HARVARD LAW SCHOOL | The Case Studies

CSP059
JUNE 2020

Regulating Consumer Permissioned Access to Financial Data

CONNOR TWEARDY AND NAFISA ABUBAKAR ADAMA

TO: Junior.Attorney@joebiden.com
FROM: Senior.Attorney@joebiden.com
DATE: June 1, 2020
RE: Consumer Permissioned Access to Financial Data

Welcome to the Biden for President Policy Team! We've got a live topic that needs your immediate attention, so I hope you're ready to get started. A few groups that support our campaign are at loggerheads over an issue in the Fintech space and we need you to prepare a platform on the topic and recommend a series of steps for us to implement if and when we take the White House.

The debate is between Fintech startups and privacy advocates and focuses on how the Consumer Financial Protection Bureau ("CFPB") should regulate access to consumer financial data. To give you some general background, the United States ("U.S.") federal government is lagging behind many other bodies in regulating consumer data. The European Union ("E.U.") in particular set the new global standard with their General Data Protection Regulation ("GDPR"). That provision implemented consumer rights to access, rectify, and delete their data, the right to data portability, and a number of other novel and innovative consumer protections.[1] The regulation also reaches extraterritorially and applies to any US companies storing or processing personal data of E.U. residents.[2]

In the US, Title V of the Gramm-Leach-Bliley Act ("GLBA") provides some very limited protections for consumer *financial* data (as compared to data regulations of general application). It gives consumers

[1] GDPR, Art. 1-20.
[2] *See* GDPR, Art. 3.

Written by Nafisa Abubakar Adama, HLS LLM 2020, and Connor Tweardy, HLS JD 2020, under the supervision of Professor Howell E. Jackson, James S. Reid, Jr., Professor of Law, Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

nationwide a right to disclosure of privacy practices by some financial institutions and the right to prevent those institutions from sharing their data with non-affiliated parties. Even these narrow rights are subject to exemptions.[3]

At the state level, California enacted a general data protection measure similar to GDPR in the California Consumer Privacy Act ("CCPA"). Similar to GDPR, the CCPA does not restrict its application to any industry in particular but rather applies to all companies that collect the personal information of Californians provided the company is a for-profit, carries on business activities in California, and qualifies as a "business" per the definition in the CCPA.[4] Many national financial institutions are thus subject to these rules.

This patchwork regulatory approach has produced outcries from different groups for different reasons. US financial institutions bemoan the patchwork approach as subjecting them to duplicative regulation. Fintechs and large banks alike fear that other states might follow California's lead and enact local privacy regulations in the absence of a federal approach.[5] Privacy advocates meanwhile argue that too many banks are under regulated at the moment. GBLA provides only narrow rights while CCPA and GDPR are both bounded geographically, leaving many small financial institutions and those that segment their operations into under regulated regional entities.[6] For these reasons, actors on both sides are calling for federal action on data privacy protection, but with different views as to the content of appropriate measures.

One specific issue has come to the forefront of this debate in the financial sector: consumer- permissioned access to financial data. To be clear, this issue goes beyond the rights of consumers themselves to *directly* access their data held by financial institutions. That right is relatively uncontroversial. The debate here is about consumer-*permissioned* access to financial data.[7] An industry has sprung up in recent years with data aggregators and Fintech startups using consumer consent to gather data from traditional financial institutions.[8] These data flows have been integral to the Fintech boom and have produced innovative services and greater competition in the financial sector. In fact, some estimate that increasing access to data in consumer finance could add between $210 to $280 billion a year to global GDP, with up to 50 percent of this total flowing to consumers through enhanced price transparency and tailored product offerings.[9]

[3] 15 U.S.C. § 6802; 12 C.F.R. § 1016.10(a).

[4] CAL CIV. CODE § 1798.140(c)(1).

[5] *See* Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499 (2020), available at https://scholarship.law.unc.edu/ncbi/vol24/iss1/22https://scholarship.law.unc.edu/ncbi/vol24/iss1/22.

[6] *America Should Borrow from Europe's Data-Privacy Law*, The Economist, April 5, 2018, Available at https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-lawhttps://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

[7] *See* Brian Knight, *Statement Regarding CFPB Dodd-Frank Section 1033 Symposium* (Feb. 26, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdfhttps://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf.

