial services companies are often subject to regulatory oversight. The specific nature of that oversight varies based on the type of institution to which the third party is providing services, the ownership structure of the service provider, and, in some cases, the kind of the services being provided.

1. Oversight of Wholly Owned Service Providers

BSCA specifically permits prudential bank regulators to directly regulate and examine "bank service companies," which are defined to include any corporation or limited liability company performing certain enumerated services for a depository institution and that is wholly owned by one or more insured banks.[606] Those enumerated services include "check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions."[607] Supervisory guidance has included subsidiaries providing data processing, Internet banking, and mobile banking services within that definitional scope.[608]

2. Prudential Oversight of Other Third-Party Service Providers to Depository Institutions

In addition to jurisdiction over wholly owned subsidiaries under BSCA, prudential regulators may also examine any "services authorized under" BSCA[609] that a depository institution has

https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-20191018-sd002-u1.pdf ("As banks deliver more products and services through digital channels and mitigate operational risk, those that lack the in-house expertise to set up and maintain these technologies are increasingly relying upon third-party service providers, including cloud service providers.").

606 12 U.S.C. § 1861(b)(2).

607 12 U.S.C. § 1863.

608 *See* FED. DEPOSIT INS. CORP., FIL-19-2019, TECHNOLOGY SERVICE PROVIDER CONTRACTS 3 (2019), https://www.fdic.gov/news/financial-institution-letters/2019/fil19019.pdf ("Services covered by Section 3 of the Act include check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, or similar functions such as data processing, Internet banking, or mobile banking services.").

609 *See* 12 U.S.C. §§ 1863, 1864.

outsourced "to the same extent as if such services were being performed by the depository institution itself on its own premises."[610] In addition, prudential bank regulators have broad safety and soundness powers to oversee the activities performed by or on behalf of regulated financial institutions.

Each of the prudential bank regulators has offered broad definitions for what types of third parties qualify as service providers subject to such oversight. For example, the OCC defines a "third-party relationship" as "any business arrangement between the bank and another entity, by contract or otherwise."[611] It has further explained that "the term 'business arrangement' is meant to be interpreted broadly and is synonymous with the term third-party relationship" and has provided examples of covered third-party relationships such as outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing, services provided by affiliates and subsidiaries, and joint ventures.[612] Similarly, the FRB has stated that the term "service provider" "is broadly defined to include all entities that have entered into a contractual relationship with a financial institution to provide business functions or activities."[613] The FRB clarified that such entities may be banks or non-banks, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign.[614] The FDIC has offered a substantially similar definition.[615]

3. DFA Authority Over Service Providers

Under DFA, the CFPB has supervisory authority over service providers to certain "covered persons," which include supervised banks and non-banks, as well as service providers to a substantial number of small insured depository institutions or small insured credit unions.[616] DFA defines a "service provider" as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial

610 12 U.S.C. § 1867(c)(1). See Section V.D. below for a fuller discussion of prudential supervisory authority over service providers.

611 *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

612 OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020), https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html.

613 FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 1 (2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf.

614 FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK *FN* 3 (2013).

615 *See, e.g.*, FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 2 (2008), https://www.fdic.gov/news/financial-institution-letters/2008/fil08044a.html ("[T]he term 'third party' is broadly defined to include all entities that have entered into a business relationship with the financial institution, whether the third party is a bank or a nonbank, affiliated or not affiliated, regulated or nonregulated, or domestic or foreign[.]").

616 *See* 12 U.S.C. §§ 5514 (as relates to supervised non-banks), 5515 (as relates to supervised banks), 5516 (as relates to small depository institutions and small insured credit unions); *see also* CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 2 (2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_OfficialGuidanceServiceProviderBulletin.pdf.

product or service."[617] Service providers include parties that are affiliated or unaffiliated with the covered person to which they provide services.[618] The CFPB's third-party risk guidance clarifies that the CFPB expects "supervised banks and non-banks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law," thus providing an avenue for indirect supervision as well as its direct DFA authority.[619]

4. Application of Regulatory Coverage to Financial Technology Entities

Financial technology companies, including data aggregators, often fall within the scope of third-party service providers over which federal regulators have examination authority, or will be classified such that regulators expect covered entities to exercise oversight.[620] Some fintech companies may be wholly-owned subsidiaries of banks and therefore qualify as "bank service companies" under BSCA.[621] Many more fintech companies provide services to banks or "covered persons" subject to CFPB supervision under DFA and thus are often subject to regulatory oversight. This oversight may occur through their coverage under BSCA, DFA, or indirectly through supervision of the institution to which they provide services.[622]

Fintech services can include traditional vendor roles, such as compliance technology or mobile banking services to the bank. In other cases, fintech companies may offer a bank's products and services directly to consumers or small businesses on the bank's behalf as a program manager for the bank. Despite not acting as a traditional vendor to the bank, such entities will still be treated as third-party service providers by the regulated entity for purposes of regulatory oversight.[623] To date, despite these broad oversight powers, federal regulatory agencies have

617 12 U.S.C. § 5481(26).

618 CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 2 (2016).

619 CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 1 (2016).

620 *See, e.g.*, OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020) (listing examples of bank-fintech partnerships that are considered to constitute a third-party relationship requiring oversight per OCC Bulletin 2013-29).

621 12 U.S.C. § 1861(b)(2).

622 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-254, FINANCIAL TECHNOLOGY: ADDITIONAL STEPS BY REGULATORS COULD BETTER PROTECT CONSUMERS AND AID REGULATORY OVERSIGHT 31 (2018), https://www.gao.gov/assets/700/690803.pdf ("Some fintech firms may be subject to indirect federal oversight as part of relationships they have entered into with regulated financial institutions. If fintech firms partner with federally-regulated financial institutions, such as a bank or credit union, federal financial regulators may conduct examinations of the regulated financial intuition that could include some review of the extent to which the fintech firm may affect the partner financial institution's adherence to relevant regulations through the services provided to the financial institution.").

623 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020), (noting inclusion of all "business arrangements in which the bank has an ongoing relationship or may have responsibility for the associated records" as third-party relationships subject to OCC guidance on risk management and discussing marketplace lending in partnership with non-bank entities.

engaged in only limited direct examinations of fintech service providers.[624] Financial data that originates with closely-regulated financial institutions may ultimately flow through to "entities that are not subject to the same degree of direct regulation . . . result[ing] in inconsistent levels of protection."[625]

Commentary Box 20: Application of Third-Party Oversight to Data Intermediaries

As noted above, after the 2017 Equifax breach, federal prudential regulators reportedly disclaimed authority to supervise nationwide consumer reporting agencies as third-party service providers to banks. However, they have exercised it over at least one data aggregator in providing data transmission services.[626]

To date, only the OCC has put forth specific guidance on managing third-party risks posed by data aggregators.[627] The OCC has advised banks under its supervision that "[w]hether a bank has a business arrangement with the data aggregator depends on the level of formality of any arrangements that the bank has with the data aggregator for sharing customer-permissioned data."[628] The establishment of bilateral agreements with data aggregators for sharing customer-permissioned data through APIs "can allow bank customers to better define and manage the data they want to share with a data aggregator and limit access to unnecessary sensitive customer data," but also establishes a business arrangement that requires the bank to engage in third-party oversight of the data aggregator.[629]

---

624 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-254, FINANCIAL TECHNOLOGY: ADDITIONAL STEPS BY REGULATORS COULD BETTER PROTECT CONSUMERS AND AID REGULATORY OVERSIGHT 32 (2018), https://www.gao.gov/assets/700/690803.pdf (noting single examination of a fintech firm by FDIC and OCC limited to data security matters).

625 Kaitlin Asrow, Fed. Reserve Bank of San Francisco, *The Role of Individuals in the Data Ecosystem: Current Debates and Considerations for Individual Data Protection and Data Rights in the U.S.,* FINTECH EDGE 58 (June 3, 2020), https://www.frbsf.org/banking/publications/fintech-edge/2020/june/role-individuals-data-ecosystem/.

626 Kate Berry, *Is CFPB Punting on Equifax? It's Complicated*, AM. BANKER (Feb. 5, 2018), https://www.americanbanker.com/news/is-cfpb-punting-on-equifax-its-complicated; Envestnet/Yodlee, Comment Letter in Response to the OCC/FDIC/FRB NPRM Regarding Enhanced Cyber Risk Management Standards, (Feb. 17, 2017), https://www.federalreserve.gov/SECRS/2017/February/20170227/R-1550/R-1550_022117_131738_464167618786_1.pdf.

627 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020).

628 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020).

629 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020).

The applicability of third-party service provider regulatory oversight is less clear in instances where data aggregators access bank financial data on behalf of customers but do not have a formal business relationship with the bank. In such situations, aggregators are often acting as agents on behalf of the bank's competitors. The OCC has noted that permitting data aggregators to engage in screen scraping, which generally occurs in such instances, typically will not qualify as a business arrangement, but that the banks should nonetheless "take appropriate steps to identify the source of these activities and conduct appropriate due diligence to gain reasonable assurance of controls for managing this process."[630]

C. Data Covered

Third-party risk management is not specific to the type of data held by either the regulated entity or the third-party service provider, but rather broadly covers all financial data held by a third-party service provider. A regulated entity is expected to "adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships," which includes an evaluation of the type, scope, and amount of data that the third party can access.[631] Regulators have placed substantial emphasis on covered entities overseeing third-party information security standards and data breach issues in a manner that would extend the basic tenets of the GLBA Safeguards Rule to those service providers.[632]

630 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020).

631 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013), https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

632 *See, e.g.*, OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE, (2013) ("Stipulate the third party's responsibility for backing up and otherwise protecting programs, data, and equipment, and for maintaining current and sound business resumption and contingency plans."); OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2017-7, THIRD-PARTY RELATIONSHIPS: SUPPLEMENTAL EXAMINATION PROCEDURES (2017), https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-7.html (directing examiners to consider whether bank management has an effective process for escalating issues of data loss by third parties); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 7 (2013) ("Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data."); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 3 (2008) ("Additionally, the ability of the third party to maintain the privacy of customer records and to implement an appropriate information security and disclosure program is another compliance concern. Liability could potentially extend to the financial institution when third parties experience security breaches involving customer information in violation of the safeguarding of customer information standards under FDIC and Federal Trade Commission regulations. Compliance risk is exacerbated when an institution has inadequate oversight, monitoring or audit functions."); NAT'L CREDIT UNION ADMIN., LTR. NO. 01-CU-20, DUE DILIGENCE OVER

D. Oversight

Pursuant to BSCA, prudential banking regulators have rulemaking, supervisory, and enforcement oversight over a limited range of third-party service providers that qualify as "bank service companies."[633]

The prudential banking regulators also have the statutory authority to make rules for and supervise all of the activities and records of the financial institution—whether performed by the covered entity or by a service provider on its behalf.[634] As the OCC has stated, "[a] bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws."[635] Such safety and soundness considerations can be vast, ranging from concentration risk to reputational risk to operational risk.[636] The potential risks include numerous topics relevant to financial data such as compliance with consumer protection laws such as EFTA and ECOA, information security, and data privacy.

The prudential banking regulators have each issued supervisory guidance to regulated entities on risk management of their third-party service providers.[637] In addition, the FDI Act sets out criteria under which the prudential regulators may take direct enforcement action against an "institution-affiliated third party" engaging in legal or regulatory violations, breaches of fiduciary

---

THIRD-PARTY SERVICE PROVIDERS (2001), https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/due-diligence-over-third-party-service-providers ("Typically, at a minimum, third-party contracts should address the following . . . Data security and member confidentiality (including testing and audit) . . . Compliance with regulatory requirements (e.g. GLBA, Privacy, BSA, etc.)").

633 12 U.S.C. §§ 1661, 1867(c).

634 *See* 12 U.S.C. §§ 1464(d)(7), 1867(c)(1). Note that the NCUA does not have independent regulatory authority over service providers.

635 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013).

636 For a non-exhaustive listing of potential risks from third-party service providers, s*ee* FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 1–2 (2013) (listing sources of compliance risks, concentration risks, reputational risks, country risks, operational risks, and legal risks from bank use of third-party service providers); FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS BOOKLET 8–9 (2012), https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf (listing key risks for technology service providers to financial institutions as operational risk; reputation risk; strategic risk; compliance (legal) risk; and credit, interest rate, liquidity, and price (market) risks).

637 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE, (2013) (providing "guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships"); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK (2013) (setting third-party risk management expectations for financial institutions regulated by the FRB); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK (2008) (outlining expected risk management considerations related to third-party service providers for entities regulated by FDIC); NAT'L CREDIT UNION ADMIN., LTR. NO. 01-CU-20, DUE DILIGENCE OVER THIRD-PARTY SERVICE PROVIDERS (2001), (setting expectations for credit unions to engage in third-party service provider oversight).

duty, or unsafe or unsound practices.[638] At least one court has found that a service provider must be engaged in "conducting the business or affairs of the bank" to be subject to enforcement action under the FDI Act, potentially limiting the scope of prudential authority.[639]

DFA affords the CFPB broad "supervisory and enforcement authority over supervised service providers, which includes the authority to examine the operations of service providers on site."[640] The CFPB has issued supervisory guidance that it "expects supervised banks and non-banks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law, which is designed to protect the interests of consumers and avoid consumer harm."[641]

E. Substantive Requirements

Third-party risk management guidelines reflect a primarily principles-based approach to regulation based on regulated entities' assessment of the level of risk and criticality of the services provided by the third party. Given the breadth of potential types of third parties and the array of the services they provide to regulated entities, the scope of the substantive guidance is also wide-ranging. Moreover, the intensity of third-party monitoring has varied significantly within different areas of the financial services industry. Below, we address the substantive themes most relevant to financial data issues, most of which focus on the higher-risk areas of information technology and information security.

1. Bank Service Company Requirements

BSCA sets out substantive and procedural requirements relating to "bank service companies." As noted above, bank service companies are a subset of all third-party service providers to financial institutions, insofar as they perform specifically designated services and are wholly owned by one or more insured banks.[642] BSCA limits the amount of investment an insured bank may make into a bank services company and restricts banks service companies to a limited

638 12 U.S.C. § 1818. "Institution-affiliated party" includes, among other parties, "any independent contractor (including any attorney, appraiser, or accountant) who knowingly or recklessly participates in—(A) any violation of any law or regulation; (B) any breach of fiduciary duty; or (C) any unsafe or unsound practice, which caused or is likely to cause more than a minimal financial loss to, or a significant adverse effect on, the insured depository institution." 12 U.S.C. § 1813(u).

639 *Grant Thornton LLP v. O.C.C.*, 514 F.3d 1328 (D.C. Cir. 2008).

640 CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 3 (2016); *see also* 12 U.S.C. §§ 5514–5516 (granting CFPB supervisory authority over service providers to offerors of mortgage products, payday loans, student loan products, large insured depository institutions and credit unions, and a substantial number of smaller depository institutions).

641 CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 1 (2016).

642 12 U.S.C. § 1861(b)(2).

range of services: “check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements, notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution.”[643] As noted above, supervisory guidance has characterized services such as “data processing, Internet banking, [and] mobile banking services” as within the services covered by BSCA.[644]

BSCA requires that supervised banks provide written notification to their federal prudential regulator of any contracts or relationships with “bank service companies” within thirty (30) days of making the service contract or performing the services, whichever occurs first.[645] Bank services companies are subject to prudential rulemaking and supervisory oversight “by the appropriate Federal banking agency of its principal investor to the same extent as its principal investor.”[646] Insured banks must seek prior regulatory approval before investing in a bank service company.[647] Prudential regulators may also terminate a bank service company’s status “as if the bank service company were an insured bank.”[648]

2. Risk-Tailored Approach to Oversight

Federal financial regulators have shared a common approach for instructing regulated entities to engage in third-party risk management that is commensurate with the assessed level of risk and complexity and importance of the activities being outsourced.[649] These agencies have, overall, indicated both explicitly and implicitly that outsourced activities related to financial data, its security, and its management represent a relatively high level of risk and complexity and should receive significant scrutiny.[650] The OCC, in particular, has cautioned banks that they should engage in “comprehensive risk management and oversight of third-party relationships involving critical activities” and has indicated that many activities related to financial data would be so categorized.[651]

643 *See* 12 U.S.C. §§ 1862–1863.

644 *See* FED. DEPOSIT INS. CORP., FIL-19-2019, TECHNOLOGY SERVICE PROVIDER CONTRACTS 3 (2019); *see also* FED. DEPOSIT INS. CORP., FIL-49-99, REQUIRED NOTIFICATION FOR COMPLIANCE WITH THE BANK SERVICE COMPANY ACT (1999).

645 *See* 12 U.S.C. § 1867(c)(2).

646 *See* 12 U.S.C. § 1867(a).

647 *See* 12 U.S.C. § 1865.

648 12 U.S.C. § 1867(b).

649 *See, e.g.*, CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 4 (2016).

650 *See, e.g.*, FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 1 (2008) (“A third-party relationship should be considered significant if . . . the third party stores, accesses, transmits, or performs transactions on sensitive customer information . . . .”).

651 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE, (2013).

The OCC defines "critical activities" as "significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that:

- could cause a bank to face significant risk if the third party fails to meet expectations;
- could have significant customer impacts;
- require significant investment in resources to implement the third-party relationship and manage the risk; or
- could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house."[652]

Given the potential for direct customer impacts and reliance on complex information technology, fintech companies and data aggregators may be considered to involve critical activities and, thus, receive heightened scrutiny.[653] The OCC has declined to specify that all fintech companies are critical third parties, stating instead that "each bank's board and management to identify the critical activities of the bank and the third-party relationships related to these critical activities."[654] The FDIC has called for special consideration of third-party service providers involved in the modeling of financial data, and has emphasized that banks will likely require heightened internal controls and clear justifications for the models used.[655]

Several regulatory agencies have paid special attention to the role third-party data storage companies—particularly cloud-based storage firms—may play for covered entities, flagging it as a particularly high-risk endeavor.[656] In its latest guidance, the OCC has cautioned banks that a business arrangement with a cloud services provider requires risk management oversight and

652 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE, (2013).

653 *See, e.g.*, FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 5 (2008) ("For example, large-scale, highly visible programs or programs dealing with sensitive data integral to the institution's success warrant an in-depth due diligence of the potential third party, while the due diligence process for isolated low-risk third-party activities would be much less comprehensive.").

654 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29, 2020).

655 FED. DEPOSIT INS. CORP., CONDUCTING BUSINESS WITH BANKS: A GUIDE FOR FINTECHS AND THIRD PARTIES 3 (2020), https://www.fdic.gov/fditech/guide.pdf.

656 *See, e.g.*, OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29, (2020); Fed. Fin. Inst. Examination Council, Supervision Tip 2018-04, Joint Statement: Security in a Cloud Computing Environment (2020), https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf; *see also* MAJ. STAFF OF H. COMM. ON FIN. SERVS., 116TH CONG., MEMORANDUM ON AI AND THE EVOLUTION OF CLOUD COMPUTING: EVALUATING HOW FINANCIAL DATA IS STORED, PROTECTED, AND MAINTAINED BY CLOUD PROVIDERS 3–4 (2019) (reviewing regulatory framework for cloud service providers to financial services entities, including FFIEC, FRB, and SEC guidance).

that “specific technical controls in cloud computing may operate differently than in more traditional network environments.”[657] The OCC advises banks to ensure effective oversight and notes that “the bank is ultimately responsible for the effectiveness of the control environment” even where they do not control it.[658]

3. Risk Management Life Cycle

Although regulatory agencies have stated that they expect entities under their prudential supervision to engage in a risk management oversight process of third-party service providers, they have declined to dictate the specific steps that covered entities must take. The FFIEC’s interagency guidance notes that:

The Agencies recognize that management practices, particularly as they relate to risk management, vary considerably among financial institutions and [service providers], depending on their size and sophistication, the nature and complexity of their business activities, and their risk profile. Accordingly, the Agencies also recognize that for less complex information systems environments, detailed or highly formalized systems and controls may not be required.[659]

Similarly, the OCC most recently stated that “[t]here is no one way for banks to structure their third-party risk management process” and reminded banks that the regulatory expectation was for them to engage in risk management “commensurate with the level of risk and complexity of their third-party relationships.”[660] The FDIC has advised that “[t]he scope and depth of due diligence is directly related to the importance and magnitude of the institution’s relationship with the third party . . . large-scale, highly visible programs or programs dealing with sensitive data integral to the institution’s success warrant an in-depth due diligence of the potential third party, while the due diligence process for isolated low-risk third-party activities would be much less comprehensive.”[661] The CFPB has similarly set expectations for “covered persons” under its supervisory jurisdiction that “the depth and formality of the entity’s risk management program for service providers may vary depending upon the service being performed—its size, scope,

657 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020).

658 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29 (2020).

659 FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS BOOKLET 9 (2012) (specifically discussing risk management of technology service providers).

660 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2020-10, THIRD-PARTY RELATIONSHIPS: FREQUENTLY ASKED QUESTIONS TO SUPPLEMENT OCC BULL. 2013-29, 2020).

661 FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 5 (2008).

complexity, importance and potential for consumer harm—and the performance of the service provider . . . ."[662]

The agencies' regulatory guidance has generally focused on a "risk management life cycle," which is a continuous process of risk appraisal in a regulated institution's relationships with service providers.[663] As described by the OCC, there are five steps in this life cycle, each of which requires supervised institutions to manage risks including those related to financial data: (i) planning; (ii) due diligence and third-party selection; (iii) contract negotiation; (iv) ongoing monitoring; and (v) termination.[664] Although each step encompasses broad considerations related to third-party service providers, below are some of the relevant considerations for each step that relate to financial data.

a. Planning

Regulators have sought for entities holding financial data to conduct careful risk assessments on the following topics before deciding to outsource activities: (i) third-party service provider access to customer confidential information;[665] (ii) the potential for unauthorized disclosure of confidential information from information security failures;[666] (iii) the extent to which the activities are subject to specific privacy or information security laws, such as GLBA, and could result in liability to the entity;[667] and (iv) data confidentiality, integrity, and availability (e.g., transportability and interoperability).[668]

662 CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 4 (2016).

663 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013).