[8] U.S. Dep't of Treasury, *A Financial System that Creates Economic Opportunity: Nonbank Financials, Fintech, and Innovation* 22 (2018) (hereinafter "Treasury Fintech Report").

[9] Manyika et al., *Open Data: Unlocking Innovation and Performance with Liquid Information*, Mckinsey Global Institute 91-101, available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-informationhttps://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information.

At the same time, transfer of sensitive financial data from well-regulated entities to unregulated startups carries inherent risks to consumer privacy and data security and these practices have been opposed by many banks and consumer advocates. Consent, if not fully informed, may allow private data to be shared in ways that a consumer would likely not approve. A consumer might think they are sharing only a small part of their data for a limited purpose only to find that a Fintech or other third party is receiving income data or other sensitive information they did not intend to share, holding that data indefinitely, and even reselling it on to other groups.[10] Startups and other small Fintech players also make attractive targets for hackers, creating even more unintended spreading of a consumer's data.[11]

Our objective is to find a policy platform that addresses these concerns and makes the sharing of consumer financial data both freer and safer. We have two basic sets of levers to pull in reaching that goal. First, we can direct the CFPB to use the authority granted to it under Section 1033 of the Dodd-Frank Act ("Section 1033 of the DFA") to issue a new rule clarifying the right of consumers to grant permissioned access to their data. Second, we can have the CFPB issue guidance regarding how existing regulations apply to these new business models.

Senior staff would like you to prepare a briefing in which you propose a regulatory direction for our administration and propose concrete steps that should be taken.[12] Please consider the reactions we should expect from Fintech firms, established financial institutions (both large and small), and privacy advocates, including a discussion of how we might structure our approach to be responsive to their legitimate interests.

Included is a memo we obtained from the CFPB to help get you started. It was prepared in advance of a symposium that was held on this topic earlier this year and lays out several of the key regulatory questions at issue.

Here's a list of specific questions to address during the briefing:

<u>Section 1033 of the DFA</u>

1. Does Section 1033 of the DFA include a right to consumer-permissioned access to data?
2. Assuming a consumer's consent is informed, should their ability to grant permissioned access to their data be unlimited?
3. Should financial service providers be able to decline transfers to certain parties despite customer consent (e.g. if they find that a company has insufficient security protocols in place to protect the transferred data)? If so, who should determine the criteria for disqualification?

[10] National Consumer Law Center (on behalf of its low income clients), *Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act* (Feb. 12, 2020), accessible at https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdfhttps://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf (hereinafter "NCLC Symposium Statement").

[11] American Bankers Association, *Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048* 9-10 (Feb. 21, 2017) available at https://www.regulations.gov/document?D=CFPB-2016-0048-0041https://www.regulations.gov/document?D=CFPB-2016-0048-0041 (hereinafter "ABA RFI Response").

[12] Please also assume that our administration will have sufficient authority and influence to guide the direction of the CFPB on this issue, setting aside their status as an independent agency.

4. Does the text of DFA 1033 specify whether consumers may access observed and/or inferred data under their financial service provider's control? If the text is ambiguous, what stance should the CFPB take?
5. Should the CFPB take any steps to encourage API adoption and discourage the use of screen-scraping?

FAIR CREDIT REPORTING ACT ("FCRA")

6. Are data aggregators consumer reporting agencies under FCRA?

7. Is a financial institution a data furnisher if it provides an API through which aggregators access data?

ELECTRONIC FUNDS TRANSFER ACT ("EFTA")

8. As a legal matter, do banks remain liable under Reg E for unauthorized charges made in their systems that result from a consumer data breach at a Fintech company?
9. As a policy matter, how should liability be apportioned between Fintechs and traditional financial institutions in such cases?

Note that we also have a second policy team addressing the broader question of whether our administration should adopt a general privacy regulation (in the same vein as GDPR or CCPA). Their recommendation will likely have implications for your research and we may ask you both to coordinate your work, and possibly even present at a joint meeting. I'm attaching an academic memorandum that they are using as a reference point.

Thank you for your help and we look forward to your presentation.

Best,
Policy Team Lead

Memorandum

DATE: February 20, 2020
TO: Kathy Kraninger, Director, CFPB
Tom Pahl, Policy Associate Director for Policy, Research and Regulations
FROM: Office of Susan Bernard, Assistant Director for Regulations
RE: Primer for the Upcoming Symposium on Consumer Access to Financial Data

Thank you both for your help in organizing the upcoming Symposium on Consumer Access to Financial Records. This internal memorandum is meant to serve as a primer to help prepare you and your teams for the debates that we expect to take place at the event, specifically focusing on the regulation of data aggregation and consumer-permissioned access to financial data. It first looks at the basic policy concerns underlying this debate and then turns to a general description and brief history of the market for consumer financial data. It ends with a discussion of ongoing regulatory debates that could require CFPB actions including potential rulemaking under Section 1033 of the Dodd-Frank Act ("Section 1033 of the DFA") and the need for guidance on the applicability of other existing regulations to data aggregation and Fintech.

General Policy Considerations

Regulation of the modern information economy has increasingly focused on giving consumers greater control over their own data. This emphasis on consumer autonomy has led several countries to recognize new consumer rights relating to their personal data, such as rights to access, correction and deletion. One less-discussed right in this toolkit is the right to data portability. The right to data portability allows individuals to obtain and reuse their personal data and can require data controllers to transfer the data to other service providers upon a consumer's request.[13] The right to permissioned access to consumer data is a variation of this concept.

Policy debates regarding the desirability of the right to data portability, and the appropriate limitations that should apply to it, focus on balancing four policy considerations:

- *Consumer Autonomy*[14] - The datafication of the information economy has led to a general loss in power of consumers relative to businesses. Consumers have little ability to negotiate privacy terms in contracts as a result of insufficient expertise, asymmetric information, and a collective action problem. This leaves them without many options to exercise choice and control over their personal information (apart from declining to participate all together in certain industries). Regulation can address this power imbalance, restoring consumer choice and meaningful consumer control over their data.

[13] See GDPR Art. 20.

[14] *See generally* Michiel Rhoen, *Beyond consent: improving data protection through consumer protection law*, 5 *Internet Policy Review* (Mar. 31, 2016), accessible at https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-lawhttps://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law.

- *Competition*[15] - Access to data is a driving competitive dynamic in many modern industries. A company with more data on a consumer is often better able to serve that consumer. For instance, Amazon's ability to recommend books based on your shopping history gives it an advantage over Barnes & Noble. Allowing consumers to move their data between service providers makes it easier for new entrants to compete in the market or to provide new and innovative services that make use of that data.

- *Privacy*[16] - Sharing consumer data between providers inherently reduces a consumer's privacy. Consent arguably mitigates this concern, but regulators and privacy advocates worry that consent alone does not provide sufficient protection. Consumers may not understand the types of data that are being shared, whom they might be shared with, and how they might be used. Absent regulation, the private sector arguably has little incentive to ensure that consent is fully informed and effective, worsening consumer privacy.

- *Security*[17] - Data breaches and other illegal activities create costs for both consumers and businesses. Increasing data sharing between service providers introduces vulnerabilities that can increase the likelihood of breaches. For example, fraudsters may entice consumers to give them permission to access their data. Startups and other smaller companies may have weaker security relative to larger market players, making them attractive targets for hackers.

In the United States, the current regulatory debate surrounding the implementation of a right to permissioned access to consumer financial data involves the interaction of these considerations with the current state of the market for consumer financial data and, specifically, the emergence of modern financial data aggregators.

The Market for Financial Data Aggregation

Data Aggregation as a Business

Data aggregation is the process by which information from one or more sources is gathered and standardized.[18] In finance, the basic form of this market involves four groups of players:

- *Consumers* are individuals who use financial services. Their interactions with financial service firms create consumer financial data. They also decide which consumer Fintech applications they would like to use, and provide their consent to facilitate the flow of data from financial service firms to data aggregators and those consumer Fintech applications.

- *Financial services firms* are those that gather consumer financial data from users in the first instance, usually through direct commercial interactions with consumers. These are the banks,

[15] *See* Michael Barr et al, Consumer Autonomy and Pathways to Portability in Banking and Financial Services, University of Michigan Center on Finance, Law and Policy 1-2 (November 3, 2019), available at http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdfhttp://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[16] *See* NCLC Symposium Statement, *supra* note 10, at 4-5.