664 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE, (2013). Other regulators have used slightly different terminology in their descriptions of the risk management life cycle for service providers but have described a materially similar process. *See, e.g.*, FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, OUTSOURCING TECHNOLOGY SERVICES BOOKLET 4 (2004), https://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf (describing risk management life cycle steps as "risk assessment and requirements definition; due diligence in selecting a service provider; contract negotiation and implementation; and ongoing monitoring"); CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 4–5 (2016) (describing steps as conducting thorough due diligence, requesting and reviewing internal control materials, including specific contractual provisions, establishing ongoing monitoring, and taking action to address problems including terminations).

665 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013); FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, OUTSOURCING TECHNOLOGY SERVICES BOOKLET 6 (2004).

666 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013); FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, OUTSOURCING TECHNOLOGY SERVICES BOOKLET 5 (2004); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 3 (2008) ("the ability of the third party to maintain the privacy of customer records and to implement an appropriate information security and disclosure program").

667 OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 3 (2008).

668 FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, BUSINESS CONTINUITY MANAGEMENT BOOKLET 22–23 (2019), https://ithandbook.ffiec.gov/media/296178/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf.

b. Due Diligence and Third-Party Selection

Regulators have called for the following types of risk assessment and due diligence attention by covered entities related to financial data privacy: (i) strong information technology systems that provide security, reliability, and availability of data;[669] (ii) appropriate internal controls over data privacy and security, with particular emphasis on customer records;[670] (iii) adequate insurance coverage to compensate for data losses;[671] and (iv) sufficient systems for compliance with the regulatory requirements of the covered entity.[672] Regulators have also urged caution in selecting foreign-based third parties that will handle customer financial data.[673]

c. Contract Negotiations

Regulators have advised covered entities to incorporate the following terms with regard to financial data privacy in their contracts with third-party service providers: (i) data confidentiality;[674] (ii) clear division of roles and responsibilities for data security;[675] (iii) third-party responsibility for data loss or breach notification;[676] (iv) return or destruction of consumer financial data;[677] and (v) responsibility for compliance with data privacy and security laws.[678] The FDIC has advised

669 *See* FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, SUPERVISION OF TECHNOLOGY SERVICE PROVIDERS BOOKLET 9, A-11–A-12 (2012); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 5 (2013).

670 *See* FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 5–6 (2008) ("The evaluation of a third party may include the following items: . . . Scope of internal controls, systems and data security, privacy protections, and audit coverage."); Kevin W. Hodson and Todd L. Hendrickson, *Third-Party Arrangements: Elevating Risk Awareness*, FDIC SUPERVISORY INSIGHTS (Summer 2007 ed.), at 6, https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum07/sisummer07-article1.pdf.

671 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013).

672 *See* NAT'L CREDIT UNION ADMIN., LTR. NO. 01-CU-20, DUE DILIGENCE OVER THIRD-PARTY SERVICE PROVIDERS (2001); FED. DEPOSIT INS. CORP., CONDUCTING BUSINESS WITH BANKS: A GUIDE FOR FINTECHS AND THIRD PARTIES, 3–4 (2020); CONSUMER FIN. PROT. BUREAU, 2016-02, COMPLIANCE BULLETIN AND POLICY GUIDANCE: SERVICE PROVIDERS 4 (2016).

673 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE, 2013) ("The potential for serious or frequent violations or noncompliance exists when a bank's oversight program does not include appropriate audit and control features, particularly when … customer and employee data is transmitted to foreign countries."); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 9 (2013) ("Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions."); FED. DEPOSIT INS. CORP., FIL-52-2006, GUIDANCE FOR FINANCIAL INSTITUTIONS ON THE USE OF FOREIGN-BASED THIRD-PARTY SERVICE PROVIDERS, (2006), https://www.fdic.gov/news/financial-institution-letters/2006/FIL-52-2006a.pdf.

674 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2017-7, THIRD-PARTY RELATIONSHIPS: SUPPLEMENTAL EXAMINATION PROCEDURES (2017).

675 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 7 (2013); NAT'L CREDIT UNION ADMIN., LTR. NO. 01-CU-20, DUE DILIGENCE OVER THIRD-PARTY SERVICE PROVIDERS (2001).

676 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 7 (2013); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK (2008).

677 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013); FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 8 (2013); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK (2008).

678 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2017-7, THIRD-PARTY RELATIONSHIPS: SUPPLEMENTAL EXAMINATION PROCEDURES (2017); NAT'L CREDIT UNION ADMIN., LTR. NO. 01-CU-20, DUE DILIGENCE OVER THIRD-PARTY SERVICE PROVIDERS (2001).

that a covered entity's contract with a third-party service provider should ensure that "[a]ny nonpublic personal information on the institution's customers must be handled in a manner consistent with the institution's own privacy policy and in accordance with applicable privacy laws and regulations" that would be applicable directly to the covered person.[679]

d. Ongoing Monitoring

Regulators expect covered persons to implement ongoing monitoring through service provider risk-management programs, including: a focus on activities that involve sensitive customer information;[680] review of the privacy protection of confidential information;[681] and monitoring of information security controls related to GLBA compliance.[682] Regulators have also advised that oversight of service providers should be tightened in instances where information security incidents lead to the release of consumer financial data.[683]

e. Termination

Regulators have emphasized to covered persons that their third-party risk management obligations extend to planning for how they will recover their financial data in the event that they must terminate the third-party relationship.[684]

Commentary Box 21: Areas for Potential Expansion of Financial Data Oversight

There are incipient signs of legislative and regulatory interest in policy changes related to third-party risk management of financial data. Given that third-party risk management is largely an extension of safety and soundness supervision,

679 FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 8 (2008).

680 FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 2 (2013).

681 FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 5 (2013).

682 FED. FIN. INST. EXAMINATION COUNCIL, IT EXAMINATION HANDBOOK, OUTSOURCING TECHNOLOGY SERVICES BOOKLET 19–26 (2004).

683 FED. RESERVE BD., SR 13-19, GUIDANCE ON MANAGING OUTSOURCING RISK 10 (2013).

684 *See* OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2013-29, THIRD-PARTY RELATIONSHIPS: RISK MANAGEMENT GUIDANCE (2013) (advising that termination plans cover "risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship"); FED. DEPOSIT INS. CORP., FIL-44-2008, GUIDANCE FOR MANAGING THIRD-PARTY RISK 8 (2008) ("The contract should state termination and notification requirements, with operating requirements and time frames to allow for the orderly conversion to another entity without excessive expense. Return of the financial institution's data, records, and/or other resources should also be addressed.").

regulators have some flexibility to adapt this body of law based on evolving industry developments and risk assessments.

For example, federal financial regulators have noted the risks to the financial markets related to increasing financial institution reliance "on third-party firms that aggregate and distribute marketwide data," as well as on "outside cloud computing services to supplement existing technology infrastructures for data storage, redundancy, and computational capacity."[685] More frequent and detailed supervisory examinations of service providers may be the next step for both prudential and consumer protection regulators seeking to better understand the risks posed by third parties that hold, transmit, or analyze financial data.[686] An increase in such supervisory examinations, however, may raise questions about the need for increased efficiency in third-party oversight as regulated depository institutions and nonbanks would likely need to perform repeated individual due diligence on a single set of common service providers; this need for repeated suitability evaluation may incentivize industry cooperation to establish a shared protocol (such as the Standardized Information Gathering questionnaire or SIG framework) or development of an industrywide list of approved vendors. The FDIC issued a Request for Information in July 2020 exploring the possibility of creating a private standard setting organization and/or voluntary certification program that could ease burdens with regard to vendor management, particularly for community banks that may otherwise struggle to form fintech partnerships.[687] In addition, there appears to be legislative interest in extending service provider oversight powers to both the NCUA and FHFA.[688]

685 FIN. STABILITY OVERSIGHT COUNCIL, ANNUAL REPORT 91 (2018), https://home.treasury.gov/system/files/261/FSOC2018AnnualReport.pdf.

686 *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-18-254, FINANCIAL TECHNOLOGY: ADDITIONAL STEPS BY REGULATORS COULD BETTER PROTECT CONSUMERS AND AID REGULATORY OVERSIGHT 32 (2018), https://www.gao.gov/assets/700/690803.pdf (noting only a single supervisory examination of a fintech service provider and advocating for more examinations of fintech service providers).

687 85 Fed. Reg. 44890 (July 24, 2020).

688 *AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers: Hearing Before the H. Comm. Of Fin. Servs., Task Force on Artificial Intelligence,* 116th Cong. (2019) (discussing draft of legislation entitled "Strengthening Cybersecurity for Financial Sector Act" extending NCUA and FHFA oversight powers to service providers for credit unions, Fannie Mae, Freddie Mac, and FHLBs).

VI. Equal Credit Opportunity Act (ECOA)

A. Introduction

The Equal Credit Opportunity Act ("ECOA")[689] was enacted in 1974, making it unlawful for creditors to discriminate against applicants in any aspect of a credit transaction on the basis of sex or marital status. The enactment of ECOA followed in the footsteps of the Fair Housing Act [690] passed in 1968, which was enacted to prevent discrimination involved in the sale, rental, and financing of housing based on race, religion, national origin, or sex. Congress has since amended ECOA several times, the most significant of which was in 1976 with the expansion of the statute's prohibition to include discrimination based on race, color, national origin, age, receipt of public assistance income, or an applicant's good faith exercise of any right provided under the Consumer Credit Protection Act.[691] ECOA's restrictions on using any such "prohibited basis" to treat certain consumers less favorably are intended to remedy pernicious discriminatory practices in the United States that limited consumer and business access to credit on fair terms.[692] To promote transparency in credit decisions, ECOA also requires creditors to provide applicants with notice containing a "statement of reasons" when making a decision considered adverse to the applicant. ECOA's implementing regulation, known as Regulation B, provides additional detail regarding compliance requirements for creditors, including rules and standards for evaluating credit applications, data collection and retention, as well as model forms.[693]

ECOA and Regulation B have important implications for the regulation of financial data in the United States. Credit underwriting is a fundamentally data-based process by which creditors determine whether and at what cost they are prepared to offer credit. Widespread advances in technology and data analysis capabilities now permit evaluation of large datasets for credit

689 Pub. L. No. 93-495, 88 Stat. 1521 (1974) (codified as amended at 15 U.S.C. § 1691 *et seq.*). The passage of this legislation stemmed from hearings held by the National Commission on Consumer Finance ("NCCF") regarding credit discrimination against women. Senator Bill Brock noted that "legislation is needed not only to assure that women have access to mortgage credit, but that women are not subtly denied opportunities to purchase homes or rent dwellings." *1973 Housing and Urban Development Legislation: Hearings on S. 1604 Before the Subcomm. on Housing and Urban Affairs of the S. Comm. on Banking, Housing and Urban Affairs*, 93rd Cong. 1227, 1228 (1973) (statement of Sen. Bill Brock, Member, S. Comm. on Banking, Housing and Urban Affairs). Although the Fair Housing Act, passed five years prior, put in place some protections, the Senator notes in his speech that discrimination on account of sex should have been included in that act. *Id.*

690 Pub. L. No. 90-284, 82 Stat. 81 (1968) (codified as amended at 42 U.S.C. § 3601 *et seq.*).

691 Equal Credit Opportunity Act Amendments of 1976, Pub. L. No. 94-239, 90 Stat. 251 (1976) (codified as amended at 15 U.S.C. § 1691 et seq.). In addition to ECOA, the Consumer Credit Protection Act also includes the following statutes: TILA, CROA, FCRA, FDCPA, EFTA, the Federal Wage Garnishment Law. *See* 15 U.S.C. §§ 1601–1693r.

692 *See generally* Barbara J. Klein, *The Equal Credit Opportunity Act Amendments of 1976: A Meaningful Step Toward the Elimination of Credit Discrimination*, 26 CATH. U. L. REV. 149 (1977), https://scholarship.law.edu/cgi/viewcontent.cgi?article=2470&context=lawreview.

693 *See* 12 C.F.R. § 1002.1–16.

decisions at speeds that were not possible historically. Taken together, ECOA's prohibition on discrimination, its implementing rules, and judicial decisions and enforcement actions interpreting these requirements significantly impact what applicant data creditors can collect and use in making these decisions. These restrictions and the significant penalties that can result from violations limit discrimination but also create uncertainty around the implementation of innovative uses of data and new methodologies that could lead to greater credit access for traditionally underserved borrowers.[694]

B. Entities Covered

ECOA prohibits creditors from discriminating against any applicant[695] with respect to any aspect of a "credit transaction."[696] "Creditor" is defined under ECOA to include "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."[697] Regulation B extends the definition of creditor to include any person who assists in setting the terms of the credit.[698] The discrimination and discouragement prohibitions of Regulation B also apply to a person "who, in the ordinary course of business, regularly refers applicants or prospective applicants to creditors, or selects or offers to select creditors to whom requests for credit may be made."[699] In practice, this definition includes, but is not limited to, banks, retailers, credit card companies, finance companies, and credit unions. The term has also been construed to cover individuals or entities not traditionally viewed as creditors that assist in setting the terms of a credit arrangement, such as mortgage brokers,[700] or car dealerships.[701]

694 *See* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS (2020), https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf.

695 An applicant means "any person who requests or who has received an extension of credit from a creditor, and includes any person who is or may become contractually liable regarding an extension of credit." 12 C.F.R. § 1002.2.(e). For purposes of Regulation B's rules concerning the signature requirements, the term includes guarantors, sureties, endorsers, and similar parties." *Id.*

696 A "credit transaction" is defined as "every aspect of an applicant's dealings with a creditor regarding an application for credit or an existing extension of credit (including, but not limited to, information requirements; investigation procedures; standards of creditworthiness; terms of credit; furnishing of credit information; revocation, alteration, or termination of credit; and collection procedures)." 12 C.F.R. § 1002.2(m).

697 15 U.S.C. § 1691a(e).

698 12 C.F.R. § 1002.2(l). A person is not a creditor under Regulation B with respect to the acts of another creditor, unless the person had reasonable notice of the act, policy, or practice that comprised the violation before becoming involved in the credit transaction. *Id.*

699 12 C.F.R. § 1002.2(l).

700 *Kivel v. WealthSpring Mortg. Corp.*, 398 F. Supp. 2d 1049 (D. Minn. 2005) (holding that a mortgage broker was a "creditor" of mortgagors who sought to refinance because the broker participated in setting the terms of the credit arrangement).

701 *Cannon v. Metro Ford, Inc.*, 242 F. Supp. 2d 1322 (S.D. Fla. 2002) (holding that a car dealership was considered a "creditor" because the dealer accepted the application, set the terms of the retail installment sales contract, and subsequently shopped the contract to selected lenders).

C. Data Covered

ECOA's prohibition against discrimination on protected bases impacts what data creditors can collect and how that data can be used in connection with credit transactions. Specifically, Regulation B provides express guidance on whether certain information related to a prohibited basis may be requested in connection with a credit transaction[702] and how creditors can use certain data in evaluating applicants[703] and extending credit.[704] Unlike other consumer protection statutes, such as GLBA, that apply only to consumers, ECOA and Regulation B also encompass commercial credit.[705]

In addition, as discussed further below in Section VI.E.1.c., the broad statutory and regulatory prohibition on discrimination has been interpreted by regulators and courts to prohibit practices that have a "disparate impact": facially neutral practices applied evenly to all applicants that have disproportionate (and often unintentional) adverse effects on protected classes, unless the creditor has a legitimate business need that cannot be achieved through less impactful means.[706] As a result, the types and uses of data potentially covered by ECOA and Regulation B are extremely broad, and creditors must ensure they have taken appropriate steps to ensure that seemingly neutral data practices do not give rise to unintended, avoidable, negative consequences for protected populations.

As the quantity of available data multiplies and the capabilities for analyzing it continue to progress, determining what data types and uses are permissible for credit underwriting is becoming increasingly important. For example, one recent study discussed further below analyzed the effects and policy implications of using bank account and other cash-flow data in credit underwriting, finding that the degree to which the information was predictive of credit risk appeared to be relatively consistent across borrowers who likely belong to different demographic groups.[707] While data was not available to conduct certain types of analyses, these

---

702 *See* 12 C.F.R. § 1002.5.

703 *See* 12 C.F.R. § 1002.6.

704 *See* 12 C.F.R. § 1002.7.

705 12 C.F.R. cmt. 1002.1(a)-1. Although ECOA and Regulation B apply to commercial credit, the requirements differ in some instances with respect to the rules related to consumers. For example, creditors must only notify business credit applicants with over $1 million in gross revenue for the prior year within a reasonable time period after an adverse action decision, as opposed to the 30-day requirement for consumer credit applicants. 12 C.F.R. § 1002.9(a)(3).

706 The Supreme Court has not yet ruled on whether a claim predicated on disparate impact theory is available under ECOA. However, in 2015 it held that disparate impact claims are cognizable under the Fair Housing Act. *See Tex. Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc.*, 576 U.S. 519 (2015).

707 FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS (2020).

and other initial results suggested that cash-flow variables and scores do not create a disparate impact among protected populations.[708]

D. Oversight

Regulatory enforcement authority of ECOA is primarily split among the following agencies: CFPB, FTC, OCC, FDIC, FRB, and NCUA.[709] ECOA requires these agencies to refer matters to the U.S. Department of Justice ("DOJ") when there is reason to believe a creditor is engaged in a pattern or practice of discrimination.[710] When originally enacted, rulemaking authority under ECOA resided with the FRB.[711] However, DFA transferred ECOA rulemaking responsibility to the CFPB except with regard to certain auto dealers,[712] which are still governed by rules written by the FRB.[713] The CFPB restated ECOA's implementing regulation, Regulation B, in December 2011.[714]

ECOA also provides a private right of action to bring civil suits for alleged violations in both an individual capacity and as members of a class action.[715] ECOA permits punitive damages of up to $10,000 in individual lawsuits and up to the lesser of $500,000 or 1% of the creditor's net worth in class action suits.[716]

708 FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 27 (2020).

709 *See* 15 U.S.C. § 1691c. Additional agencies tasked with ensuring compliance with ECOA include: (i) Secretary of Transportation, with respect to all carriers subject to the jurisdiction of the Surface Transportation Board; (ii) Secretary of Transportation with respect to any air carrier or foreign air carrier subject to Part A of subtitle VII of title 49; (iii) Secretary of Agriculture with respect to any activities subject to the Packers and Stockyards Act; (iv) Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, and production credit association; (v) Securities and Exchange Commission with respect to brokers and dealers; and (vi) the Small Business Administration, with respect to small business investment companies.

710 15 U.S.C. § 1691e(g). The DOJ provided guidance to the federal bank regulatory agencies on pattern or practice referrals in 1996. *See* U.S. DEP'T OF JUSTICE, MEMORANDUM, IDENTIFYING LENDER PRACTICES THAT MAY FORM THE BASIS OF A PATTERN OR PRACTICE REFERRAL TO THE DEPARTMENT OF JUSTICE (1996), https://www.justice.gov/sites/default/files/crt/legacy/2014/03/05/regguide.pdf (describing the factors that the DOJ would consider in determining which matters it would return to the agency for administrative resolution and which it would pursue for potential litigation). Generally, the "reason to believe" standard establishes a very low bar.

711 *See* 15 U.S.C. § 1691 *et seq.*

712 *See* 12 U.S.C. §§ 5481(12)(D), 5581.

713 After the passage of DFA, the FTC retained ECOA enforcement authority over entities within its jurisdiction, including most non-bank financial services companies, as well as most motor vehicle dealers. See 15 U.S.C. § 1691c(c). Importantly, given the history of fair lending concerns, most motor vehicle dealers are not subject to CFPB jurisdiction.

714 76 Fed. Reg. 79442 (Dec. 21, 2011) (codified at 12 C.F.R. Part 1002).

715 15 U.S.C. § 1691e(a).

716 15 U.S.C. § 1691e(b).

E. Substantive Requirements

1. Prohibition on Discrimination

As previously discussed, ECOA prohibits discrimination on any of the prohibited bases in connection with credit transactions.[717] In practice, violations of the statute are pursued under three general theories of liability: (i) disparate treatment based on overt evidence of discrimination—e.g., disparaging statements or express policies revealing a discriminatory preference; (ii) disparate treatment based on comparative evidence—evidence consisting of differences in treatment between similarly situated individuals that cannot be fully explained by legitimate, nondiscriminatory factors; or (iii) disparate impact—the application of a facially neutral policy or practice that is applied evenly across all applicants but disproportionately excludes or burdens individuals on a prohibited basis, unless the policy or practice effectuates a legitimate business justification that cannot be reasonably achieved through less impactful means.[718]

a. Disparate Treatment – Overt Evidence

ECOA violations based on a disparate treatment theory supported by overt evidence can involve statements made by creditors. A lender telling an individual that a bank does not lend to borrowers of a particular race would be an example. Overt evidence can also include a lender having an express policy of offering credit terms that differ based on a prohibited basis, such as a credit card with higher limits made available only to male applicants but not female applicants. A 2016 enforcement action brought by the CFPB against a bank provides an example of a disparate treatment complaint based on overt evidence.[719] In this complaint, the CFPB alleged that the bank had discriminated against African-American applicants in the underwriting and pricing of mortgage loans.[720] Specifically, the Complaint alleged that the bank had instructed loan officers to deny applications from African-Americans and others more quickly, and, for those approved, "charged them, on average, 30–64 basis points more for first lien and second lien mortgage loans[.]"[721]

---

717 15 U.S.C. § 1691(a).