[17] *See* ABA RFI Response, *supra* note 11, at 9-10.

[18] Treasury Fintech Report, *supra* note 8, at 23.

insurance companies, wealth management firms, and other financial institutions that one might associate with traditional consumer finance. The companies are the source of consumer financial account and transaction data.

- *Data aggregators* access, aggregate, standardize, store, and disseminate consumer financial account and transaction data from a variety of financial services firms. They act as intermediaries between financial service firms as suppliers and consumer Fintech applications as clients. They may, but generally do not, have a direct commercial relationship with consumers. Instead they commonly function as back-end tools enabling Fintech applications.

- *Consumer Fintech applications* use consumer financial data to provide value-added services to consumers that may either complement or substitute services provided by traditional financial institutions. They obtain the data needed to provide their service either directly from financial services firms or from a data aggregator.[19]

A single entity may play multiple roles in this system. For example, a Fintech startup using a machine learning algorithm to make loans may at once use consumer financial data to make a lending decision, then gather new data as the loan is paid down.

Financial data aggregation is a technically demanding task, involving the large upfront cost of connecting to thousands of different financial institutions.[20] Connecting to banks can be particularly difficult. Banks are incentivized to impose switching costs on their depositors, giving them little reason to invest in easy data portability.[21] As a result, a handful of data aggregators who have sunk time and effort into making these connections serve as the backbone of the modern Fintech ecosystem.[22] A company like Plaid provides a single interface through which a startup can interact with the data from thousands of financial services firms.

Data Aggregation Methods

In practice, data aggregators generally access consumer financial data through one of two methods: screen-scraping or application programming interfaces ("APIs").[23]

Screen-scraping is a method by which a data aggregator can retrieve consumer data from a financial services provider that does *not* have the technology to allow other companies to access their data directly.[24] Under this method, a consumer will give a Fintech application their login credentials for each financial service provider at which they have an account. For example, a consumer might want to use the application Mint to view their total cash balance across the multiple banks at which they have open

[19] *Id.* at 23-4.

[20] *Id.* at 25-7.

[21] Thomas P. Brown, *Section 1033 of Dodd-Frank—A Decade of Waiting for the Green Flag to Drop*, available at https://files.consumerfinance.gov/f/documents/cfpb_brown-statement_symposium-consumer-access-financial-records.pdfhttps://files.consumerfinance.gov/f/documents/cfpb_brown-statement_symposium-consumer-access-financial-records.pdf.

[22] *See* MX Technologies Inc., *A List of Financial Data Aggregators in the United States*, blog post (Mar. 5, 2018), available at: *https://www.mx.com/moneysummit/a-list-of-financial-data-aggregators-in-the-united-states*. (listing eight major consumer financial data aggregators in the United States).

[23] Treasury Fintech Report, *supra* note 8, at 26-8.

[24] *See id.*

accounts. The consumer would then give Mint their login credentials for, say, Bank of America and JP Morgan Chase. Mint would then, either directly or through a tool like Plaid, use those credentials to automatically login to the consumer's online account at each of those banks and "scrape" their account balances off of the screens made available through the banks' web portals. With this information, Mint could display the aggregate consumer's aggregate bank account balance.

Screen scraping is an effective method for data aggregators to access data from banks that may not have the resources to build an API, improving the comprehensiveness, and thus the usefulness, of Fintech applications. But it has drawbacks as well and is generally considered a suboptimal solution.[25] Most notably, it requires users to trust small Fintech startups with their login credentials to all of their financial accounts. These startups are then attractive targets for hackers and new sources of vulnerabilities for banks. It can also impose costs on banks as the repeated requests to their web portals needed to refresh the data in these apps will quickly increase their web volume and costs. It's even suboptimal for data aggregators as they need to track any changes that banks make to their web interfaces.

APIs, by contrast, are software packages that allow a data source or other system to interact with or be used by other software.[26] This can be thought of as a direct feed that allows data aggregators and Fintech applications to interact with a financial service firm's data without requiring the consumer to store their login credentials with the new service. APIs allow banks and other data providers to specify with granularity which data fields they are comfortable sharing. They also allow for more robust security features and make related information technology costs easier to predict. Their primary drawback is that they cost money to develop, potentially placing an excessive burden on small financial institutions and creating barriers to entry.[27] By definition, they also require data providers to allow data under their control to be shared, making it easier for banks to shut off access and otherwise exert control over smaller companies that rely on the data provided therein.[28]

Increasing Demands for Regulation

As is often true when regulating financial technology, a bit of history can help explain the stakeholder battle taking place today. Data aggregators have been using screen scraping to accumulate financial data for the past twenty years at least.[29] But, data aggregation and the Fintech ecosystem built on it have begun to grow exponentially in the last decade. By 2015, the industry had grown large enough to draw the ire of the traditional financial institutions it was disrupting.[30] That year, a few large banks tried to shut

[25] *Id.*

[26] *Id.*

[27] *See* Independent Community Bankers of America, *Docket No. CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records*, 6 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0035https://www.regulations.gov/document?D=CFPB-2016-0048-0035 (hereinafter "ICBA RFI Response").

[28] *See* Plaid Technologies, Written Statement for the Symposium on Consumer Access to Financial Records (Feb. 19, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdfhttps://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf (hereinafter "Plaid Symposium Statement").

[29] Treasury Fintech Report, *supra* note 8, at n.46.

[30] Brian Hurh et al, *Consumer Financial Data Aggregation & the Potential for Regulatory Intervention*, Davis Wright Tremaine LLP (June 2010), available at https://www.dwt.com/files/paymentlawadvisor/2017/06/Blog_Article_-_Consumer_Financial_Data_Aggregation.pdfhttps://www.dwt.com/files/paymentlawadvisor/2017/06/Blog_Article_-_Consumer_Financial_Data_Aggregation.pdf.

the industry down and turned off aggregators' access to consumer financial account information.[31] Banks justified this decision by pointing to the security issues created by these applications and the operational costs incurred on their servers from the constant stream of aggregator data requests.[32] But consumer outcry forced banks to reverse course within days, allowing data aggregators to access their data even as the banks sought new ways to limit these requests.[33]

The CFPB entered the scene soon after, expressing concern with the banks' actions. CFPB Director Richard Cordray chastised financial institutions for "looking for ways to limit, or even shut off, access to financial data rather than exploring ways to make sure that such access, once granted, is safe and secure."[34] The CFPB subsequently issued a Request for Information ("RFI") to: (1) help the industry develop best practices to deliver benefits to consumers and address potential consumer harms; and (2) evaluate whether any guidance or future rulemaking is needed.[35] The Bureau followed the RFI with a document maintaining that Section 1033 of the DFA granted consumers the right to give permission to third parties to access their data, but stating that right should be qualified.[36]

Despite these actions, uncertainty persists over fundamental questions and furor for new regulation has grown on all sides. Today, data aggregators and Fintech applications ask the CFPB to use its rulemaking authority under Section 1033 of the DFA to confirm the right to the permissioned access to consumer financial data.[37] Banks ask regulators to subject these new players to the same regulatory scrutiny under which they operate, and to clarify uncertainty over who bears liability for breaches.[38] Commentators on both sides criticize the CFPB's lack of action, arguing that the lack of decisive regulatory action is distorting the market's development.[39] These forces convinced the CFPB to convene the upcoming Symposium on this topic.

Potential Areas for CFPB Action

The various stakeholders at the Symposium have divergent interests and all lay out different paths that the CFPB might take. The regulatory questions the CFPB is facing fall into two main groups: first, whether and how to implement Section 1033 of the DFA; and second, how to apply other preexisting regulations to data aggregation and the new economy for consumer financial data. These two courses of action are not mutually exclusive and either would help increase certainty in this space. The CFPB should assess the

[31] *See* Robin Sidel, *Big Banks Lock Horns With Personal-Finance Web Portals*, Wall Street Journal (November 4, 2015), available at https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450.

[32] *See* Patrick Dehan, *Banking, Consumer Groups Battle Over Mint.com*, Associations Now (Nov. 16, 2015), available at http://associationsnow.com/2015/11/banking-consumer-groups-battle-mint-comhttp://associationsnow.com/2015/11/banking-consumer-groups-battle-mint-com.