718 FED. RESERVE BD., CONSUMER COMPLIANCE HANDBOOK, FEDERAL FAIR LENDING REGULATIONS AND STATUTES: OVERVIEW 2–3 (2017), https://www.federalreserve.gov/boarddocs/supmanual/cch/fair_lend_over.pdf.

719 *See* Complaint, *C.F.P.B. v. BankCorpSouth Bank*, No. 1:16cv118-GHD-DAS (N.D. Miss. June 29, 2016).

720 Complaint at 2, *C.F.P.B. v. BankCorpSouth Bank*, No. 1:16cv118-GHD-DAS (N.D. Miss. June 29, 2016).

721 Complaint at 2, *C.F.P.B. v. BankCorpSouth Bank*, No. 1:16cv118-GHD-DAS (N.D. Miss. June 29, 2016).

b. Disparate Treatment – Comparative Evidence

More commonly, disparate treatment claims are based on circumstantial evidence involving differences in treatment that cannot be explained by legitimate, nondiscriminatory reasons. Evidence of this type of discrimination is ordinarily obtained by comparing two "similarly situated" individuals that received different treatment; for example, a creditor that sees adverse information on a credit report for a couple of one race and chooses to approve the application but when presented with the same circumstances for couple of another race, denies the application. Unless the creditor can present a valid, non-discriminatory reason for this difference in treatment, the creditor violated ECOA.[722] In 2011, the DOJ released a consent order settling allegations of disparate treatment on the basis of race related to residential real-estate transactions.[723] The DOJ alleged that "African-American and Hispanic borrowers were more than twice as likely to be placed in subprime loans than non-Hispanic White wholesale borrowers who had similar credentials."[724]

c. Disparate Impact

Disparate impact, by comparison, involves a specific, facially neutral policy that is applied uniformly to all consumers that nonetheless results in disproportionately adverse impacts on a prohibited basis. For example, a creditor may decide to have a minimum mortgage loan amount policy of $100,000. While such a policy does not overtly discriminate on a prohibited basis, minimum loan amounts can often have an exclusionary effect on residents of lower-income communities, which in many areas consist of large racial minority populations.[725] Evidence of a policy's impact, however, is not by itself sufficient to establish a violation. It must also be shown that the policy is either unsupported by a valid "business necessity" or "justification" or, if such a valid justification exists, that an alternative policy or practice would serve the same purpose with less discriminatory effect.[726] One enforcement example that relied on disparate impact theory involved a bank's facially neutral policy of allowing its loan officers discretion in pricing loans without requiring manager approval or review.[727] The complaint alleged that African-American

722 *See* Fed. Deposit Insurance Corp., Policy Statement on Discrimination in Lending (Apr. 15, 1994), https://www.fdic.gov/regulations/laws/rules/5000-3860.html.

723 *See* Consent Order, *United States v. Countrywide Fin. Corp. et al.*, No. 2:11-cv-10540-PSG-AJW (C.D. Cal. Dec. 23, 2011). The Order also included additional allegations on the basis of sex with overt evidence. *Id.*

724 Consent Order at 3, *United States v. Countrywide Fin. Corp. et al.*, No. 2:11-cv-10540-PSG-AJW (C.D. Cal. Dec. 23, 2011).

725 *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK, FAIR LENDING: CONSUMER COMPLIANCE EXAMINATION (2010), https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/fair-lending/pub-ch-fair-lending.pdf; *see also* CONSUMER FIN. PROT. BUREAU, EQUAL CREDIT OPPORTUNITY ACT EXAMINATION PROCEDURES (2015), https://files.consumerfinance.gov/f/documents/201510_cfpb_ecoa-narrative-and-procedures.pdf.

726 OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK, FAIR LENDING: CONSUMER COMPLIANCE EXAMINATION 9 (2010).

727 *See* Complaint, *United States v. Sage Bank*, No. 1:15-cv-13969 (D. Mass. Nov. 30, 2015).

and Hispanic borrowers received higher interest rates than non-Hispanic White borrowers due to this policy.[728]

Commentary Box 22: Alternative Data and Disparate Impact

Traditional credit-scoring models rely on data from consumer reports supplied by nationwide CRAs, but there are significant limitations and gaps in this data. For example, roughly 50 million Americans cannot be scored using traditional models because of insufficient information ("thin files") or no information at all ("no files").[729] As a result, they may be denied credit or charged higher rates that are not necessarily commensurate with the consumers' actual default risk. More broadly, consumer advocates have expressed concern 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, as well as by differences in geographic access to banks and other factors.[730]

In recent years, lenders, creditors, CRAs, scoring vendors, and other stakeholders have been attempting to capitalize on new data processing and collection capabilities to improve the predictiveness of credit scoring models. Many of these new efforts are exploring the use of "alternative data" inputs in lieu of or in addition to traditional consumer reports and credit scores. Many types of alternative data are financial in nature, such as information relating to income, recurring expenses, owned assets, property ownership, etc. But some research suggests that nonfinancial data—such as information about social media habits, online search engine history, types of magazine subscriptions, or library visits—may also be predictive of creditworthiness. More than simply reducing creditors' default losses, the efforts to incorporate alternative data have also been billed as a way to expand

728 Complaint at 2, *United States v. Sage Bank*, No. 1:15-cv-13969 (D. Mass. Nov. 30, 2015).

729 FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 12 (2020).

730 NAT'L CONSUMER LAW CTR., PAST IMPERFECT: HOW CREDIT SCORES AND OTHER ANALYTICS "BAKE IN" AND PERPETUATE PAST DISCRIMINATION (2016), https://www.nclc.org/images/pdf/credit_discrimination/Past_Imperfect050616.pdf; Robert Avery, Kenneth Brevoort & Glenn Canner, *Does Credit Scoring Produce a Disparate Impact?*, 40 REAL ESTATE ECON. 965 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2194276; Lisa Rice & Deidre Swesnik, *Discriminatory Effects of Credit Scoring on Communities of Color*, 46 SUFFOLK L. REV. 935 (2013), https://pdfs.semanticscholar.org/7b5e/56d741d9ad848f54650b3ada2d987d00b7be.pdf?_ga=2.96954719.1560807314.1598531912-1403663734.1598531912.

access to credit for populations that historically score poorly on traditional credit models, such as thin-file and no-file consumers.[731] However, scoring model developers and lenders have to evaluate whether using particular alternative information sources will reduce or exacerbate disparate impact along protected-class lines, as well as privacy and other consumer protection considerations.

The most frequently explored types of alternative data include major recurring expenses that are not frequently reflected in reports from the nationwide CRAs (such as rental, utility, and telecom bills) and bank account or other forms of cash-flow data that reflect both income and expenses. For consumers with thin or no credit files, such cash-flow data may provide an alternative way to gain access to credit or lower interest rates. Indeed, a report from FinRegLab researching and analyzing the impact of various credit offerings based on cash-flow data suggests "that cash-flow data holds significant promise for creating more inclusive, efficient, and competitive credit markets."[732] However, some consumer advocates have expressed concerns about including particular types of data, particularly routine reporting of all utility bill payments.[733]

The student loan refinance industry has also experimented with incorporating information regarding borrower degrees into credit underwriting, building in part on a CFPB No-Action Letter (NAL) stating that the agency did not plan to seek enforcement action against a lender that intended to use "school attended," "degree obtained," and "applicant employment history" as underwriting factors.[734] A CFPB

731 U.S. DEP'T OF HOUSING AND URBAN DEV., POL'Y AND ECON. RESEARCH COUNCIL, POTENTIAL IMPACTS OF CREDIT REPORTING PUBLIC HOUSING RENTAL PAYMENT DATA (2019), https://www.huduser.gov/portal/sites/default/files/pdf/Potential-Impacts-of-Credit-Reporting.pdf; NEW YORK CITY COMPTROLLER, BUREAU OF POL'Y AND RESEARCH, MAKING RENT COUNT: HOW NYC TENANTS CAN LIFT CREDIT SCORES AND SAVE MONEY (2017), https://comptroller.nyc.gov/wp-content/uploads/documents/Rent-and-Credit-Report.pdf.

732 FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS (2020).

733 The concerns focus on the risk that scoring models would substantially penalize consumers who fall modestly behind in peak seasons and/or rely on state and local protections that restrict utility cut-offs to prioritize other bills. *See e.g.*, Gillian B. White, *Can the Flaws in Credit Scoring Be Fixed?*, THE ATLANTIC (Jan. 10, 2017), https://www.theatlantic.com/business/archive/2017/01/credit-score/512702/; *see also* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS 15–16 (2020).

734 Consumer Fin. Prot. Bureau, No-Action Letter to Upstart Network on Automated Underwriting Model (Sept. 14, 2017), https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter.pdf, https://files.consumerfinance.gov/f/documents/201709_cfpb_upstart-no-action-letter-request.pdf.

blog on the NAL indicated promising inclusion and fair lending results from the NAL recipient's lending program.[735] Still, some advocates have argued that factoring in the identity of the higher educational institution could act as a proxy for demographics and have the effect of excluding populations historically less likely to attain advanced higher education degrees—a trend that could exacerbate the credit-access issues that disparate impact theory is intended to ameliorate.[736]

2. Information Requests

ECOA's implementing Regulation B generally prohibits creditors from inquiring about the race, color, religion, national origin, or sex of an applicant in connection with a credit transaction.[737] There are limited exceptions to this rule that include collecting information for monitoring purposes in relation to credit secured by real estate, which is required by other federal laws,[738] and determining an applicant's eligibility for a special purpose credit program.[739] Additionally, creditors may collect information in connection with a self-test[740] being conducted by the creditor.[741]

735 Consumer Fin. Prot. Bureau, *An update on credit access and the Bureau's first No-Action Letter*, CFPB Blog (Aug. 6, 2019), https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/.

736 *See e.g.*, STUDENT BORROWER PROT. CTR., EDUCATIONAL REDLINING (2020), https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf; Senators Sherrod Brown, Elizabeth Warren, & Kamala Harris, Report on the Use of Educational Data to Make Credit Determinations (July 30, 2020), https://www.banking.senate.gov/imo/media/doc/Review%20-%20Use%20of%20Educational%20Data.pdf; *see also* Karen W. Arenson, *Some Lenders Are Setting Rates College by College*, N.Y. TIMES (June 19, 2007), https://www.nytimes.com/2007/06/19/us/19loans.html?_r=1&oref=slogin.

737 12 C.F.R. § 1002.5(b).

738 *See* 12 C.F.R. § 1002.13. Please reference 12 C.F.R. § 1002.5(a)(4) for other permissible purposes for collecting information related to the Home Mortgage Disclosure Act. Once implemented, Section 1071 of DFA will establish another exception under ECOA requiring creditors to collect and maintain certain data in connection with loan applications received by small businesses.

739 Special purpose credit programs are designed to meet the needs of individuals who would otherwise be denied credit without the program. In this situation, creditors may be permitted to obtain information that would otherwise be prohibited. For example, if financial need is one of the criteria under the special purpose program, the creditor could review information concerning the marital status of the applicant, such as alimony payments, child support, and the spouse's income. *See* 12 C.F.R. § 1002.8 for the guidelines around special purpose credit programs.

740 A "self-test" is defined as "any program, practice, or study that: (i) [i]s designed and used specifically to determine the extent of a creditor's compliance with [ECOA]. . .; and (ii) [c]reates data or factual information that is not available and cannot be derived from loan application files or other records related to credit transactions." 12 C.F.R. § 1002.15(b).

741 *See* 12 C.F.R. § 1002.15 for requirements necessary to collect information in connection with self-testing.

Regulation B further provides rules when creditors are permitted to inquire into an applicant's marital status. When an applicant applies for an individual credit, creditors are only permitted to inquire into marital status if the transaction would be secured, or if the applicant resides in a community property state or lists property or assets supporting the debt that are located in such a state.[742] These limited exceptions curtail the potential for discrimination. If the applicant is applying for joint credit, however, a creditor may inquire into the applicant's marital status regardless of whether the credit is secured.[743] In addition to marital status, Regulation B provides guidelines for creditors when inquiring into income from alimony, child support, or separate maintenance income, as well as an applicant's immigration or residency status.[744] These inquiries are permitted because they directly relate to an applicant's ability to repay and a creditor's ability to collect on any debts. Creditors may also obtain age-related data as necessary to determine an applicant's ability to enter into a contract; age can also be used as a factor during underwriting in certain, narrow circumstances.[745]

3. Information Use

Creditors are generally prohibited from considering prohibited bases[746] in underwriting, subject to certain exceptions, such as payment of alimony or receipt of public assistance income, (which may also implicate marital status and age, respectively) if such information affects the applicant's ability to repay.[747] In addition to prohibiting explicit consideration of prohibited bases, ECOA also prohibits creditors from considering factors that act as a proxy for a prohibited basis, such as providing preferential treatment to certain zip codes known to be inhabited by primarily White borrowers, or consideration of whether an applicant is retired, acting as a proxy for age.[748] Regulation B provides specific rules concerning the use of information in evaluating applications. These rules cover how creditors may use information, such as age[749] and marital status in a way that does not violate the purpose of the statute, and in some instances, such as the "shoebox rule," consumers can require lenders to consider information. For a summary of Regulation B's evaluation limitations based on type of information, please see Appendix C.

742 12 C.F.R. § 1002.5(d)(1).

743 12 C.F.R. § 1002.5(d)(1). The creditor is limited to using the terms "married," "unmarried," and "separated." *Id.*

744 *See* 12 C.F.R. §§ 1002.5(d)(2), 1002.5(e).

745 *See* 12 C.F.R. § 1002.6(b)(2).

746 "Prohibited basis" is defined as race, color, religion, national origin, sex, marital status, or age (provided that the applicant has the capacity to enter into a binding contract); the fact that all or part of the applicant's income derives from any public assistance program; or the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act or any state law upon which an exemption has been granted by the CFPB. 12 C.F.R. § 1002.2(z).

747 *See* 12 C.F.R. §§ 1002.6(b)(5), 1002.6(b)(2)(iii).

748 *See* CONSUMER FIN. PROT. BUREAU, EQUAL CREDIT OPPORTUNITY ACT EXAMINATION PROCEDURES (2015).

749 Although age is a prohibited basis, Regulation B provides that creditors may use age in "an empirically derived, demonstrably and statistically sound, credit scoring system . . . provided that the age of an elderly applicant is not assigned a negative factor or value." 12 C.F.R. § 1002.6(b)(2)(ii).

4. Notification to Applicants

If a creditor takes an adverse action against an applicant, the creditor must provide notification to the applicant in writing that contains certain information to allow an applicant to contact the creditor and better understand how the decision was reached.[750] An "adverse action" is defined as:

- a refusal to grant credit in substantially the amount or on substantially the terms requested in an application unless the creditor makes a counteroffer (to grant credit in a different amount or on other terms) and the applicant uses or expressly accepts the credit offered;

- a termination of an account or an unfavorable change in the terms of an account that does not affect all or substantially all of a class of the creditor's accounts; or

- a refusal to increase the amount of credit available to an applicant who has made an application for an increase.[751]

Within the adverse action notice, the creditor must provide the applicant with (i) a statement about the action taken; (ii) a statement regarding ECOA and its purpose;[752] (iii) the name and address of the creditor; (iv) a statement about the reasons the action was taken or disclosure of the consumer's right to receive such a statement upon request; and (v) the name and address of the federal agency that administers compliance with respect to that creditor.[753] When providing the applicant with a statement of reasons, Regulation B requires the statement "must be specific and indicate to the principal reason(s) the action was taken."[754] ECOA adverse action notices have a slightly different focus than FCRA adverse action and risk-based pricing

750 *See* 12 C.F.R. § 1002.9(a).

751 12 C.F.R. § 1002.2(c). The term adverse action does not include: (i) a change in the terms of an account expressly agreed to by an applicant; (ii) any action or forbearance relating to an account taken in connection with inactivity, default, or delinquency as to that account; (iii) a refusal or failure to authorize an account transaction at point of sale or loan, except when the refusal is a termination or an unfavorable change in the terms of an account that does not affect all or substantially all of a class of the creditor's accounts, or when the refusal is a denial of an application for an increase in the amount of credit available under the account; (iv) a refusal to extend credit because applicable law prohibits the creditor from extending the credit requested; or (v) a refusal to extend credit because the creditor does not offer the type of credit or credit plan requested. *Id.*

752 12 C.F.R. § 1002.9(b)(1) provides specific language that satisfies the requirement of this statement.

753 12 C.F.R. § 1002.9(a)(2)(ii). The disclosure required must include the name, address, and telephone number of the person or office from which the statement of reasons behind the decision can be obtained. *Id.* If the creditor elects to provide the reasons orally, the creditor must also inform the applicant of his or her right to have them confirmed in writing within 30 days of receiving the applicant's written request for confirmation. *Id.*

754 12 C.F.R. § 1002.9(b)(2). Although Regulation B does not specify a required number of reasons that must be provided, the official interpretations suggest more than four reasons would be unhelpful to consumers. 12 C.F.R. cmt. 1002.9(b)(2)-1–4.

notices, which are structured in part to help consumers determine whether data inaccuracies may need to be corrected.[755]

The notice of adverse action or a counteroffer must be provided to applicants who do not qualify for the credit requested within 30 days after the creditor receives a completed application.[756] Creditors also have 30 days to provide notification after taking adverse action on an incomplete application or an existing account.[757] If the creditor provides a counteroffer rather than an adverse action notice and the applicant does not accept the offer, the creditor has a further 90 days after providing notice of the counteroffer to provide the applicant with an adverse action notice with respect to the original request for credit.[758]

755 *Compare* 12 C.F.R. § 1002.9, *with* 12 C.F.R. §§ 1022.72, 1022.74(b).

756 12 C.F.R. § 1002.9(a)(1)(i).

757 12 C.F.R. § 1002.9(a)(1)(ii)–(iii). Regulation B provides certain notice alternatives for incomplete applications which can be found at 12 C.F.R. 202.9(c).

758 12 C.F.R. § 1002.9(a)(iv). Regulation B also provides notification options for small-volume creditors, withdrawals of approved applications, multiple applicants, and applications submitted by a third party, which can be found at 12 C.F.R. 1002.9(d)–(g). Additional information may be included in adverse action and risk-based pricing notices related to FCRA. See Section IV.E.2.a. for more information on these requirements.

VII. Unfair, Deceptive, and/or Abusive Acts or Practices (UDA(A)P) Authority

A. Introduction

Section 5 of the Federal Trade Commission Act (the "FTC Act")[759] prohibits covered entities from engaging in "unfair or deceptive acts or practices in or affecting commerce,"[760] commonly known as "UDAPs."[761] In drafting the FTC Act, Congress opted for a principles-based approach rather than enumerating the types of acts or practices that would be unfair or deceptive.[762] In 2010, DFA added a prohibition against "unfair, deceptive, or abusive acts or practices" by providers of consumer financial products or services, as well as service providers to those entities, known as a "UDAAP."[763]

As discussed below, federal regulators, including not only the FTC and CFPB but also prudential agencies, have used their "UDA(A)P"[764] powers with respect to financial data in relatively limited ways to date. The FTC's UDAP powers are the primary means by which the FTC addresses data security and privacy issues for general commercial entities. In financial services, however, UDA(A)P authority has tended to play a secondary role because regulators

759 Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. § 41 *et seq.*).

760 15 U.S.C. § 45. Its scope has also been found to include acts or practices involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States. 15 U.S.C. § 45(a)(4)(A).

761 In addition to its Section 5 powers, the FTC also enforces a variety of other consumer protection statutes that prohibit specifically defined practices, many of which specify that violations are to be treated as if they were "unfair or deceptive" acts or practices under Section 5 of the FTC Act. *See, e.g.*, FAA Reauthorization Act of 2018, 49 U.S.C. § 44801 (providing for UDAP for a person using drones to violate a privacy policy); Mortgage-Related Provisions of Omnibus Appropriations Act of 2009, 12 U.S.C. § 5538 (empowering the FTC to conduct initial rulemaking on UDAPs regarding mortgage loans); Opioid Addiction Recovery Fraud Prevention Act of 2018, 15 U.S.C. § 45d (authorizing FTC to seek civil penalties for UDAPs related to any substance use disorder treatment service or product); Postal Reorganization Act of 1970, 39 U.S.C. § 3009 (permitting FTC to prosecute as UDAP any use of mails to send unordered merchandise); Telephone Disclosure and Dispute Resolution Act of 1992, 15 U.S.C. §§ 5701–5724 (granting UDAP enforcement authority to FTC over pay-per-call services).

762 A conference report accompanying the FTC Act's passage in 1924 stated that "It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task." H.R. REP. NO.1142, at 18–19 (1914) (Conf. Rep.).

763 *See* 12 U.S.C. §§ 5531, 5536(a)(1)(B) (emphasis added); CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 1 (2012), https://files.consumerfinance.gov/f/documents/102012_cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures.pdf.

764 Prior to 2010, the commonly used acronym with respect to the prohibition of unfair or deceptive acts and practices was "UDAP." The addition by DFA of "abusive" to the standard for providers of consumer financial products and services has rendered the acronym as "UDAAP" when applied to violations under DFA. *See* CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 1 (2012). This paper uses the acronym "UDA(A)P" when referring to both standards. When referring to violations under the FTC Act specifically, the document will use the term "UDAPs," and when referring to violations under DFA specifically, the document will use "UDAAP."

often can rely on other laws, such as GLBA and FCRA, in the event of financial data-related violations. As such, UDA(A)P violations often have been asserted as additional causes of action alongside violations of more specific statutes. The broad, principle-based nature of regulators' UDA(A)P powers, however, means that regulators' UDA(A)P authority has the potential to be used flexibly in new ways to correct new or evolving market practices that regulators view as harmful to consumers. Trends in UDA(A)P enforcement are thus important for market participants to track given the rapid changes taking place in the financial services sector.

B. Entities Covered

As discussed further below, the prohibitions against UDA(A)Ps under the FTC Act and DFA apply in aggregate to a broad swath of market actors. The FTC Act applies to nearly all commercial businesses in the United States, with the exception of insurance companies and telecommunications firms.[765] The breadth of this jurisdiction means that the FTC may apply its UDAP authority to oversee financial data practices of entities that would not typically be deemed to be in the business of financial services or otherwise subject to GLBA, EFTA, or FCRA. DFA prohibitions against unfair, deceptive, or abusive acts or practices apply to all "covered persons" as defined under Title X of DFA, including banks and credit unions,[766] non-bank providers of consumer financial products and services, and their service providers.[767]

C. Data Covered

UDA(A)P authority constitutes a broad, principles-based prohibition on certain harmful acts and practices with respect to consumers, including but not limited to harmful acts and practices related to consumer financial data. The FTC has also interpreted the UDAP authority under Section 5 of the FTC Act to extend to acts and practices injurious to businesses and relating to small business financial data.[768] As such, regulators' UDA(A)P authority covers both consumer

765 The FTC also has jurisdiction under Section 5(a) of the FTC Act over acts involving foreign commerce that cause or are likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States. 15 U.S.C. § 45(a)(4)(A).

766 The prudential regulators may also enforce their UDAP authority with respect to "institution-affiliated parties" of insured depository institutions. *See, e.g.*, FED. DEPOSIT INS. CORP., CONSUMER COMPLIANCE EXAMINATION MANUAL, VII. UNFAIR AND DECEPTIVE PRACTICES—FEDERAL TRADE COMMISSION ACT 1 (2018), https://www.fdic.gov/regulations/compliance/manual/7/vii-1.1.pdf. "Institution-affiliated parties" include directors, officers, and employees of the financial institution, as well as controlling shareholders; shareholders participating in the affairs of the institution; and, in certain cases, independent contractors. *See* 12 U.S.C. § 1813(t).

767 See Section II.B. for a discussion of the definition of "covered persons" under Title X of DFA.

768 *See, e.g.*, Complaint, *F.T.C. v. Equifax, Inc.*, No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019) (The FTC brought allegations under Section 5 for unfairness related to failure to take adequate steps to protect the information security of small business data); Stipulated Order for Permanent Injunction and Monetary Relief, *F.T.C. v. Equifax, Inc.*, No. 1:19-mi-99999-UNA , slip op. (N.D. Ga. July 22, 2019); *see also F.T.C. v. IFC Credit Corp.*, 543 F. Supp. 2d 925, 943 (N.D. Ill. 2008) ("The FTC has construed the term 'consumer' to include businesses as well as individuals. Deference must be given to the interpretation of the agency charged by Congress with the statute's implementation.").

financial data and, in the case of the FTC Act, business financial data, but is not otherwise limited to specific types of data.

D. Oversight

1. Federal Trade Commission

The FTC Act provides the FTC with rulemaking and enforcement authority, but not supervisory powers, related to the prohibition on UDAPs, although as noted above and discussed further below there are substantial procedural constraints on the agency in issuing UDAP rules.[769] Under Section 18 of the FTC Act, the FTC is authorized to prescribe "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce" within the meaning of Section 5(a)(1) of the Act.[770] The FTC's enforcement authority permits it to issue administrative cease-and-desist orders[771] and to seek judicially ordered injunctive relief[772] and civil penalties for violating cease-and-desist orders.[773] As discussed below, the FTC's rulemaking and enforcement authority overlaps with that of the CFPB with respect to covered persons under the CFPB's jurisdiction.

Some scholars have argued that specific legislation is needed to give the FTC express authority to take action under well-defined regulations against companies that experience data breaches.[774] Other information privacy law scholars counter that "FTC enforcement has certainly changed over the course of the past fifteen years, but the trajectory of development has followed a predictable set of patterns. These patterns are those of common law development."[775]

---

769 *See* 15 U.S.C. § 45. The FTC's rulemaking authority under Section 5 of the FTC Act is subject to strict procedural requirements over-and-above those imposed by the Administrative Procedural Act ("APA"). *See* 15 U.S.C. § 57a. In addition to the APA requirements for rulemaking, the FTC is required to "(A) publish a notice of proposed rulemaking stating with particularity the text of the rule, including any alternatives, which the Commission proposes to promulgate, and the reason for the proposed rule; (B) allow interested persons to submit written data, views, and arguments, and make all such submissions publicly available; (C) provide an opportunity for an informal hearing in accordance with subsection (c); and (D) promulgate, if appropriate, a final rule based on the matter in the rulemaking record (as defined in subsection (e)(1)(B)), together with a statement of basis and purpose." *Id.* at § 57a(b)(1). Congress has the ability to review each step in this process. *Id.* at § 57a.

770 15 U.S.C. § 57(a).

771 *See* 15 U.S.C. § 45(b).

772 15 U.S.C. § 53(b).

773 15 U.S.C. § 45(l), (m); *see also* 16 C.F.R. § 1.98(c) (adjusting civil monetary penalties for inflation).

774 *See, e.g.*, Michael D. Scott, *The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008), http://www.administrativelawreview.org/wp-content/uploads/2014/04/The-FTC-The-Unfairness-Doctrine-and-Data-Security-Breach-Litigation-Has-the-Commission-Gone-Too-Far_.pdf.

775 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 608 (2014), https://cyberlaw.stanford.edu/files/publication/files/SSRN-id2312913.pdf; *see generally The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury:*

In 2014, Wyndham Hotels and Resorts challenged the FTC's authority to engage in financial data privacy oversight through enforcement.[776] Wyndham argued that Congress did not give the FTC the necessary authority to regulate data security through the FTC's general authority to regulate UDAPs, pointing to a lack of clear statutory authority over data security and a more narrowly tailored legislative intent to regulate data security through FCRA, GLBA, and COPPA.[777] The U.S. Court of Appeals for the Third Circuit, however, disagreed with Wyndham's arguments and held that a company's data security conduct may constitute unfair acts or practices such that the FTC has authority to enforce Section 5 of the FTC Act.[778]

2. Consumer Financial Protection Bureau

Under DFA the CFPB is authorized to take enforcement actions against covered persons under CFPB jurisdiction, as well as their service providers, to prevent UDAAPs in connection with any transaction with a consumer for a consumer financial product or service or the offering of a consumer financial product or service.[779] The CFPB may also prescribe rules identifying UDAAPs in connection with such consumer financial products or services, including rules that include requirements designed to prevent UDAAPs.[780]

The CFPB's rulemaking and enforcement powers over consumer protection, including UDAAPs, overlap with those of the FTC with regard to entities under the CFPB's jurisdiction. As a result, the two agencies have entered into a Memorandum of Understanding to coordinate their consumer protection efforts for consumer financial services, including rulemaking, guidance, and enforcement actions concerning UDAAPs by covered persons.[781] Civil penalties for UDAAP violations, like Section 1033, range from $1,000 to $1,000,000 per day the violation continues,

---

Hearing Before the H. Comm. on Oversight and Gov't Reform, 113th Cong. (2014) (statement of Woodrow Hartzog, Associate Professor of Law, Samford University's Cumberland School of Law).

776 *See F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015). The data at issue in the Wyndham case included both financial data (payment card account numbers, expiration dates, and security codes) and non-financial data (names, home addresses, email addresses, and telephone numbers). While the case stands for the general proposition regarding the FTC's ability to enforce data security standards, it is equally and importantly applicable to the financial data at issue as well.

777 *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015) ("Wyndham contends these 'tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field.' Wyndham Br. at 25."). Wyndham relied on a similar argument that had prevailed against the FDA regarding that agency's ability to mandate disclaimers on tobacco packaging. *See Food & Drug Admin. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000).

778 *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247–49 (3d Cir. 2015).

779 *See* 12 U.S.C. § 5531(a).

780 *See* 12 U.S.C. § 5531(b).

781 *See* FTC-CFPB, MEMORANDUM OF UNDERSTANDING (Feb. 25, 2019), https://www.ftc.gov/system/files/documents/cooperation_agreements/ftc-cfpb_mou_225_0.pdf.

depending upon the violation tier level.[782] Unlike the FTC, however, the CFPB also has supervisory authority over certain covered persons, including with respect to UDAAPs.[783] The CFPB has leveraged that power to conduct supervisory examinations that impact financial data issues, including conducting targeted data security and cybersecurity examinations that assessed "risks to consumers posed by potential cybersecurity lapses and to markets for consumer financial products and services."[784] That supervisory oversight, however, has been limited in practice to date.[785]

Commentary Box 23: Viability and Likelihood of UDA(A)P Rulemaking

Although the FTC has traditionally relied on Section 5's enforcement powers to address data issues in general commerce, at a 2018 FTC hearing one FTC commissioner noted "that case-by-case adjudication may simply be too slow and cumbersome to produce specific and clear standards adequate to the needs of businessmen, the private bar, and the government agencies."[786] According to this commissioner, UDAP rulemaking would provide three critical benefits: (i) clear rules and clear notice, (ii) reduced costs and time for compliance, and (iii) transparency and civil participation.[787] Despite these benefits, FTC rulemaking related to UDAPs is severely limited by the "extensive hurdles posed by the Magnuson-Moss Warranty Federal Trade Commission Improvements Act."[788]

The FTC's Credit Practices Rule, which was issued in 1984 to address wage assignments and various other back-end credit practices, illustrates some of the procedural hurdles. After the FTC issued the Credit Practices Rule under its UDAP

782 *See* 12 U.S.C. § 5565(c).

783 *See* 12 U.S.C. §§ 5514, 5515(b)(1), 5516(b).

784 GOV'T ACCOUNTABILITY OFFICE, GAO-18-559, DATA PROTECTION: ACTIONS TAKEN BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 26 (2018), https://www.gao.gov/assets/700/694158.pdf.

785 *See* GOV'T ACCOUNTABILITY OFFICE, GAO-19-196, CONSUMER DATA PROTECTION: ACTIONS NEEDED TO STRENGTHEN OVERSIGHT OF CONSUMER REPORTING AGENCIES 26-27 (2019), https://www.gao.gov/assets/700/697026.pdf ("CFPB staff said that they do not routinely consider data security risks during their examination prioritization process and have not reassessed the process to determine how to incorporate such risks going forward.").

786 Hearing #1 on Competition and Consumer Protection in the 21st Century, FTC-2018-0074 (Sept. 6, 2018) (comment of Commissioner Rohit Chopra, Federal Trade Commission) https://www.ftc.gov/system/files/documents/public_statements/1408196/chopra_-_comment_to_hearing_1_9-6-18.pdf.

787 Hearing #1 on Competition and Consumer Protection in the 21st Century, FTC-2018-0074 (Sept. 6, 2018) (describing benefits of rulemaking over enforcement by FTC related to Section 5 "unfair competition" doctrine).

788 Hearing #1 on Competition and Consumer Protection in the 21st Century, FTC-2018-0074 (Sept. 6, 2018), at 8.

powers, an association of over 550 consumer finance and small-loan companies contested it, arguing that it exceeded the FTC's regulatory authority and was not supported by the evidence in the rulemaking record.[789] As the court in that matter explained, the FTC published its initial notice of rulemaking on the subject on April 11, 1975.[790] After a comment-and-hearing stage, promulgation of multiple staff reports, and a 60-day comment period, the FTC then recommended a final modified proposed rule on April 14, 1983.[791] The FTC then invited prior rulemaking participants to present their views orally and ultimately published a final rule on March 1, 1984—nearly nine years after the original notice of proposed rulemaking.[792] Nonetheless, the rule was still met with challenge for failing to have support "by substantial evidence in the record."[793] Given the onerous burdens that the FTC must meet to promulgate such rules, the length of time those procedural steps take, and the speed at which innovations in financial technology and data-sharing occur, FTC UDAP rulemaking seems an unlikely path for responding to changes in financial or general data practices. Indeed, even without the FTC's procedural constraints, any UDA(A)P rulemaking by either the FTC or CFPB would be hindered by the speed of market and technological changes and the difficulties in crafting a single standard to govern diverse financial data market participants.

The CFPB has acknowledged industry concerns about standards for defining "abusive" practices under DFA, but has provided no indications that it is planning a rulemaking on financial data matters specifically. In her remarks introducing a June 2019 symposium on abusive acts or practices, CFPB Director Kathleen L. Kraninger indicated that the agency did not currently see the need for any rulemakings related to either unfairness or deception, stating that:

[F]or more than 80 years, the Federal Trade Commission has used its authority under the FTC Act to address unfair and deceptive acts and practices that harm consumers. Statutory language, regulations, agency policy statement, and a

789 *See generally Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957 (D.C. Cir. 1985).

790 *Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 962 (D.C. Cir. 1985).

791 *Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 963 (D.C. Cir. 1985).

792 *Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 963 (D.C. Cir. 1985).

793 *Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 984–88 (D.C. Cir. 1985).

substantial body of caselaw have clarified the metes and bounds of these concepts. Over time, this has provided reasonably clear standards for market participants to use in assessing whether their own conduct comports with laws prohibiting unfair and deceptive acts and practices.[794]

While the CFPB first announced in the Fall 2018 Unified Regulatory Agenda that it was "considering whether rulemaking or other activities may be helpful to further clarify the meaning of abusive acts or practices" and issued guidance regarding when it will bring claims for abusive conduct, it has not yet issued any notices of proposed rulemaking or advanced notices of proposed rulemakings related to UDAAPs.[795] Moreover, as Congress has excluded the CFPB from rulemaking authority over the more specific information security and data privacy regimes such as GLBA, any CFPB regulation on this subject under its UDAAP authority would be likely to trigger litigation challenging its authority to do so. Thus, given the current legal and practical constraints, the likelihood of UDAAP rulemaking with respect to data issues in the financial context or more generally appears low.

3. Prudential Banking Regulators

The prudential banking regulators have supervisory and enforcement oversight of entities within their jurisdiction with respect to UDAPs resulting from violations of the FTC Act.[796] The OCC,[797]

794 Kathleen L. Kraninger, Director of the Consumer Fin. Prot. Bureau, Speech at the Abusive Acts or Practices Symposium (June 25, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-kathleen-l-kraninger-speech-symposium-abusive-acts-or-practices/.

795 Consumer Fin. Prot. Bureau, Semiannual Regulatory Agenda, pmbl. (Aug. 30, 2018), https://www.reginfo.gov/public/jsp/eAgenda/StaticContent/201810/Preamble_3170.html. In January 2020, the CFPB issued supervisory guidance regarding when it would consider bringing enforcement actions under the abusiveness prong.

796 *See* FED. DEPOSIT INS. CORP., CONSUMER COMPLIANCE EXAMINATION MANUAL, VII. UNFAIR AND DECEPTIVE PRACTICES—FEDERAL TRADE COMMISSION ACT 1 (2018) ("THE BANKING AGENCIES HAVE AUTHORITY TO ENFORCE SECTION 5 OF THE FTC ACT FOR THE INSTITUTIONS THEY SUPERVISE."); OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: UNFAIR OR DECEPTIVE ACTS OR PRACTICES AND UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES 2 (2020), https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/unfair-deceptive-act/pub-ch-udap-udaap.pdf.

797 OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC AL 2002-3, GUIDANCE ON UNFAIR OR DECEPTIVE ACTS OR PRACTICES (2002), https://www.ots.treas.gov/news-issuances/advisory-letters/2002/advisory-letter-2002-3.pdf.

FDIC,[798] FRB,[799] and NCUA[800] have each issued general supervisory guidance regarding the definition of "unfair and deceptive acts and practices" that tracks FTC guidance on UDAPs. In addition to their authority under Section 5 of the FTC Act, the prudential bank regulators also have supervisory and enforcement jurisdiction for depository institutions with total assets of $10 billion or less.[801]

On March 11, 2004, the FDIC and the FRB issued a joint statement regarding the agencies' responsibilities to enforce the prohibitions against UDAPs as they apply to state-chartered banks.[802] The statement contained a discussion of managing risks relating to UDAP and general guidance on measures that state-chartered banks can take to avoid engaging in such acts or practices, including best practices. The agencies stated that "[i]n analyzing a particular act or practice, the Agencies will be guided by the body of law and official interpretations for defining unfair or deceptive acts or practices developed by the courts and the FTC."[803]

4. States

States have authority to bring suit for UDAAPs under DFA.[804] State attorneys general may generally bring such actions against any defendant, subject to personal jurisdiction limitations, but may only bring actions against national banks or federal savings associations "to enforce a regulation prescribed by the [CFPB] under a provision of this title and to secure remedies under provisions of this title or remedies otherwise provided under other law."[805] State regulators may also bring actions against any "entity that is State-chartered, incorporated, licensed, or otherwise authorized to do business under State law."[806] Before initiating any such actions,

---

798 FED. DEPOSIT INS. CORP., CONSUMER COMPLIANCE EXAMINATION MANUAL, VII. UNFAIR AND DECEPTIVE PRACTICES—FEDERAL TRADE COMMISSION ACT (2018); *SEE ALSO* GOV'T ACCOUNTABILITY OFFICE, GAO-18-254, FINANCIAL TECHNOLOGY: ADDITIONAL STEPS BY REGULATORS COULD BETTER PROTECT CONSUMERS AND AID REGULATORY OVERSIGHT 48–49 (2018), https://www.gao.gov/assets/700/690803.pdf ("FDIC staff told us that FDIC applies the same standards as FTC in determining whether an act or practice is unfair or deceptive . . . .").

799 FED. RESERVE BD., CONSUMER COMPLIANCE HANDBOOK, FEDERAL TRADE COMMISSION ACT—SECTION 5, APPENDIX: STATEMENT ON UNFAIR OR DECEPTIVE ACTS OR PRACTICES (2016).

800 NAT'L CREDIT UNION ADMIN., FED. CONSUMER FIN. PROT. GUIDE, COMPLIANCE MGMT., UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAP) (2019), https://www.ncua.gov/regulation-supervision/manuals-guides/federal-consumer-financial-protection-guide/compliance-management/unfair-deceptive-or-abusive-acts-or-practices-udaap.

801 12 U.S.C. §§ 5516, 5581; *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: UNFAIR OR DECEPTIVE ACTS OR PRACTICES AND UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES 2 (2020).

802 *See* Fed. Reserve Bd. and Fed. Deposit Ins. Corp., Joint Statement on Unfair or Deceptive Acts or Practices by State-Chartered Banks (Mar. 11, 2004), https://www.federalreserve.gov/boarddocs/press/bcreg/2004/20040311/attachment.pdf.

803 Fed. Reserve Bd. and Fed. Deposit Ins. Corp., Joint Statement on Unfair or Deceptive Acts or Practices by State-Chartered Banks (Mar. 11, 2004), at 2.

804 *See* 12 U.S.C. § 5552.

805 12 U.S.C. § 5552(a).

806 12 U.S.C. § 5552(a)(1).

states need to "timely provide" the CFPB with a copy of the complaint and a written notice, which permits the CFPB to intervene in the action as a party or appeal any order or judgment to the same extent as any other party in the proceeding may.[807] Some states have brought UDAAP claims using this authority.[808]

In addition, all fifty states and the District of Columbia have passed consumer protection laws that prohibit unfair or deceptive acts or practices.[809] For example, New York's Consumer Protection from Deceptive Acts and Practices Law provides that "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."[810] Many states import federal precedent for defining unfair and deceptive conduct and permit consumers to bring suit to enforce their laws and recover monetary damages,[811] though private suits are not available under the federal UDA(A)P provisions.

E. Substantive Requirements

1. Overview of Core Definitions

Due to the broad reach of the FTC Act and DFA, nearly all businesses are prohibited from engaging in unfair or deceptive acts or practices, including those in connection with financial data.[812] In addition, covered persons offering or providing a consumer financial product or service are also prohibited from engaging in abusive acts or practices with respect to financial data pertaining to consumer financial products or services.[813]

In its supervisory guidance, the CFPB has noted that the principles of unfair and deceptive practices in DFA are similar to those under Section 5 of the FTC Act and that the FTC "and prudential banking regulators have applied these standards through case law, official policy

---

807 12 U.S.C. § 5552(b)(1). The written notice must identify the parties to the action, the alleged facts underlying the proceeding, and "whether there may be a need to coordinate the prosecution of the proceeding so as not to interfere with any action, including any rulemaking, undertaken by the Bureau, a prudential regulator, or another Federal agency." *Id.* at § 5552(b)(1)(C).

808 *See, e.g.*, *Illinois v. Alta Colleges, Inc.*, No. 14-3786, 2014 WL 4377579 (N.D. Ill. Sept. 4, 2014); *Pennsylvania v. Navient Corp.*, 354 F. Supp. 3d 529 (M.D. Pa. 2018); *Office of Attorney Gen. v. Berger Law Grp., P.A.*, No. 14-1825, 2015 WL 5922933 (M.D. Fla. Oct. 9, 2015).

809 *See generally* CAROLYN L. CARTER, NAT'L CONSUMER LAW CTR., CONSUMER PROTECTION IN THE STATES: A 50-STATE REPORT ON UNFAIR AND DECEPTIVE ACTS AND PRACTICES STATUTES (2009), https://www.nclc.org/images/pdf/udap/report_50_states.pdf.

810 N.Y. GEN. BUS. LAW § 349.

811 *See, e.g.*, ALA. CODE § 8-19-10; FLA. STAT. § 501.211; ME. STAT. tit. 5, § 213; N.J. STAT. ANN. § 56:8-2.12; UTAH CODE ANN. § 13-11-19.

812 *See* 15 U.S.C. § 45; 12 U.S.C. § 5531.

813 *See* 12 U.S.C. § 5531.

statements, guidance, examination procedures, and enforcement actions that may inform CFPB."[814] In January 2020, the CFPB issued a statement of policy to clarify when it intends to bring enforcement actions for "abusive" acts or practices.[815]

a. Unfair

An act or practice is unfair if it causes or is likely to cause consumers substantial injury that is not reasonably avoidable and if the substantial injury is not outweighed by countervailing benefits to consumers or to competition.[816] In determining whether an act or practice is unfair, regulators may consider established public policies as evidence to be considered with all other evidence, although such public policy considerations may not serve as a primary basis for their determination.[817]

A substantial injury "typically takes the form of monetary harm, such as fees or costs paid by consumers because of the unfair act or practice" but could include nonmonetary harm as well.[818] An injury "is not reasonably avoidable by consumers when an act or practice interferes with or hinders a consumer's ability to make informed decisions or take action to avoid that injury."[819] The inability to make informed decisions may result from an entity withholding or failing to generate critical data that renders consumers without the ability to make informed comparison, from overt coercion, or from undue influence over highly susceptible classes of purchasers.[820]

---

814 CONSUMER FIN. PROT. BUREAU, SUPERVISION AND EXAMINATION MANUAL, UNFAIR, DECEPTIVE OR ABUSIVE ACTS OR PRACTICES UDAAP 1 (2012).

815 Consumer Fin. Prot. Bureau, Statement of Policy Regarding Prohibition on Abusive Acts or Practices (Jan. 24, 2020), https://files.consumerfinance.gov/f/documents/cfpb_abusiveness-enforcement-policy_statement.pdf.

816 *See* 12 U.S.C. § 5531(c); 15 U.S.C. § 45(n).

817 *See* 12 U.S.C. § 5531(c).

818 CONSUMER FIN. PROT. BUREAU, CFPB BULL. 2013-07, PROHIBITION OF UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES IN THE COLLECTION OF CONSUMER DEBTS 2 (2013), https://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf; *see also* Fed. Trade Comm'n, Policy Statement on Unfairness (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness; CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 2 (2012); FED. RESERVE BD., CONSUMER COMPLIANCE HANDBOOK, FEDERAL TRADE COMMISSION ACT—SECTION 5, APPENDIX: STATEMENT ON UNFAIR OR DECEPTIVE ACTS OR PRACTICES 8 (2016).

819 CONSUMER FIN. PROT. BUREAU, CFPB BULL. 2013-07, PROHIBITION OF UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES IN THE COLLECTION OF CONSUMER DEBTS 2 (2013); *see also* Fed. Trade Comm'n, Policy Statement on Unfairness (Dec. 17, 1980).

820 Fed. Trade Comm'n, Policy Statement on Unfairness (Dec. 17, 1980) ("Finally, the injury must be one which consumers could not reasonably have avoided. . . . Sellers may adopt a number of practices that unjustifiably hinder such free market decisions. Some may withhold or fail to generate critical price or performance data, for example, leaving buyers with insufficient information for informed comparisons. Some may engage in overt coercion, as by dismantling a home appliance for 'inspection' and refusing to reassemble it until a service contract is signed. And some may exercise undue influence over highly susceptible classes of purchasers, as by promoting fraudulent 'cures' to seriously ill cancer patients."); *see also* CFPB, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 2 (2012) ("A key question is not whether a consumer could have made a better choice. Rather, the question is whether an act or practice hinders a consumer's decision-making. For example, not having access to important information could prevent consumers from comparing available alternatives, choosing those that are most desirable to them, and avoiding those that are inadequate or unsatisfactory. In addition, if almost all market participants engage in a practice, a consumer's incentive to search elsewhere for better terms is reduced, and the practice may not be reasonably avoidable.").

b. Deceptive

Deceptive acts or practices involve a material representation, omission, or practice that is likely to mislead a consumer acting reasonably in the circumstances.[821] To the extent that the representation or practice primarily impacts a particular group, the reasonableness of the consumer is understood from the perspective of a member of the impacted group.[822] Moreover, the relevant inquiry is whether such representations or practices are likely to mislead rather than whether the representation or practice has caused actual deception.[823] Similar to the unfairness standard, when representations or sales practices are targeted to a specific audience, the effect of the practice on a reasonable member of that group is the relevant inquiry in determining whether the act or practice is deceptive.[824] Finally, a "material" misrepresentation or practice is "one which is likely to affect a consumer's choice of or conduct regarding a product."[825]

c. Abusive

"Covered persons" under DFA are also prohibited from engaging in acts or practices in connection with consumer financial products and services that are "abusive." An act or practice is "abusive" when it:

- materially interferes with the ability of a consumer to understand a term or condition or a consumer financial product or service; or

- takes unreasonable advantage of:
    - a consumer's lack of understanding of the material risks, costs, or conditions of the product or service;

    - a consumer's inability to protect his or her interests in selecting or using a consumer financial product or service; or

821 Fed. Trade Comm'n, Policy Statement on Deception (Oct. 14, 1983), at 1, https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf; CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 5–7 (2012).

822 Fed. Trade Comm'n, Policy Statement on Deception (Oct. 14, 1983), at 1; CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 5–7 (2012).

823 Fed. Trade Comm'n, Policy Statement on Deception (Oct. 14, 1983), at 2; CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 4 (2012).

824 Fed. Trade Comm'n, Policy Statement on Deception (Oct. 14, 1983), at 2–3.

825 Fed. Trade Comm'n, Policy Statement on Deception (Oct. 14, 1983), at 5.

- a consumer's reasonable reliance on a covered person to act in his or her interests.[826]

The Congressional intent of this prohibition on abusive acts or practices was to empower the CFPB to "cover practices where providers unreasonably take advantage of consumers."[827] In January 2020, the CFPB stated its intent, going forward, to enforce the abusiveness standard only where "the harms to consumers from the conduct outweigh its benefits to consumers" and where the facts related to the abusive conduct are different from facts related to unfair or deceptive conduct.[828]

2. Application of UDA(A)P to Financial Data Issues

The FTC has not issued any regulations related to UDAPs concerning financial data or consumer data in general commerce.[829] Instead, the FTC has focused on outlining "best practices" and publishing guidance summarizing its enforcement approach to unfairness and deception allegations related to data security issues that may affect both financial services providers and companies involved in commerce more generally.[830] For example, in March 2012, the FTC issued a Privacy Report articulating "best practices" for companies collecting and using data that can be reasonably linked to a consumer, computer, or device.[831] The agency specifically noted that it did not expect entities that collect only non-sensitive data from fewer than 5,000 consumers per year and that do not share the data with third parties to adhere to the

826 12 U.S.C. § 5531(d); *see also* CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 9 (2012).

827 *See, e.g.*, S. REP. No. 111-176, at 172 (2010) ("Current law prohibits unfair or deceptive acts or practices.
The addition of 'abusive' will ensure that the Bureau is empowered to cover practices where providers unreasonably take advantage of consumers."); *see also* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376, pmbl. (2010) (listing as one of the purposes of the Act "to protect consumers from abusive financial services practices"); S. Rep. No. 111-176, at 9 n.19 (2010) ("Today's consumer protection regime . . . could not stem a plague of abusive and unaffordable mortgages."); S. REP. No. 111-176 at 11 (2010) ("This financial crisis was precipitated by the proliferation of poorly underwritten mortgages with abusive terms."); H.R. REP. NO. 111-376, at 91 (2009) ("Th[e] disparate regulatory system has been blamed in part for the lack of aggressive enforcement against abusive and predatory loan products that contributed to the financial crisis, such as subprime and nontraditional mortgages."); H.R. REP. NO. 111-517, at 876–77 (2010) (Conf. Rep.) ("The Act also prohibits financial incentives . . . that may encourage mortgage originators . . . to steer consumers to higher-cost and more abusive mortgages.").

828 Consumer Fin. Prot. Bureau, Statement of Policy Regarding Prohibition on Abusive Acts or Practices (Jan. 24, 2020), at 10. This guidance appears to represent a departure from the FTC and CFPB's prior practice of bringing allegations of UDA(A)Ps for the same underlying factual conduct constituting violations of other laws protecting financial data.

829 *See generally* 16 C.F.R. Subchapter B.

830 CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 3–4 (2014), https://fas.org/sgp/crs/misc/R43723.pdf.

831 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

practices.[832] In 2014, in tandem with the announcement of its fiftieth settlement in a data security case, the FTC issued a statement outlining, among other things, its current approach to data security:

The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[833]

The CFPB has also not issued any regulations or published any supervisory guidance specifically focusing on UDAAPs in the context of financial data matters.[834]

Given the paucity of rulemaking or public supervisory information in this area, understanding trends in FTC and CFPB enforcement actions provides the most helpful lens for understanding the impact of UDA(A)P laws on financial data. Since 2002, the FTC has investigated the data security practices of many companies, and brought enforcement actions against over 50 companies that have engaged in "unfair" or "deceptive" practices that it alleges put consumers' personal data at unreasonable risk in violation of the FTC Act,[835] including UDAPs against data brokers.[836] Additionally, in recent years the CFPB has also brought several enforcement actions targeted at UDA(A)Ps related to financial data.[837] Appendix B contains a non-exhaustive summary of UDA(A)P enforcement actions related to financial data selected to provide relevant examples of the trends discussed below.

---

832 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS *IV* (2012).

833 Fed. Trade Comm'n, Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), at 1, https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

834 See Commentary Box 24 further discussion regarding the ways in which the CFPB has used UDAAP supervisory authority to oversee the information security controls of non-bank financial services companies.

835 CONG. RESEARCH SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR OR DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 1–2 (2014).

836 *See* Press Release, Fed. Trade Comm'n, FTC Puts An End to Data Broker Operation that Helped Scam More Than $7 Million from Consumers' Accounts (Nov. 30, 2016), https://www.ftc.gov/news-events/press-releases/2016/11/ftc-puts-end-data-broker-operation-helped-scam-more-7-million; *see also* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

837 *See* In the Matter of Dwolla, Inc., 2016-CFPB-0007 (Mar. 2, 2016) (consent order).

a. UDA(A)Ps Violations Are Often Coextensive with Other Statutory Violations Related to Financial Data

Both the FTC and the CFPB have alleged UDA(A)Ps as well as violations of other federal laws related to data privacy in connection with the same underlying facts.[838] The FTC has brought overlapping UDAP charges with respect to conduct that it has alleged to violate FCRA[839] and GLBA.[840] The CFPB has also explicitly acknowledged the frequent overlap between UDAAP violations and violations of other laws.[841] The CFPB has brought at least one enforcement action [842] for conduct it also charged violated the Fair Debt Collections Practices Act ("FDCPA").[843]

b. Substantive Themes in UDA(A)P Oversight Related to Financial Data

Over the past two decades, the FTC and CFPB have applied their UDA(A)P in a limited number of instances related to financial data. Among those enforcement actions, the FTC and CFPB have targeted two primary types of harms: (i) violations resulting from covered persons' failure to protect financial data with reasonable information security practices (usually stemming from data breaches); and (ii) violations resulting from covered persons' misrepresentations to consumers of their data privacy and security practices, often in the context of breakdowns in notice and consent processes.

Failure to Protect Information Security

According to the FTC, the basic principles of a reasonable data security program are that companies should (i) know what consumer information they have and what employees or third parties have access to it; (ii) limit the information they collect and retain based on their legitimate business needs; (iii) protect the information they maintain by assessing risks and implementing protections in certain key areas—physical security, electronic security, employee training, and oversight of service providers; (iv) properly dispose of information that they no longer need; and

838 Some of the statutes that the FTC is empowered to enforce provide explicit language rendering a statutory violation to be a UDAP. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681s(a)(1) ("[A] violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce, in violation of section 5(a) of the Federal Trade Commission Act (15 U.S.C. 45(a)), and shall be subject to enforcement by [FTC] under section 5(b) of that Act.").

839 *See* Complaint, *United States v. NCO Group, Inc.*, No. 04-2041 (E.D. Pa. May 12, 2004) (alleging violations of Section 623(a)(5) of FCRA); *United States v. NCO Group, Inc.*, Civ. A. No. No. 04-2041, slip op. (E.D. Pa. May 20, 2004) (consent decree); s*ee also* Complaint, *United States v. Rental Research Services, Inc.*, No. 09-524 (D. Minn. Mar. 5, 2009) (alleging data breach constituted both FCRA violation and unfair practice for failure to take appropriate information security measures to protect consumer reports).

840 *See* In the Matter of Sunbelt Lending Services., Inc., No. C-4129 (Fed. Trade Comm'n Jan. 7, 2005) (complaint); In the Matter of Nationwide Mortgage Group, Inc., No. 9319 (Fed. Trade Comm'n Apr. 15, 2005) (decision and order). Both complaints explicitly stated that GLBA violations also per se constitute UDAP violations.

841 CONSUMER FIN. PROT. BUREAU, UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES (UDAAPS) EXAMINATION PROCEDURES 10 (2012).

842 *See* In the Matter of CMM, LLC et al., 2019-CFPB-0004 (Feb. 5, 2019) (consent order) (finding that disclosure of debt to third parties listed as references for loans constituted both a violation of FDCPA and an unfair practice).

843 Pub. L. No. 95-109, 91 Stat. 874 (1977) (codified as amended at 15 U.S.C. § 1692 *et seq.*).

(v) have a plan in place to respond to security incidents, should they occur.[844] The FTC and CFPB have brought a number of enforcement actions in connection with companies' failure to maintain such reasonable and appropriate information security programs to protect consumers' sensitive personal information, alleging that such failure constitutes unfair acts or practices.

For example, the FTC has filed actions alleging that companies engaged in unfair behavior by implementing suboptimal information security that led to consumer harms.[845] Unlike the FTC, the CFPB has no authority to enforce the GLBA Safeguards Rule. Accordingly, the CFPB's use of its UDAAP enforcement powers is its primary means to enforce information security requirements.[846] For instance, the CFPB used its UDAAP authority to enforce information security standards against Equifax, Inc. in 2019 as part of a joint action by the CFPB, FTC, and fifty U.S. states and territories.[847] Notably, the FTC alleged that the identical conduct constituted a violation of the GLBA Safeguards Rule, while the CFPB relied solely on UDAAP authority because it does not have Safeguards Rule authority.[848]

Misrepresentations of Financial Data Privacy and Security Practices

The FTC has also brought claims of deceptive acts or practices in instances in which covered persons have misrepresented to consumers the steps taken to protect their information security.[849] The FTC also alleged deception in at least one instance in which a covered person misrepresented the intended use of the financial data that it collected from consumers, including with what entities the covered person would share the data.[850] In 2016, the CFPB brought an action against Dwolla, Inc. on unfairness grounds for failing to implement a reasonable and

844 *See* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS 1 (2011); *see generally* Fed. Trade Comm'n, *Data Security*, http://business.ftc.gov/privacy-and-security/data-security (last visited Mar. 11, 2020).

845 *See* In the Matter of CardSystems Solutions, Inc., No. C-4168 (Fed. Trade Comm'n Sept. 8, 2006) (complaint) (alleging UDAP by payment processor that set up its information security system in a manner that nonetheless permitted a hacker to obtain thousands of consumer files); Complaint, *United States v. Rental Research Services., Inc*., No. 09-524 (D. Minn. Mar. 5, 2009) (alleging UDAP by consumer reporting agency that failed to include adequate customer screening measures in its information security system, leading to dissemination of consumer information to unauthorized persons); In the Matter of EPN, Inc., also d/b/a Checknet, Inc, No. C-4370 (Fed. Trade Comm'n Oct. 26, 2012) (complaint; decision and order) (alleging UDAP against debt collector that failed to institute information security measures to prevent data breach).

846 *See* 12 U.S.C. § 5481(12)(J) (excluding financial institutions' information security safeguards under GLBA Section 501(b) from the CFPB's rulemaking, examination, and enforcement authority); *see also* CONSUMER FIN. PROT. BUREAU, GRAMM-LEACH-BLILEY ACT (GLBA) PRIVACY OF CONSUMER FINANCIAL INFORMATION EXAMINATION PROCEDURES (2016), https://files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf.

847 Complaint, *C.F.P.B. v. Equifax, Inc.*, No. 19-3300 (N.D. Ga. July 22, 2019); Stipulated Order for Permanent Injunction and Monetary Judgment, *C.F.P.B. v. Equifax, Inc.*, No. 19-3300, slip op. (N.D. Ga. July 22, 2019).

848 Complaint, *F.T.C. v. Equifax, Inc.*, No. 19-99999 (N.D. Ga. July 22, 2019); Stipulated Order for Permanent Injunction and Monetary Judgment, *F.T.C. v. Equifax, Inc.*, No. 19-99999, slip op. (N.D. Ga. July 22, 2019).

849 *See* Complaint, *United States v. PLS Fin. Services., Inc. et al*, No. 12-8334 (N.D. Ill. Oct. 17, 2012); In the Matter of Franklin's Budget Car Sales, Inc., also dba Franklin Toyota/Scion, No. C-4371 (Fed. Trade Comm'n Oct. 26, 2012) (complaint).

850 *See* Complaint, *F.T.C. v. Sequoia One, LLC*, No. 15-1512 (D. Nev. Aug. 7, 2015) (alleging that website operator gathered financial and other sensitive data from consumers for purpose of payday loan applications when it sold information to entity that made unauthorized debits to accounts).

effective information security program and for making deceptive claims about the strength of its information security standards.[851]

Commentary Box 24: Expansion of UDA(A)P Authority to New Financial Data Issues

Regulators to date have used their UDA(A)P authority relatively narrowly with respect to acts and practices related to financial data to focus on issues regarding information security practices and breakdowns in notice and consent proceduresSome stakeholders have posited, however, that the broad, principles-based nature of UDA(A)P powers could enable regulators to use their authority to address gaps in or limitations of financial data regulation under existing statutes or regulations. For example, some scholars have argued that regulators should use UDA(A)P authority to impose "requirements for confidentiality and data minimization and prohibitions on re-identification, data mining, and certain kinds of advertising and marketing to those identified in the data."[852] Some regulators have already indicated a willingness to consider broader questions of unfairness and deception. For example, the FRB has highlighted a number of questions relating to fairness and transparency that might apply to companies using financial data, stemming from why a company is selecting and considering specific data and from how it is using the data.[853]

The potential use of unfairness claims to impose data minimization obligations on participants in financial markets has also attracted significant attention. Parties in pending civil litigation have made the argument that collecting large amounts of data beyond what is necessary to facilitate a particular financial product or service constitutes a data privacy violation, regardless of the consent obtained.[854] This type of unfairness allegation gives rise to questions of what constitutes valid and legally

851 In the Matter of Dwolla, Inc., 2016-CFPB-0007 (Mar. 2, 2016) (consent order).

852 Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2288 (2015), https://www.gwlr.org/wp-content/uploads/2016/01/83-Geo-Wash-L-Rev-2230.pdf. Data minimization is the principle that data holders should limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose of the collection.

853 *See generally* Carol A. Evans, Fed. Reserve Bd., *Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks*, CONSUMER COMPLIANCE OUTLOOK 2d. ed. (2017), https://www.consumercomplianceoutlook.org/2017/second-issue/keeping-fintech-fair-thinking-about-fair-lending-and-udap-risks/.

854 *See Cottle, et al. v. Plaid Inc.*, Civ. A. No. 20-03056 (N.D. Cal. May 4, 2020).

appropriate consent, whether there are any limits to fair reuse of shared financial data, and what constitutes appropriate disclosure by data aggregators or the ultimate users of such data.

A 2019 Clearing House survey of fintech application users also implicates these open questions. It found that 70% of respondents believed that their financial data is confidential and secure, but 79% of respondents do not read the terms and conditions that govern the use of their financial data by those fintech companies and associated data aggregators.[855] In addition, 80% were not fully aware that the applications or third parties may store their bank account username and password, and 79% were not aware that financial apps have access to their data until they revoke their bank account username and password.[856]

855 *See* THE CLEARINGHOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY 2–3 (2019), https://www.theclearinghouse.org/payment-systems/articles/2019/11/-/media/ec23413b9f98467ea7bdf55e93854278.ashx.

856 *See* THE CLEARINGHOUSE, CONSUMER SURVEY: FINANCIAL APPS AND DATA PRIVACY 2–3 (2019).

VIII. Electronic Fund Transfer Act (EFTA)

A. Introduction

The Electronic Fund Transfer Act ("EFTA")[857] was signed into law in 1978 in response to the emergence and growth of electronic banking technology, in particular the automated teller machine ("ATM"). Introduced to the public in the early 1970s, ATMs were an innovative product that enabled consumers to withdraw funds without a teller, outside of narrow "bankers' hours." By 1975, nearly half of states had enacted some form of statute addressing ATMs and electronic fund transfers ("EFTs").[858] Although ATMs would eventually revolutionize the financial world and the consumer banking experience, many consumers at the time were skeptical of the new technology.[859]

In response to these developments, Congress enacted EFTA to preempt state law regimes and provide a uniform federal framework for financial institutions, merchants, and others to facilitate EFTs; to protect consumers from deceptive or abusive practices that may occur; and to create federal consumer rights to assuage the public's concerns and encourage the adoption of new technologies.[860] These public concerns included consumer privacy in light of the predicted expansion of transactional information and the ease with which it could be accessed, as well as consumers' ability to control the accuracy of transactional records.[861] EFTA provides a basic legal structure for EFTs by allocating rights, liabilities, and responsibilities of participants in electronic fund transfer systems with a primary objective of establishing individual consumer rights and protections.[862] These statutory rights were the first federal laws in the country to specifically address access to and the accuracy of consumers' electronic fund transfers and related records, and thus by proxy one of the first federal laws to protect consumers' financial data.

857 Pub. L. No. 95-630, 92 Stat. 3728 (1978) (codified at 15 U.S.C. § 1693 *et seq.*).

858 Roland E. Brandel & Eustace A. Olliff III, The Electronic Fund Transfer Act: A Primer, 40 OHIO ST. L. J. 530 (1976), https://kb.osu.edu/bitstream/handle/1811/65105/OSLJ_V40N3_0531.pdf (citing Daniel Prives, *Electronic Fund Transfer Systems and State Laws*, 93 BANKING L.J. 527 (1976)).

859 Janine Hornicek, *Electronic Fund Transfers, Branch Banks, and Potential Abuse of Privacy*, 6 FORDHAM URB. L. J. 571 (1978), https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1111&context=ulj (citing N.Y. TIMES, May 31, 1977, at 41, col. 1.).

860 NAT'L COMM'N ON ELECTRONIC FUND TRANSFER, FINAL REPORT, EFT IN THE UNITED STATES: POLICY RECOMMENDATIONS AND THE PUBLIC INTEREST 6 (1977), https://hdl.handle.net/2027/umn.31951d00818933a.

861 NAT'L COMM'N ON ELECTRONIC FUND TRANSFER, FINAL REPORT, EFT IN THE UNITED STATES: POLICY RECOMMENDATIONS AND THE PUBLIC INTEREST 7–8 (1977).

862 15 U.S.C. § 1693(b).

EFTA has twice been amended by major legislative efforts. The Credit Card Accountability, Responsibility, and Disclosure Act of 2009 ("CARD Act") added provisions governing gift cards, gift certificates, and prepaid accounts.[863] DFA added provisions governing international remittance transfers and transferred most rulemaking authority for EFTA from FRB to the newly created CFPB.[864] EFTA's enabling regulation, Regulation E, has been updated and altered numerous times since its adoption. In addition to the changes made pursuant to the passage of the CARD Act and DFA, in 2009 the FRB promulgated significant amendments to Regulation E to include rules governing affirmative consent to certain overdraft charges.[865]

With respect to consumer financial data, EFTA and Regulation E created one of the first legal frameworks for facilitating consumer access to financial data, ensuring data accuracy, and apportioning liability for transaction errors. Specifically, EFTA and Regulation E require financial institutions to provide consumers with transactional and account information in the form of periodic account statements, receipts, notices, and otherwise upon request. Separate and apart from other federal privacy laws, the circumstances under which account and transactional information will be shared with third parties must also be disclosed. The law and regulation further obligate financial institutions to accept, investigate, and ultimately resolve assertions of errors or inaccuracies from consumers within prescribed processes and timeframes. Liability for losses stemming from transaction errors are then apportioned between the consumer and financial institution according to how promptly the consumer discovers and reports the error.

B. Entities Covered[866]

In general, EFTA applies to "financial institutions" that use EFTs to debit or credit a consumer's account,[867] employing language intended to establish coverage as a rule and noncoverage as the exception to the rule.[868] EFTA defines "financial institution" as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit

863 15 U.S.C. §§ 1693l-1, 1693o-2.

864 15 U.S.C. § 1693o-1.

865 *See* 74 Fed. Reg. 59033 (Nov. 17, 2009) (originally codified at 12 C.F.R. Part 205).

866 The analysis of this statutory section is primarily limited to EFTA's requirements and coverage with respect to financial institutions. EFTA also imposes additional and different obligations on non-financial persons that are beyond the scope of this paper.

867 12 C.F.R. § 1005.3(a).

868 Note: remittance transfer providers are also covered entities under EFTA, even when they do not provide accounts. "'Remittance transfer provider' or 'provider' means any person that provides remittance transfers for a consumer in the normal course of its business, regardless of whether the consumer holds an account with such person." 12 C.F.R. § 1005.30(f)(1).

union, or any other person who, directly or indirectly, holds an account belonging to a consumer."[869]

"Consumer account," in turn, is defined under EFTA as "a demand deposit, savings deposit, or other asset account . . . established primarily for personal, family, or household purposes."[870] Regulation E interprets the term broadly. Regulation E clarifies that "account" includes "a demand deposit (checking), savings, or other consumer asset account . . . held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes."[871] Regulation E's addition of the language "directly or indirectly" reinforces the breadth of coverage Congress intended to establish. Regulation E also extends the definition of account beyond traditional deposit accounts by making clear that the term includes "prepaid accounts" such as, among other things, payroll and government benefit accounts, as well as stored value cards accepted at multiple, unaffiliated merchants.[872] Regulation E only exempts from coverage accounts that are subject to "bona fide trust agreements," such as individual retirement accounts, mortgage escrow accounts, or pensions accounts.[873]

EFTA authorizes regulation to extend coverage to entities beyond account-holding institutions.[874] Pursuant to this authority, Regulation E expanded the definition of "financial institution" to include "any other person . . . that issues an access device and agrees with a consumer to provide electronic fund transfer services," provided that there is no agreement between the person and the account-holding institution regarding such services.[875] An "access device" is "a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers."[876] The most ubiquitous example is an ATM or debit card. However, PINs or codes that a consumer uses to access an account can also be access devices, which could include a consumer's username and password for online banking services or mobile applications.[877] Thus, entities that do not hold

869 15 U.S.C. § 1693a(9).

870 15 U.S.C. § 1693a(2).

871 12 C.F.R. § 1005.2(b)(1).

872 12 C.F.R. § 1005.2(b)(3). "Prepaid accounts" encompass what is more commonly known as prepaid or reloadable debit cards, as well as cards used to distribute payroll payments, government benefits, and other funds in lieu of deposits into a traditional deposit account. The term refers to the underlying asset account or benefits rather than the card itself.

873 12 C.F.R. § 1005.2(b)(2); *see also* 12 C.F.R. cmt. 1005.2(b)-2.

874 *See* 15 U.S.C. § 1693b(d) (authorizing the CFPB to promulgate rules regulating "person[s] other than a financial institution holding a consumer's account" to the extent such persons provide electronic fund transfer services to consumers).

875 12 C.F.R. §§ 1005.2(i), 1005.14(a)(2).

876 12 C.F.R. § 1005.2(a)(1).

877 *See* 65 Fed. Reg. 40061, 40064 (June 29, 2000) (originally codified at 12 C.F.R. Part 205) (acknowledging that a "security code" used to access an account online can be considered an "access device"); OFFICE OF THE COMPTROLLER OF CURRENCY, OCC BULL. 2001-12, BANK-PROVIDED ACCOUNT AGGREGATION SERVICES: GUIDANCE TO BANKS (2001), https://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-12.html.

consumer accounts, but permit consumers to authorize transfers among qualified accounts through an access device they issue, qualify as "financial institutions" covered by EFTA.[878] These "EFT service providers" are generally subject to the full scope of EFTA and Regulation E with certain modifications to specific requirements.[879]

Commentary Box 25: Application of EFTA Coverage to Emerging Business Models

As new methods and models of financial services companies emerge, determining whether a company is a covered entity under EFTA and Regulation E becomes less straightforward. Such questions often depend on what constitutes an "access device" or an "account" for purposes of the law. Notably, the CFPB has not publicly opined on whether a consumer's username and password to an online platform or mobile application that allows consumers to conduct EFTs constitute an "access device," though it is widely assumed by industry participants that such login credentials do qualify.

For example, a company that provides personal financial management services by aggregating consumers' accounts into a single dashboard could qualify as a "financial institution" if, in addition to providing a consumer access to information concerning accounts at other institutions, the company allows the consumer to initiate EFTs to or from those accounts. The login credentials issued by the company to the consumer to access data could be construed as an access device when coupled with an ancillary EFT service (such as third-party bill pay capabilities) or the

878 In addition, EFTA and Regulation E address merchant gift cards and certificates, and impose various requirements on "any person" that sells or issues them, which encompasses retailers and other merchants. 15 U.S.C. § 1693l-1; 12 C.F.R. § 1005.20. EFTA and Regulation E also address international remittance transfers and "remittance transfer providers," which includes "any person that provides remittance transfers for a consumer in the normal course of its business[.]" 12 C.F.R. § 1005.30(f)(1).

879 These modifications are contained in 12 C.F.R. § 1005.14 and adjust certain disclosure and error resolution requirements to account for differences between EFT services provided by financial institutions that hold the consumer's account and those that do not. While these specific provisions refer to covered entities as "electronic fund transfer service providers," such entities are a subset of "financial institution." Indeed, FRB originally proposed using the phrase "financial institutions not holding a consumer's account" and including the provisions within a more generally applicable section of Regulation E, 44 Fed. Reg. 59474, 59485 (Oct. 15, 1979), but ultimately decided to change the language and separate the provisions from all others "to emphasize that it has limited and narrowly defined applicability, unlike the remainder of [the existing section] which may affect many financial institutions." 45 Fed. Reg. 8248, 8258 (Feb. 6, 1980) (originally codified at 12 C.F.R. Part 205).

ability to otherwise transfer funds electronically between accounts. Both the FRB and the OCC have recognized the potential applications of EFTA to such services.[880]

Application of EFTA to "digital wallets" is similarly complicated. A fintech company offering digital wallets that allow a consumer to make payments from an account held by another depository institution can be considered a "financial institution" depending on the way in which the digital wallet operates. The CFPB, in its 2016 Prepaid Card Rule, defined "prepaid account" for purposes of EFTA to include digital wallets that can hold funds directly, but excluded those that simply act as a pass-through device for transmitting the consumer's payment credentials.[881]

For instance, if a company inserts itself into the payment stream by first initiating a transfer from the consumer's account to the company, and then directs those funds to the merchant in a second transfer, the company could be deemed to have provided an access device (the digital wallet and/or "code" used to access the wallet service) and agreed to provide the consumer an EFT service (initiating electronic transfers from a consumer account to the merchant) even where the wallet provider is not storing the consumer's funds in an "account."[882] By contrast, a digital wallet that merely acts as a pass-through device for transmitting the consumer's payment credentials may not be considered a "financial institution" because, despite offering what appears to be an access device, it is not agreeing to provide an EFT service. Still, some observers have suggested that application of the "EFT service provider" definition could extend coverage to additional types of digital wallets.[883] While the

880 65 Fed. Reg. 40061, 40064 (proposed June 29, 2000) (originally codified at 12 C.F.R. Part 205) (discussing in a proposed amendment to Regulation E the FRB's opinion as to how aggregators may fall within the definition of "financial institution"); OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. 2001-12, BANK-PROVIDED ACCOUNT AGGREGATION SERVICES: GUIDANCE TO BANKS (2001) (discussing the same from the OCC's perspective).

881 12 C.F.R. § 1005.2(b)(3), cmt. 1005.2(b)(3)(i)-6.4.

882 Another, similar example would be decoupled debit cards, which are cards that are not associated with any specific bank or account. The issuer of such cards does not hold the consumer's account, but is offering an access device and providing a service where it initiates electronic fund transfers by authorizing transactions put through the card and using a separate ACH transfer from the consumer's account to fund the transaction.

883 *See generally* Adam J. Levitin, *Pandora's Digital Box: The Promise and Perils of Digital Wallets*, 166 U. PA. L. REV. 305, 315–18 (2018), https://www.pennlawreview.com/wp-content/uploads/2020/04/166-U-Pa-L-Rev-305.pdf (discussing the way in which digital wallets function, including comparing "pass-through wallets" to "staged wallets" where the wallet provider acts as intermediary between the consumer and merchant).

CFPB has attempted to add clarity to this issue, its efforts are currently being litigated.[884]

The examples above illustrate how uncertainty around EFTA and Regulation E coverage lead to uncertainty as to which entities are responsible for fulfilling regulatory requirements (such as error resolution) or liable for unauthorized or erroneous transactions. This uncertainty is compounded where both the bank and the fintech involved may have issued what could be considered "access devices" that are being used in tandem by the consumer, both may have consumer agreements disclaiming liability for issues that may arise[885] and the entities involved in a transaction do not have commercial agreements among themselves. These examples also highlight that EFTA and Regulation E do not directly address many new business models involving data aggregators that provide commercial services to fintechs and other institutions by, for example, providing application programming interfaces (APIs) to capture consumer financial data from other financial institutions. These entities are not issuing access devices, are not entering into agreements with consumers to provide EFT services, and are not otherwise holding consumer accounts, but may nevertheless act as a vital conduit passing consumers' financial data between the entities involved in a transaction.

C. Data Covered

EFTA predominantly focusing on data relating to "electronic fund transfers" ("EFTs") involving a consumer account. EFTs are defined as:

884 In light of the ambiguity surrounding application of Regulation E to digital wallets, the CFPB formally amended the Prepaid Card Rule to cover digital wallets as well. *See* 81 Fed. Reg. 83,934 (Nov. 22, 2016) (final rule); 83 Fed. Reg. 6364 (Feb. 13, 2018) (amending final rule and delaying the effective date until April 1, 2019); 12 C.F.R. §§ 1005.18–20. However, Paypal has brought suit against the CFPB arguing that amending the Prepaid Card Rule to cover digital wallet products is both beyond the statutory authority of the CFPB and is arbitrary and capricious in light of the evidentiary record. *See* Complaint, *Paypal, Inc. v. C.F.P.B.*, No. 1:19-cv-03700 (D.D.C. Dec. 11, 2019).

885 For example, the aggregator may claim that the wallet is not an "access device" and contractually disclaim liability, while the bank may argue that the consumer willingly provided their debit card information to the aggregator for the purpose of initiating transactions and is therefore not liable for transactions initiated by the aggregator given the definition of "unauthorized electronic fund transfer." *See* 12 C.F.R. § 1005.2(m)(1) (stating that transactions initiated by "a person who was furnished the access device to the consumer's account by the consumer" are not an "unauthorized electronic fund transfer").

[A]ny transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account. Such term includes, but is not limited to, point-of-sale transfers, automated teller machine transactions, direct deposits or withdrawals of funds, and transfers initiated by telephone.[886]

EFTA and Regulation E specifically exclude from the definition of EFTs any transfer of funds initiated by check or paper instrument, transfer through wire transfer systems used primarily for transfers between financial institutions or between businesses, transfers made for the purchase or sale of securities or commodities, or automatic transfers of funds subject to an agreement between the consumer and financial institution (such as transfers associated with overdraft protection products, collection of account fees, and sweep accounts).[887]

Regulation E also has special provisions governing gift cards, prepaid accounts, and EFTs involving those accounts, as well as a subpart devoted to international remittance transfers.[888] Although wire transfers are excluded from the definition of EFT, international consumer wire transfers fall within the ambit of remittance transfers.[889]

D. Oversight

As initially enacted, rulemaking authority under EFTA was granted to the FRB which originally promulgated Regulation E. In 2011, subject to a few exceptions,[890] DFA transferred rulemaking authority under EFTA from the FRB to the CFPB.[891] In 2011, the CFPB re-issued Regulation E under its rulemaking authority.[892] Since 2011, the CFPB has issued several updates and additions to Regulation E.[893] The biggest substantive changes to Regulation E since its

886 15 U.S.C. § 1693a(7).

887 15 U.S.C. § 1693a(7)(A)–(D); 12 C.F.R. § 1005.3(c)(1)–(5). Many of these exceptions are intended to allow the internal workings of a financial institution to operate unimpeded, such as transfers related to sweep accounts, the assessment of fees, and transfers that allow for the payment of overdrafts.

888 *See* 12 C.F.R. §§ 1005.18–20, 1005.30–36.

889 12 C.F.R. cmt. 1005.30(e)-3(i)(B).

890 12 U.S.C. §§ 5517, 5519. 15 U.S.C. § 1693o-2.

891 12 U.S.C. § 5481(12)(C).

892 Issued as 12 C.F.R. § 1005.

893 *See* 77 Fed. Reg. 40459 (July 10, 2012) (codified at 12 C.F.R. Part 1005); 77 Fed. Reg. 50243 (Aug. 20, 2012) (codified at 12 C.F.R. Part 1005); 78 Fed. Reg. 6025 (Jan. 29, 2013) (codified at 12 C.F.R. Part 1005); (78 Fed. Reg. 30661) (May 22, 2013); 78 Fed. Reg. 49365 (Aug. 14, 2013) (codified at 12 C.F.R. Part 1005); 79 Fed. Reg. 55970 (Sept. 18, 2014) (codified at 12 C.F.R. Part 1005); 81 Fed. Reg. 70319 (Oct. 12, 2016) (codified at 12 C.F.R. Part 1005); 81 Fed. Reg. 83934 (Nov. 22, 2016) (codified at 12 C.F.R. Parts 1005, 1026); 82 Fed. Reg. 18975 (Apr. 25, 2017) (codified at 12 C.F.R. Parts 1005, 1026); 83 Fed. Reg. 6364 (Feb. 13, 2018) (codified at 12 C.F.R. Parts 1005, 1026).

enactment have been the FRB's added provisions for overdraft services and gift cards, and the CFPB's added provisions for prepaid accounts and international remittance transfers.[894]

EFTA further grants administrative enforcement authority to numerous federal agencies, each of which is responsible for ensuring those under its purview or supervisory authority comply with the law's requirements. These agencies include the FRB, CFPB, OCC, FDIC, NCUA, SEC, the Secretary of Transportation (with respect to air carriers), and the FTC.[895] Especially noteworthy is DFA's extension to the CFPB of supervisory authority over non-depository persons, including non-bank entities involved in mortgage lending and servicing, private education loans, and payday loans, as well as "larger participants" in certain markets for consumer financial products or services.[896] In addition, EFTA grants consumers a private right of action and permits both individual claims and class actions.[897]

Civil and criminal liability are contemplated under EFTA, with penalties, in excess of actual damages, for civil actions in individual cases up to $1,000 and $500,000 in class actions.[898] EFTA allows financial institutions to utilize unintentional error and good faith compliance as defenses against actions brought under this statute.[899]

E. Substantive Requirements

1. Summary

EFTA and Regulation E address consumer financial data by (i) requiring that consumers be given access to certain transaction data and be informed of how that and other account data will be shared with third parties; (ii) providing consumers with the ability to dispute transactions and thereby correct inaccurate financial data maintained by the financial institution; and (iii) balancing the rights of consumers and the responsibilities of financial institutions through a liability framework. This system incentivizes both consumers and financial institutions to maintain accurate financial data and correct errors in a timely, orderly fashion.

894 *See* 12 C.F.R. §§ 1005.18–20, 1005.30–36.

895 15 U.S.C. § 1693o(a).

896 12 U.S.C. § 5514; 12 C.F.R. § 1090.100 *et seq.* The CFPB, in consultation with the FTC, determines by rulemaking who constitutes a "larger participant" subject to the Bureau's supervision. Currently, the CFPB supervises entities that exceed certain income thresholds within the consumer reporting, consumer debt collection, student loan servicing, international money transfer, and automobile financing markets. 12 C.F.R. § 1090.104–08.

897 15 U.S.C. § 1693m(a).

898 *See* 15 U.S.C. §§ 1693n, 1693m(a).

899 *See* 15 U.S.C. § 1693m(c)–(d).

2. Disclosures to Consumers (Access)

A financial institution that offers consumer EFT services or accounts that can be debited or credited using EFTs must provide the consumer with various disclosures for the duration of the relationship. These disclosures must, at a minimum, be provided in writing in clear and readily understandable language.[900] Disclosures of information required under Regulation E may be combined with disclosures required under Regulation DD or another statute or regulation and provided in the same statement.[901]

First, financial institutions must provide consumers with initial disclosures regarding the terms and services of EFTs. An initial disclosure regarding the terms and services of EFTs must be provided to the consumer before any EFTs may be processed.[902] Among other things, the initial disclosure informs consumers of (i) their right to receive periodic statements, receipts, and notices with respect to EFT transactions;[903] (ii) the circumstances under which third parties will receive information about their transactions or account; (iii) their right to report errors involving EFTs and have them corrected; and (iv) their liability for errors and unauthorized EFTs.[904] If the financial institution changes any of its terms regarding EFTs and those changes could result in any increased fees, increased consumer liability, or fewer or reduced services available to the consumer, the financial institution must reissue its disclosures to all potentially affected consumers at least twenty-one days prior to implementation of the changes.[905]

Second, financial institutions must make available to consumers receipts of any EFT greater than $15 initiated at an "electronic terminal."[906] Regulation E defines "electronic terminal" as "an electronic device, other than a telephone operated by a consumer, through which a consumer may initiate an electronic fund transfer."[907] The most common examples are ATMs and point-of-sale devices used by merchants.[908] However, as the language "make available"

900 12 C.F.R. § 1005.4(a)(1).

901 12 C.F.R. § 1005.4(b)–(c).

902 12 C.F.R. § 1005.7(a).

903 The substance included in these disclosures is substantially similar to that required in Regulation P disclosures. *See* 12 C.F.R. § 1005.7(b).

904 12 C.F.R. § 1005.7(a)–(b). Note that liability for unauthorized transactions must be expressly stated in disclosures, while the consumer's liability for errors is merely implied by informing consumers that errors must be reported within a certain timeframe.

905 12 C.F.R. § 1005.8(a)(1).

906 12 C.F.R. § 1005.9(a), (e).

907 12 C.F.R. § 1005.2(h).

908 Many entities have taken the position that a consumer's personal computer or mobile device falls outside the definition of "electronic terminal" and therefore beyond Regulation E's terminal receipt requirements. This is based on official interpretations to Regulation E that note, "[b]ecause the term 'electronic terminal' excludes a telephone operated by a consumer, a financial institution need not provide a terminal receipt when [a] consumer initiates a transfer by a means analogous in function to a telephone, such

suggests, financial institutions often need not provide receipts for all transactions, but rather make them available upon request. Since many electronic terminals are operated by third parties outside the control of the financial institution, this also means a financial institution can make receipts "available" by relying on those third parties to provide them to consumers.[909]

Any such EFT receipt must include (i) the amount and date of the transaction; (ii) the type of EFT involved and the account number and type of account from which the EFT was debited or credited; (iii) the electronic terminal location; and (iv) the third party to or from whom the funds were transferred.[910] In addition, Regulation E requires that consumers be provided with notices and disclosures similar to receipts in the context of international remittance transfers.[911]

Third, financial institutions must provide consumers with periodic account statements regarding consumers' accounts and their recent transaction histories.[912] For any calendar month in which the consumer initiates an EFT, the financial institution must provide a monthly statement of all account activity, EFT or otherwise, for that month.[913] If the consumer conducts no EFT activity that month, no account statement is required. However, in such circumstances the financial institution must still provide periodic statements on at least a quarterly basis.[914] Account statements must include, among other things, various information concerning the account, balances, fees assessed, and detailed information about each EFT that occurred during the statement period.[915]

3. Error Resolution (Accuracy)

In addition to addressing access to financial data, Regulation E establishes a consumer's right to contest both transactions and inaccurate financial records related to transactions, and have the financial institution correct any such errors, provided the consumer gives the institution

---

as by home banking equipment or a facsimile machine." 12 C.F.R. cmt. 1005.2(h)-1. However, industry standards and rules such as those imposed by the National Automated Clearing House Association ("NACHA") may require the provision of receipts for certain transactions authorized through these devices independently of EFTA. *E.g.*, NACHA Operating Rule 2.3.2.2 (requiring that consumers receive "an Electronic or hard copy of the [consumer's] authorization for all debit Entries to be initiated to a Consumer Account").

909 12 C.F.R. § 1005.9(a). Official Comment 9(a) allows for the account-holding institution to make receipts available through third parties such as merchants.

910 12 C.F.R. § 1005.9(a)(1)–(6).

911 *See* 12 C.F.R. § 1005.31 (requiring remittance transfer providers to furnish disclosures at the time of the transaction that provide details of the transaction).

912 12 C.F.R. § 1005.9(b). As previously noted, prepaid accounts are subsumed by Regulation E's general definition of an "account," and are therefore subject to the same periodic statement requirements. However, Regulation E allows financial institutions to choose to provide ongoing access to balance and transaction information online, by phone, and by request as an alternative to periodic statements for prepaid accounts. *Id.* at § 1005.18(b)(c)(1).

913 12 C.F.R. § 1005.9(b).

914 12 C.F.R. § 1005.9(b).

915 12 C.F.R. § 1005.9(b)(1)–(5).

adequate and timely notice.[916] Regulation E thus gives consumers a limited ability to take steps to ensure their own transaction data accuracy and also distributes the burden of ensuring the accuracy of financial data between the consumer and the financial institution by encouraging consumers to review the financial data on their monthly account statements regularly and report errors within prescribed timeframes. Notably, EFTA and Regulation E do not address errors discovered by the financial institution itself.[917] An "error" is defined as:

- an unauthorized electronic fund transfer;
- an incorrect electronic fund transfer to or from the consumer's account;
- the omission of an electronic fund transfer from a periodic statement;
- a computational or bookkeeping error made by the financial institution relating to an electronic fund transfer;
- the consumer's receipt of an incorrect amount of money from an electronic terminal;
- an electronic fund transfer not identified in accordance with requirements for receipts, periodic statements, or notices concerning direct deposits; or
- the consumer's request for documentation required by provisions concerning receipts, periodic statements, or notices concerning direct deposits or for additional information or clarification concerning an electronic fund transfer, including a request the consumer makes to determine whether an error exists.[918]

As alluded to above, both transactional errors and informational errors can be disputed by a consumer. For example, an "electronic fund transfer not identified in accordance with" periodic statement requirements would encompass not only a transaction processed and printed on statements for an incorrect amount, but inaccurate information concerning the type of transfer, the location where the transaction occurred, and mere typographical errors among others.[919]

916 *See generally* 12 C.F.R. § 1005.11.

917 12 C.F.R. cmt. 1005.11(b)(1)-5.

918 12 C.F.R. § 1005.11(a)(1)(i)–(vii).

919 *See* 12 C.F.R. § 1005.9(b) (outlining the information that must be included when identifying electronic fund transfers on periodic statements).

Commentary Box 26: Error Correction Ambiguity

EFTA and Regulation E do not make clear what constitutes an adequate "correction" of an error involving information displayed on periodic statements, receipts, or other notices that do not require adjustments to be made to a transaction,[920] as the focus of the law is on transactions rather than transactional data. Accordingly, it is arguably possible for a financial institution to "correct" the text appearing on a document without also correcting the underlying data stored within the entity's systems, or it could be possible to process a separate credit or debit to adjust the overall account balance, without altering the original entry. This could allow the institution to continue to reuse or pass along the erroneous data to third parties even after a "correction" is made. In addition, financial institutions often rely on information provided by unaffiliated third parties (e.g., other financial institutions and merchants) concerning transactions that they may not be able to confirm or change. Indeed, financial institutions generally are not expected to verify information they obtain from third parties for every transaction included on periodic statements.[921]

A consumer has sixty days after receiving the periodic account statement to give the financial institution notice of an error in the account.[922] To be considered adequate notice, the consumer must include in the notice of error the consumer's name and account number as well as an explanation of why the consumer believes an error exists and, to the extent possible, the type, date, and amount of the error.[923] Regulation E allows the financial institution to require that the consumer submit the notice of error in writing.[924] If notice is provided beyond the sixty-day period, the financial institution is released—at least with respect to EFTA and Regulation E—from the obligation to investigate or address the error.[925] However, where the error involves

920 *See* 15 U.S.C. § 1693f(b) (stating only that an error must be corrected); 12 C.F.R. § 1005.11(c) (same).

921 *See* 12 C.F.R. cmt. 1005.9(b)(1)-1 (stating that while financial institutions have an obligation to maintain reasonable procedures to ensure the integrity of the data it receives from third parties, it need not verify the accuracy of such data for each transfer that appears on a periodic statement).

922 12 C.F.R. § 1005.11(b)(1).

923 12 C.F.R. § 1005.11(b)(1).

924 12 C.F.R. § 1005.11(b)(2).

925 12 C.F.R. cmt. 1005.11(b)(1)-7. Entities may be obligated or encouraged to correct errors through other mechanisms. For example, consumers may raise breach of contract claims based on deposit agreements. Banks are further subject to a general duty to act in good faith and use ordinary care with respect to their customers. *See* U.C.C. § 4-103(a) ("The effect of the provisions of this Article may be varied by agreement, but the parties to the agreement cannot disclaim a bank's responsibility for its lack of good faith or failure to exercise ordinary care[.]"). Liability provisions contained in payment network rules may also incentivize entities to make corrections beyond what EFTA

an unauthorized transaction, financial institutions will still need to conduct some form of investigation to ensure consumer liability rules (discussed further below) are correctly applied and losses are appropriately allocated.[926]

Where the financial institution receives an adequate and timely notice of error from the consumer, it must work to investigate and determine whether an error occurred within ten business days.[927] If the financial institution is unable to do so, it may take up to forty-five calendar days to conduct its investigation provided the consumer is given provisional credit in the amount of the contested transaction.[928] If an error was determined to have occurred, the financial institution must correct the error within one business day upon the conclusion of the investigation.[929] Regardless of the result, the financial institution is required to provide the consumer with notice of the results of the investigation within three business days after the conclusion of the investigation.[930] When the result is not in favor of the consumer, the consumer is further entitled to receive the information and documents the financial institution relied upon in making its determination.[931]

In addition, Regulation E provides certain minimum standards for conducting an adequate investigation of a timely submitted notice of error. At a minimum, financial institutions must review their own records.[932] When the alleged error involves a point-of-sale transaction with a merchant, this includes verifying "the information previously transmitted when executing the transfer," such as by "request[ing] a copy of the sales receipt to verify that the [transfer] correctly corresponds to the amount of the consumer's purchase."[933] Ordinarily, this is the extent of the financial institution's obligation. However, if the error involves an EFT to or from a third party with whom the financial institution has a specific agreement concerning that type of EFT, it may be required to extend its investigation to information held by the third party.[934]

---

requires. *See* NACHA Operating Rule 2.4.5.1 (requiring financial institutions that originate ACH transactions to indemnify other financial institutions receiving such transactions for breaches of warranty or losses and liabilities stemming from certain transaction errors).

926 See 12 C.F.R. cmt. 1005.11(b)(1)-7 (stating that an institution need not comply with error resolution requirements if notice is not timely provided, but must still comply with consumer liability provisions before liability can be imposed).

927 12 C.F.R. § 1005.11(c)(1).

928 12 C.F.R. § 1005.11(c)(2). The consumer must have full access to any provisionally credited funds. *Id.* at § 1005.11(c)(2)(ii).

929 12 C.F.R. § 1005.11(c)(1).

930 12 C.F.R. § 1005.11(c)–(d).

931 12 C.F.R. § 1005(d)(1).

932 12 C.F.R. § 1005.11(c)(4). The commentary to Regulation E further provides various examples of the types of information and records a financial institution is expected to review. *Id.* at cmt. 1005.11(c)(4)-5.

933 12 C.F.R. cmt. 1005.11(c)(4)-3.

934 *See* 12 C.F.R. cmt. 1005.11(c)(4)-4.

Similar error resolution requirements apply to prepaid accounts and international remittance transfers, although the timing requirements are modified. These modifications generally account for the nature of these accounts and transactions, and the manner in which consumers are provided with account and transaction information.[935]

4. Liability Framework (Liability)

Finally, Regulation E apportions liability—and thus financial losses—for any errors in an account between the financial institution and the consumer based on the timeliness of the consumer's notice of the error to the financial institution. Further, the precise contours of liability depend on whether the error results from unauthorized transfers.

a. Errors

If a consumer discovers errors on an account statement—such as errors in transaction amounts, computational errors on the part of the financial institution, failures to stop payment, or missing transactions—the consumer bears no financial liability provided they report the error to the financial institution within sixty days from when the institution sent the consumer a periodic statement that first reflects the error.[936] Financial institutions, on the other hand, are often liable for all damages proximately caused by an error.[937] If the consumer does not timely notify the institution of an error, then liability is reversed, and the consumer absorbs any financial losses due to that error. Financial institutions, however, generally are not liable for the errors of third parties, such as when a merchant charges a consumer the incorrect price for goods or services but the financial institution otherwise processes the transaction as submitted by the merchant.[938] Additionally, institutions generally have no liability for damages that may result from data errors that do not also involve transactional errors.[939]

b. Unauthorized Transfers

Liability is more complicated with respect to unauthorized transfers. An "unauthorized transfer" is defined as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer

935 *See* 12 C.F.R. §§ 1005.18(e)(2), 1005.33 (addressing error resolution for prepaid accounts and remittance transfers).

936 *See* 12 C.F.R. § 1005.11(c)(2)(iii) (requiring financial institutions to correct errors timely reported without condition).

937 15 U.S.C. § 1693h(a).

938 This is not explicitly stated in Regulation E, but is logically derived from its definition of "error." 12 C.F.R. § 1005.11(a).

939 15 U.S.C. § 1693h(a)–(b).

receives no benefit."[940] Generally, consumers are required to report unauthorized activity to the financial institution within sixty days of the first periodic statement showing the transfer. If the sixty-day requirement is met, the consumer bears no liability for unauthorized transfers that have occurred or for subsequent, related transfers. If the consumer provides notice after the sixty-day period, the consumer still bears no liability for unauthorized transfers occurring within the sixty-day period, but may be held liable for any and all transfers that occur after the sixty-day period up to the date the consumer provided notice.[941] A financial institution's ability to hold a consumer liable for an unauthorized transfer is conditioned upon whether the financial institution has satisfied all disclosure requirements.[942]

Consumer liability is greater for unauthorized transfers conducted with a lost or stolen access device. Under such circumstances, the categorical bar on consumer liability for transfers that occur during the sixty-day period is replaced by a tiered approach that escalates with the passage of time and is based on when the consumer provides notice relative to when the consumer first learned of the loss or theft. The consumer still faces unlimited liability for transfers occurring after the sixty-day period, however, if notice is provided more than sixty days after the provision of a periodic statement.

The tiers operate as follows:

Tier 1 Consumer Provides Notice Within Two Business Days After Learning of the Loss or Theft of the Access Device

If the consumer notifies the financial institution within two business days of learning of the loss or theft of an access device, the consumer's maximum liability for any unauthorized EFTs that occur is the lesser of $50 or the amount of unauthorized transfers that occur before notice is provided to the financial institution.[943]

Tier 2 Consumer Provides Notice After the First Two Business Days But Before Sixty Calendar Days Following Provision of a Periodic Statement

940 12 C.F.R. § 1005.2(m).

941 12 C.F.R. § 1005.6(b)(3); *see also* 12 C.F.R. cmt. 1005.6(b)(3)-2.

942 12 C.F.R. § 1005.6(a).

943 12 C.F.R. § 1005.6(b)(1).

If the consumer fails to notify the financial institution within the first two days, but does provide notice within sixty days of receiving the first periodic statement showing the transaction, the consumer's maximum liability is the lesser of $500 or the combined total of:

- the maximum amount of liability under Tier 1 for transactions occurring in the first two business days; and

- the total amount of unauthorized transfers that occur after the first two business days but before the consumer provided the financial institution with notice, provided the financial institution can establish that the transactions would not have occurred had it received timely notice.[944]

Tier 3 Consumer Provides Notice After Sixty Calendar Days Following Provision of a Periodic Statement

As alluded to above, the greatest liability is imposed on consumers that fail to notify the financial institution until after sixty days have elapsed since the provision of the first periodic statement showing the transaction. In these circumstances, the consumer is liable for the amount according to the formula in Tier 2 above for transfers occurring during the sixty-day period, as well as being liable for all transfers, regardless of amount, that occur after the sixty-day period lapses up to the date notice is provided.[945] As with Tier 2, the financial institution must be able to establish that the transfers would not have occurred had notice been provided earlier.[946] Regulation E does not offer any explanation of how a financial institution can make this showing, but it does place considerable weight on the scales in favor of consumers.

c. Unauthorized Transfer Carveout

Regulation E creates a carveout from the definition of "unauthorized electronic fund transfer" for any transfer that is initiated "[b]y a person who was furnished the access device to the consumer's account by the consumer and from which the consumer receives no benefit."[947] Such transfers are considered authorized by the consumer even where the person exceeds any authority given by the consumer to initiate transfers, until such time as the consumer notifies the financial institution that the person is no longer authorized.[948] This exception was generally

944 12 C.F.R. § 1005.6(b)(2).

945 12 C.F.R. § 1005.6(b)(2)–(3).

946 12 C.F.R. § 1005.6(b)(3).

947 12 C.F.R. § 1005.2(m)(1).

948 12 C.F.R. cmt. 1005.2(m)-2.

contemplated to cover situations involving the access device most common at the time: a debit card. For example, a situation in which a consumer grants permission to a family member to use their debit card and run to the store for milk, but who uses the card to purchase lottery tickets, would not be considered an unauthorized transfer. However, as discussed below, this carveout has become highly relevant in light of new and emerging fintech business models.

Commentary Box 27: Consumer Benefit Requirement to Unauthorized Transfers

Regulation E's definition for "unauthorized transfers" also sets as a requirement that the consumer receive "no benefit" from a transfer.[949] The scope of what qualifies as a "benefit" is relatively unknown and untested in the fintech context. This requirement could potentially allow banks to claim that a consumer benefited from an otherwise unauthorized EFT performed by a fintech company with a furnished access device, even when the fintech exceeded its authority to perform limited EFTs or non-EFT services.

This framework incentivizes consumers to take an active role in keeping track of their access devices and monitoring their financial data, particularly under circumstances where the financial institution is in a poor position to detect problems, such as the case of unauthorized transfers. It also encourages consumers to safeguard their access devices, and report errors and unauthorized activity in a timely manner before losses mount. Nonetheless, EFTA and Regulation E remain decidedly consumer-friendly (and simpler to implement) by basing all liability on the timing of notice rather than whether the consumer acted responsibly[950]: a consumer's negligence cannot be used by a financial institution to evade liability for losses provided timely notice is given, while a financial institution's liability is generally absolute with respect to the consumer, although the financial institution may be able to separately recover losses from other parties.

949 12 C.F.R. § 1005.2(m).

950 This is in contrast to card network rules such as Mastercard rules, which do consider whether the consumer was negligent in protecting their access device with respect to liability for unauthorized activity.

Commentary Box 28: Unauthorized Transfers within the EFTA Liability Framework

The rise of fintech companies has stretched the bounds of EFTA and Regulation E. Further complicating the liability framework is the interplay between unauthorized transfers and fintech companies to whom consumers voluntarily provide their bank-issued access devices, such as debit card numbers or, possibly, online banking login credentials. Some banks have argued, for instance, that they are not liable for any transfers that occur on an account using credentials that a consumer furnished to a data aggregator or other third-party, even in situations in which the consumer did not authorize the credentials recipient to conduct any transfers on their account or such credentials are later stolen by hackers or other downstream parties.[951]

Application of the liability framework gets even more complicated with respect to fintech providers of payment-related services, in light of the fact that Regulation E extends coverage to "EFT service providers" that do not provide accounts themselves but "that issue[] an access device and agree[] with a consumer to provide electronic fund transfer services."[952] If the consumer can initiate EFTs to or from a bank account by using an access device issued by a fintech, that fintech is also a "financial institution" under Regulation E, and is thus subject to the error resolution regime.[953] Liability due to any errors on behalf of the fintech would be apportioned between the consumer and the fintech, not the bank providing the underlying deposit account.[954]

951 *See, e.g.*, Liz Weston, *Why Banks Want You to Drop Mint, Other 'Aggregators'*, REUTERS (Nov. 9, 2015), https://www.reuters.com/article/us-column-weston-banks/why-banks-want-you-to-drop-mint-other-aggregators-idUSKCN0SY2GC20151109 (reporting statements by JPMorgan, Chase, and Capital One). The regulatory text suggests that there must be some form of authorization to use the access device for transactions for the exception to the definition of "unauthorized electronic fund transfer" to apply. Specifically, it states that transactions initiated by "a person who is furnished the access device" are not unauthorized, "unless the consumer has notified the financial institution that transfers by that person are no longer authorized . . . ." 12 C.F.R. § 1005.2(m)(1). It is, however, not explicit and an issue contested by various stakeholders.

952 12 C.F.R. §§ 1005.2(i), 1005.14.

953 *See* 12 C.F.R. § 1005.14.

954 12 C.F.R. § 1005.14.

However, if the fintech does not itself issue an access device (or takes the position that it has not), but rather uses the bank-issued access device to perform EFTs at the direction of the consumer, it is unclear whether the consumer is liable for unauthorized activity. Even though there is an agreement between the consumer and the fintech to perform EFTs, absent a fintech-issued access device, the fintech would not be a "financial institution" under EFTA and Regulation E subject to the error resolution procedures and liability limitations. Furthermore, if any errors or unauthorized activity were to occur because of the fintech, the bank may insist that any such transfers were not "unauthorized" under EFTA and Regulation E because the consumer willingly "furnished" the bank-issued access device to the fintech to initiate EFTs.[955] The consumer may therefore be fully liable for transfers initiated by a fintech that exceeds its stated authority—even purposefully—and abuses login credentials or other bank-issued access devices that were voluntarily provided to it by the consumer.

Even if the fintech issues an access device, usually in the form of its own login credentials or mobile application, it is still unclear who bears ultimate responsibility for EFTA compliance if the fintech also utilizes a bank-issued access device in conjunction with its own access device to initiate transfers, e.g., if a consumer can log in to the fintech's mobile application and authorize EFTs through his or her bank debit card within the application. Arguably, if a code and a card must be used together to initiate a transfer, they are collectively considered a single access device.[956] However, in this scenario it would be an access device partially owned by two entities with no agreement with one another pertaining to regulatory compliance or transactional liability.

More confusing still, some fintech companies, such as data aggregators, are permissioned to use the consumer's bank-issued access device for activities other than facilitating EFTs. In these situations, the consumer would have permissioned limited use of the bank-issued access device, but not permissioned EFTs. It is

955 12 C.F.R. § 1005.2(m)(1).

956 *See* 12 C.F.R. § 1005.2(a)(1) (defining "access device" as a card, code, other means of access to a consumer's account, or "any combination thereof").

unclear how liability would be assigned among the bank, the fintech, and the consumer for any errors or unauthorized transfers made by the fintech.[957] On one hand, a fintech operating under an agreement with the consumer that does not hold an account for the consumer and does not provide for an EFT service would not be a "financial institution" subject to the error resolution procedures or EFTA liability. On the other hand, such a transfer may also be covered by the exception from the definition of "unauthorized transfers" on the basis that the consumer willingly "furnished" the fintech the bank-issued access device.[958] In other words, it is possible neither the fintech nor the bank would be subject to the error resolution procedures and the consumer would be forced to assume total liability. The text of EFTA, Regulation E, and agency guidance commentary do not officially contemplate this arrangement. However, in statements and guidance offered by the FRB and the OCC (prior to DFA's transfer of authority to CFPB), both agencies have acknowledged this ambiguous gap in the greater EFT framework, although neither has offered to weigh in definitively on how liability would be assigned among the parties for errors or EFTs performed by the fintech.[959] The CFPB has also recognized the debate over this issue, but has thus far declined to weigh in.[960]

957 The regulatory text suggests that there must be some form of authorization to use the access device for transactions for the exception to the definition of "unauthorized electronic fund transfer" to apply. Specifically, it states that transactions initiated by "a person who is furnished the access device" are not unauthorized, "unless the consumer has notified the financial institution that transfers by that person are no longer authorized[.]" 12 C.F.R. § 1005.2(m)(1). It is, however, not explicit and an issue contested by various stakeholders.

958 12 C.F.R. § 1005.2(m)(1).

959 *See* 65 Fed. Reg. 40061, 40064 (June 29, 2000) (originally codified at 12 C.F.R. Part 205) ("If the aggregator is not a financial institution and an unauthorized EFT occurs through an aggregator's service, comment 2(m)-2 could be read to suggest that a consumer who has given the aggregator access to the consumer's account assumes liability for the transfers. The guidance in the comment, however, was not originally provided to address this situation."); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULL. 2001-12, BANK-PROVIDED ACCOUNT AGGREGATION SERVICES: GUIDANCE TO BANKS (2001) ("Banks that provide their customers with usernames and passwords for electronic banking should be aware of possible exposure to liability under Regulation E. The potential exposure arises when their customer shares those usernames and passwords with an aggregator. If an attacker then steals the usernames and passwords from the aggregator and performs unauthorized transactions, it is unclear under the current regulation which party would bear responsibility for an unauthorized transfer.").

960 *See* CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION 10 (2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf (acknowledging the debate among stakeholders but providing no opinion).

IX. Conclusion

This paper describes U.S. federal laws and regulations pertaining to consumer financial data. In doing so, we have provided a contextual background, an overview of market participants, an overview of federal regulatory agencies, and a detailed summary of the relevant bodies of law.

We have also provided commentary on a number of open interpretive questions and policy issues that raise both structural and substantive questions within the current legal regime governing consumer financial data. While the issues we highlight are not exhaustive, we believe they represent areas where policymakers, market participants, consumer advocates, academics, and others should be attentive to how the emergence of new data and new intermediaries is reshaping the financial data ecosystem.

Structurally, our commentary addresses open questions about what entities are covered, what data are covered, and what regulatory agencies have oversight in specific areas. As the evolution of the financial data ecosystem continues, resolving these questions is critical to ensuring that consumers are adequately protected, market participants are appropriately accountable, and customer-friendly innovation can reach scale. For example, greater clarity on what entities are covered by FCRA's definitions of "consumer reporting agencies" and "furnishers" will become more pressing as new intermediaries increasingly supply new forms of data for use in eligibility decisions and other financial activities. To take another example, technological advancement that enables the deanonymization of certain data calls into question the exclusion of aggregate/anonymized data from GLBA's Privacy Rule and FCRA. Likewise, differences in supervision authority raise important questions about the consistency of compliance with GLBA safeguard protections. To the extent that coverage gaps create substantial consumer protection or other policy concerns, adjustments to scope or the crafting of separate protections may be warranted.

Beyond structural questions, our analysis of each of the relevant bodies of law also highlights a number of substantive interpretive and policy questions as to how and when particular requirements are applied in particular circumstances. For example, even if data aggregators are deemed to be "consumer reporting agencies" under FCRA, significant questions remain as to how to adapt their practices and establish new procedures to comply with the accuracy, policy and procedure documentation, and dispute resolution requirements that FCRA entails. Similarly, a determination that entities that provide data to aggregators, such as banks, are "furnishers" under FCRA would raise questions about how to comply with "furnisher" obligations within this

new ecosystem. In this example and in others, structural and substantive questions are inextricably linked in the minds of stakeholders, and should be carefully considered as policymakers clarify or adjust the scope of existing bodies of law and/or craft new protections.

While the nature of some questions varies from one body of law to another, many of the highlighted issues touch on key themes identified by stakeholders who have developed principles[961] and conducted analyses[962] to guide the broad-based regulation of financial data going forward. For example, the structural and substantive questions about FCRA raised above will influence whether the financial data ecosystem delivers on the principles of "Reliability" as defined by the Financial Health Network in 2016 and "Accuracy" as defined by the CFPB in 2017. Likewise, the lack of clarity relating to the scope and processes for obtaining affirmative consumer consent under GLBA and FCRA raises questions about meaningful consent that are not unlike those that have been raised in the context of DFA Section 1033 by the Financial Health Network's principles and the CFPB's principles, among others.

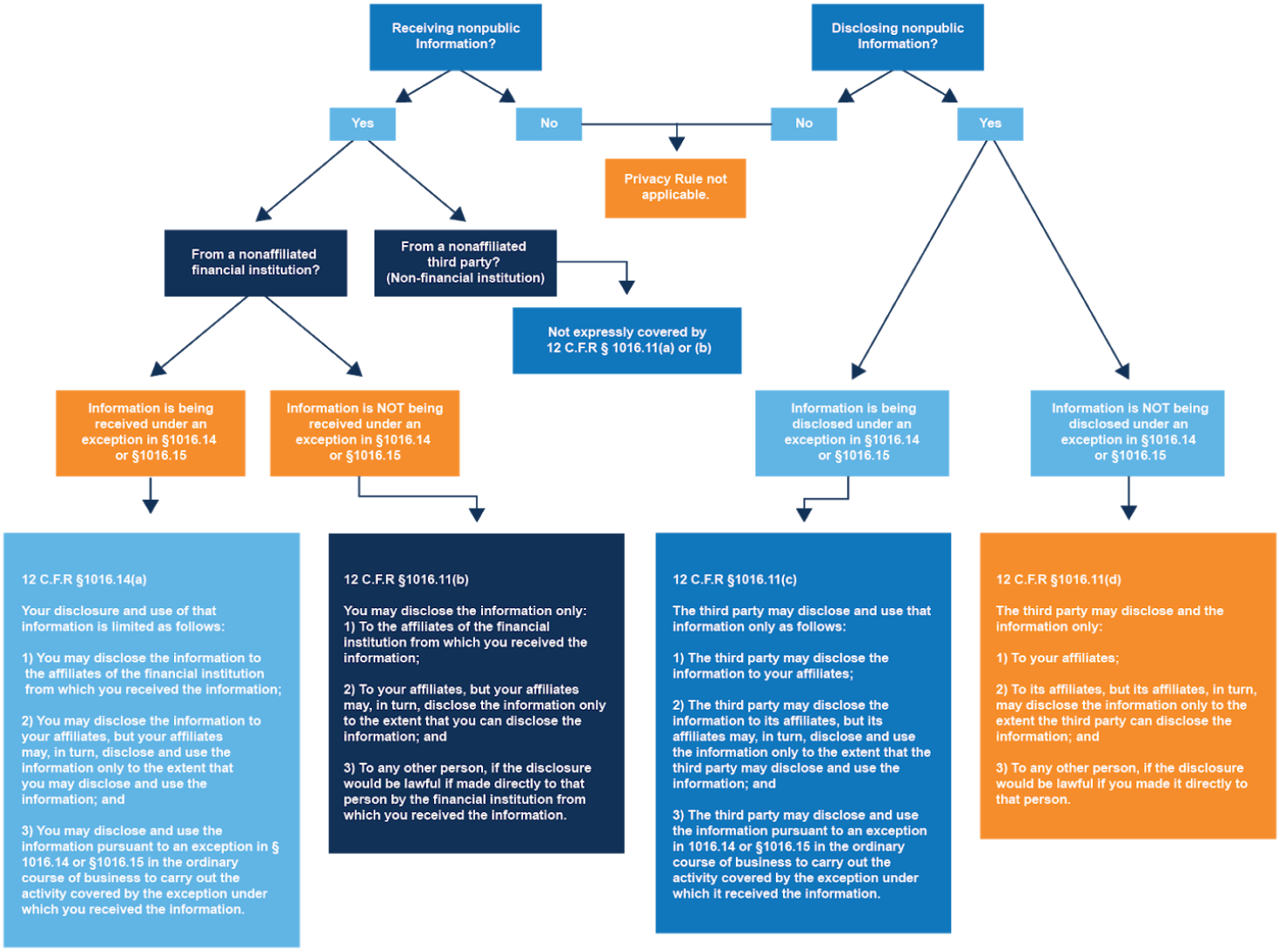
As stakeholders consider the future of the financial data ecosystem, our hope is that this paper can contribute to a foundational understanding of the current framework of financial data regulation to inform future policy analyses and dialogues. We also hope that it can serve as a useful point of comparison and even inspiration for parallel efforts in other regulated industries, as the emergence of new data and technologies, new intermediaries and service providers, and new legal and regulatory questions occurs beyond the financial data ecosystem.

961 *See* CONSUMER FIN. PROT. BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; CTR. FOR FIN. SERVS. INNOVATION, CFSI'S CONSUMER DATA SHARING PRINCIPLES: A FRAMEWORK FOR INDUSTRY-WIDE COLLABORATION (2016), https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2016/10/31152340/2016_Data-Sharing-Principles1.pdf.

962 *See* FINREGLAB, THE USE OF CASH-FLOW DATA IN UNDERWRITING CREDIT: MARKET CONTEXT & POLICY ANALYSIS (2020), https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf.

Appendix A

Summary of Redisclosure and Reuse Limitations



Appendix B

Summary of Select Enforcement Actions related to UDA(A)P Authority

Covered Person	Regulator	Complaint Year	Alleged Violations	Summary
NCO Group	FTC	2004	Unfair and deceptive acts or practices FCRA violations	The FTC charged NCO with reporting accounts to the credit bureaus using later-than-actual delinquency dates, which misrepresented the consumer's credit history and impacted their credit scores. In the complaint, the FTC also averred that "the acts and practices alleged in Paragraph 12 also constitute unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)." The UDAP violation was predicated on identical facts as FCRA violation. NCO ultimately settled the matter with the FTC, which included an agreement to pay a $1.5 million civil penalty.
Sunbelt Lending Services, Inc. Nationwide Mortgage Group, Inc.	FTC	2005	Unfair practices GLBA violations	The FTC brought a complaint against mortgage companies Sunbelt Lending Services, Inc. and Nationwide Mortgage Group, Inc. for violations of GLBA. The FTC alleged that neither company had reasonable protections for customers' sensitive personal and financial information, including names, social security numbers, credit histories, bank account numbers, and income tax returns. In its complaint, the FTC explicitly stated that violations of GLBA also per se constituted violations of the UDAP prohibitions in the FTC Act.
CardSystems Solutions, Inc.	FTC	2006	Unfair or deceptive acts or practices	CardSystems was a company that provided merchants with products and services used in credit and debit card transaction processing. In processing these transactions, CardSystems collected personal information from the magnetic strip of the card, including the card number, expiration date, and other data; CardSystems then stored this information on its computer network. The CardSystems network was hacked in September 2004, which resulted in several million dollars of fraudulent credit and debit card purchases being made with counterfeit cards. The Commission found that CardSystem's "failure to employ reasonable and appropriate security measures to protect personal information it stored caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits," resulting in an unfair act or practice. In making this finding, the FTC pointed to technical information security failures, including storing information in a vulnerable formal, failing to assess vulnerability to cyber attacks, failing to use strong passwords, and failure to limit access between computers on its network and between networked computers and the Internet.

Rental Research Services, Inc.	FTC	2009	Unfair acts or practices FCRA violations	Finding data breach constituted both FCRA violation and unfair practice for failure to take appropriate information security measures to protect consumer reports. In its Complaint, the Commission alleged that RRS had committed a UDAP because it had "not employed reasonable and appropriate measures to secure the personal information RRS collects for sale to its customers, including reasonable policies and procedures to (i) verify or authenticate the identities and qualifications of prospective subscribers; or (ii) monitor or otherwise identify unauthorized subscriber activity." RRS ultimately entered into a stipulated final judgment with the FTC, which included its agreement to "establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."
PLS Financial Services, Inc.	FTC	2012	Deceptive acts or practices GLBA violations	PLS operated stores in multiple states offering short-term installment loans, as well as debit cards, credit cards, and tax preparation assistance. The Commission alleged that PLS failed to take reasonable measures to protect consumer information based on its disposal of documents containing sensitive personal identifying information in unsecured dumpsters near PLS stores. The Commission alleged both a violation of the GLBA Safeguards Rule and that PLS had engaged in a deceptive act or practice because its privacy notice misrepresented to consumers stated that it employed "reasonable and appropriate measures to protect sensitive consumer information from unauthorized access."
Franklin's Budget Car Sales, Inc.	FTC	2012	Deceptive acts or practices GLBA Safeguards violation	Franklin's was a car dealer that provided a consumer privacy notice that advised: "We restrict access to non-public personal information about you to only those employees who need to know that information to provide products and services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard non public personal information." Despite such assurances, Franklin's permitted the personal information of 95,000 consumers to be accessed through a peer-to-peer network via a filesharing application installed on a company computer. The FTC brought claims for a GLBA Safeguards violation and a deceptive practice in misrepresenting that it took appropriate steps to keep consumer information private. In its settlement with the Commission, Franklin's agreed to institute a comprehensive information security program.

EPN, Inc., d/b/a Checknet, Inc.	FTC	2012	Unfair acts or practices	Checknet was a debt collector, which routinely obtained information about its clients' customers, including their names, addresses, dates of birth, genders, Social Security numbers, and medical information. Just as in Franklin's, a peer-to-peer filesharing application installed on a networked computer resulted in 3,800 consumer files containing personal information to be publicly distributed. The FTC did not bring a direct violation of the GLBA Safeguards Rule but instead characterized this conduct as an unfair act or practice under its UDAP authority.
Sequoia One, LLC	FTC	2015	Unfair acts or practices	Sequoia One operated a website through which it gathered extensive personal information from consumers for purported payday loan applications and purchased loan applications from other websites. Consumers believed that they were applying for loans, but Sequoia One sold their application information, including Social Security numbers and bank account information, to companies, including phony online merchants, that fraudulently debited their bank accounts.
Dwolla, Inc.	CFPB	2016	Unfair and deceptive acts or practices	Dwolla operated an online payment system that collected and stored consumers' sensitive personal information and provided a platform for financial transactions. Dwolla collected personal information including the consumer's name, address, date of birth, telephone number, Social Security number, and bank account and routing numbers for each account. Dwolla claimed to employ premier data security practices, including touting that Dwolla transactions were "safer [than credit cards] and less of a liability for both consumers and merchants," that its data-security practices "surpass industry standards," and that Dwolla "sets a new precedent for the industry for safety and security." According to the Consent Order, Dwolla failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access, did not encrypt all consumer personal information, and released applications to the public before completing security testing. The CFPB characterized Dwolla's conduct as deceptive acts and practices with respect to its representations about data security. In doing so, the CFPB was able to compel Dwolla to "adopt and implement reasonable and appropriate data-security measures to protect consumers' personal information on its computer networks and applications," even though it does not have GLBA Safeguards authority.

CMM, LLC et al. (“Cash Tyme”)	CFPB	2019	Unfair practices GLBA violations (Privacy Rule) FDCPA violations	The CFPB brought multiple charges against Cash Tyme for a wide range of conduct, most of which is inapplicable to financial data considerations or UDAP authority. The CFPB alleged GLBA violations for failure to provide initial privacy notices but did not construe this conduct as a UDAP. It also alleged UDAPs unrelated to financial data issues that concerned Cash Tyme’s failure to prevent unauthorized charges or refund overpayments and deceptive advertisement of unavailable services. Specific to financial data-related UDAPs, the CFPB alleged that Cash Tyme required consumers to list their home and cellular telephone numbers and telephone numbers for their employer, supervisor, and four other personal references as a condition of applying for a loan and then attempted to collect on delinquent debts by contacting the third parties that consumers had listed on their loan applications and disclosing the existence of the consumers’ debts without their consent. The CFPB characterized this conduct both as a violation of consumer’s right to data privacy under the FDCPA and as an “unfair” act or practice under its UDAP authority. In describing why the conduct was unfair, the CFPB stated that “[c]onsumers who were customers of Cash Tyme could not reasonably avoid the harm … because they had no reason to anticipate the impending harm and lacked the means to avoid it. They were not warned that Cash Tyme would use this collection tactic, did not know whether, when, or how these calls might occur, did not know that their delinquent debts might be revealed to third parties, and had no control over Respondents’ use of this collection tactic.”
Equifax, Inc.	FTC CFPB 50 U.S. states & territories	2019	Unfair and deceptive acts or practices GLBA Safeguards Rule violations (FTC only)	The FTC and CFPB complaints in this matter were nearly identical. They alleged that Equifax engaged in unfair and deceptive practices in connection with a 2017 data breach of its systems that impacted approximately 147 million consumers. The allegations involved both Equifax’s information security program and data privacy practices that led to the breach, as well as Equifax’s conduct in response to the data breach. In addition, the FTC’s Complaint alleged unfair data security practices related to small businesses and two different violations of the GLBA Safeguards Rule. With regard to unfairness, both agencies alleged that Equifax failed to provide reasonable security for sensitive consumer personal information collected, processed, maintained, or stored on its networks and that doing so caused substantial injury to consumers that they could not reasonably avoid and that was not outweighed by countervailing benefits. In particular, both Complaints list numerous technical deficiencies in Equifax’s information security program and find that these practices, “taken together, failed to provide reasonable security for massive quantities of sensitive personal information stored within Defendant’s computer network.“ Moreover, both the FTC and CFPB alleged that Equifax “could have prevented or

				mitigated the failures … through cost-effective measures suitable for an organization of [its] size and complexity.“ The FTC pleaded that these same failures also constituted the basis for a GLBA Safeguards Rule violation. The CFPB and FTC also brought claims for UDAP violations related to deceptive acts or practices surrounding representations contained in Equifax’s privacy notices. Both agencies alleged that Equifax represented that it limited access to personal information to employees with a reasonable need to access that information and that it employed appropriate safeguards to protect consumer personal information. The FTC brought a substantially similar count regarding Equifax’s representations regarding information access and safeguards with respect to Equifax small business products. The global settlement required Equifax to implement a “comprehensive information security program … designed to protect the security, confidentiality, and integrity of Personal Information” for a period of twenty (20) years. The settlement went on to detail significant technical specifications required as part of the information security program. In addition, the agencies compelled Equifax to submit to ongoing information security assessments by an independent third party approved by the agencies. The settlement provided up to $425 million in monetary relief to consumers and a $100 million civil money penalty to be paid to the agencies.

Appendix C

ECOA Information Use Limitations

Type of Information	Evaluation Limitations
Age or Receipt of Public Assistance Funds	A creditor may not consider the age of an applicant or whether they derive assistance from public funds except: • In an empirically derived, demonstrably and statistically sound, credit scoring system, a creditor may use an applicant's age as a predictive variable, provided that the age of an elderly applicant is not assigned a negative factor or value; • In a judgmental system of evaluating creditworthiness, a creditor may consider an applicant's age or whether an applicant's income derives from any public assistance program only for the purpose of determining a pertinent element of creditworthiness; and • In any system of evaluating creditworthiness, a creditor may consider the age of an elderly applicant when such age is used to favor the elderly applicant in extending credit.
Childbearing or Childrearing	A creditor may not make assumptions or use aggregate statistics relating to the likelihood that any category of persons will bear or rear children or will, for that reason, receive diminished or interrupted income in the future.
Telephone Listing	A creditor may not consider whether there is a telephone listing in the name of an applicant for consumer credit but may consider whether there is a telephone in the applicant's residence.
Income	A creditor may not discount or exclude from consideration the income of an applicant or the spouse of an applicant because of a prohibited basis or because the income is derived from part-time employment or is an annuity, pension, or other retirement benefit.
Credit History	If a creditor considers credit history in evaluating creditworthiness, the credit can consider • The account history of accounts in both the applicant and his/her spouse's name for which both are contractually liable; • Any information provided by the applicant to demonstrate why the credit history is not reflective of his/her creditworthiness; • If requested, the credit history of a former spouse that could provide additional insight into the applicant's creditworthiness.

Income	A creditor may not discount or exclude from consideration the income of an applicant or the spouse of an applicant because of a prohibited basis or because the income is derived from part-time employment or is an annuity, pension, or other retirement benefit.
Credit History[963]	If a creditor considers credit history in evaluating creditworthiness, the creditor shall consider: ● The account history of accounts in both the applicant and his/her spouse's name for which both are contractually liable; ● Any information provided by the applicant to demonstrate why the credit history is not reflective of the applicant's creditworthiness; and ● If requested, the credit history of a former spouse that could provide additional insight into the applicant's creditworthiness.
Immigration Status	A creditor may consider the applicant's immigration status to the extent it is necessary to determine rights and remedies available regarding payment.
Marital Status	A creditor must treat married and unmarried applicants the same, and, in evaluating joint applicants, a creditor cannot treat applicants differently depending on the existing or absence or a marital relationship between the parties.
Race, Color, Religion, National Origin, Sex	Except as otherwise permitted by law, a creditor may not consider any of these factors in any aspect of the credit transaction.[964]

963 In addition to considering the information obtained from credit bureaus, the creditor must also consider, if asked, additional data reflective of information that would be contained in a credit report. *See* 12 C.F.R. § 1002.6(b)(6), cmt. 1002.6(b)(6)-1. This rarely utilized rule, referred to colloquially as the "Shoebox Rule," derives its name from a time when creditors would routinely review paper receipts and other information provided by prospective borrowers.

964 *See* 12 C.F.R. 1002.6. These general evaluation rules are supplemented with specific rules governing extensions of credit in Regulation B. The extension of credit rule covers specific requirements regarding insurance, open-end accounts and the signature of a spouse or other person. Please see 12 C.F.R. § 1002.7 for additional details.

Appendix D

ECOA Record Retention Requirements

Type of Record	Preservation Timeline
Applications	25 months after the date the creditor notifies the applicant of an action taken on the application or of incompleteness.
Existing Accounts	25 months after the creditor notifies an applicant of adverse action.
Other Applications	25 months after the date a creditor receives an application for which the creditor is not required to provide the notification requirements under Regulation B.
Enforcement Proceedings	Until final disposition of the matter, unless an earlier time is allowed by order of the agency or court, if the creditor has actual notice that it is under investigation or is subjected to enforcement proceedings for an alleged violation of the Act, or if it has been served with notice of an civil or criminal action related to ECOA.
Business Credit	12 months for business credit applications or existing credit.[965]
Self-Tests	25 months after a self-test is completed. A creditor shall retain information beyond 25 months if it has actual notice that it is under investigation or is subject to an enforcement proceeding for an alleged violation, or if it has been served with notice of a civil action.
Prescreened Solicitations	25 months after the date on which an offer of credit is made to potential customers.[966]

965 There are different retention requirements for businesses with gross revenue in excess of $1 million, extensions of trade credit, credit incident to a factoring agreement, or other similar types of business credit. Please see 12 C.F.R. 1002.12(b)(5) for additional details.

966 12 C.F.R. 1002.12(b)(1)–(7). The specific requirements of which information needs to be kept vary depending on which of these applies. These can include (i) notification of the action taken, (ii) statement of specific reasons for the adverse action, (iii) statements filed by the applicant concerning a violation of ECOA, and (iv) other correspondence or complaints related to the matter. Please see 12 C.F.R. 1002.12(b) for additional details.