[33] Hurh et al, *supra* note 30 at 2.

[34] Prepared Remarks of CFPB Director Richard Cordray at Money 20/20, October 23, 2016, available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-money-2020/.

[35] Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83606 (Nov. 22, 2016).

[36] CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[37] *See, e.g.*, Plaid Symposium Statement, *supra* note 28.

[38] *See, e.g.*, Statement of PNC Bank, Symposium on Consumer Access to Financial Records, https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdfhttps://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf.

[39] *See* Knight, *supra* note 7, at 3.

merits of all of the options on the table as well as their interrelationships to set a policy platform that expands access to consumer financial data while still protecting consumer privacy and security.

New Regulation Pursuant to Section 1033 of the DFA

The ongoing debate regarding a potential rulemaking under Section 1033 of the DFA has coalesced around five issues:

Issue One: Does Section 1033 of the DFA include a right to consumer-permissioned access to data?

An ongoing debate questions whether Section 1033 of the DFA includes a right to consumer-*permissioned* access to financial data, or only a right to *direct* consumer access to financial data. Direct consumer access would only require financial institutions to share data with the consumers directly. Consumer-permissioned access, by contrast, would also force them to share data with other companies designated by the consumer, potentially including their competitors.

Section 1033 of the DFA specifies that "a covered person shall make available *to a consumer*, upon request" (emphasis added), certain data regarding that consumer that the covered person either possesses or controls.[40] Such right is also "subject to rules prescribed by the Bureau." Notably, the definition of "consumer" in Title X of Dodd-Frank includes not only an individual, but "an agent, trustee, or representative acting on behalf of an individual."[41] Notably, one of the drafters of the provision, Professor Michael Barr, has noted 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."[42]

Fintechs believe themselves to be covered by the broad definition of "consumer," obligating covered persons to share permissioned data with them. Traditional financial institutions, on the other hand, note that the plain language of Section 1033 itself only mentions consumers, that the broad language in the definition's section does not appear to contemplate forcing companies to give valuable data to their competitors, and that Congress could very easily have expanded the provision to create this right.[43]

Following the 2017 RFI, the CFPB issued the Consumer Protection Principles, which touch on this question. That document states that consumers are "able to authorize trusted third parties to obtain such information… to use on behalf of consumers."[44] Still, the debate persists. In a recent case, PNC used the arguments outlined above to deny Venmo access to consumer data despite consumer requests that the

[40] 12 U.S.C. §5533 (2010).

[41] 12 U.S.C. §5481(4) (2010).

[42] Michael Barr et al, Consumer Autonomy and Pathways to Portability in Banking and Financial Services, University of Michigan Center on Finance, Law and Policy 4 (November 3, 2019), available at http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdfhttp://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[43] *See, e.g.*, ICBA RFI Response, *supra* note 27.

[44] Consumer Protection Principles, *supra* note 36, at 3.

data be transferred.[45] Commentators have thus argued that the CFPB should create a rule to resolve the issue and clarify the rights of third parties to consumer-permissioned access to financial data.[46] Such a rule would also be an opportunity for the CFPB to regulate the means of obtaining consent, the limits of consented sharing of information, and other open policy debates.[47]

- Should the CFPB engage in a rulemaking process to clarify the existence of a right to consumer-permissioned access to data in Section 1033 of the DFA?
- Does the CFPB face legal risk in passing a rule that specifies a right for consumer-permissioned access to data? Could such a rule be struck down for exceeding the CFPB's statutory mandate?

Issue Two: Should the CFPB limit the power of consumers to grant third parties permissioned access to their financial data?

Assuming that consumers have a right to the permissioned sharing of their data, various stakeholders disagree over the appropriate limitations that the CFPB should impose on that right.

Fintechs argue that consumer autonomy is best supported by a broad consumer right to consent to the sharing of data, subject to disclosure requirements and the right to revoke consent.[48] Requiring consumers to jump through added hoops to share their data is an inherent limit on consumer choice and autonomy. Further, empirical evidence shows that consumers appear to value convenience and a smooth user experience in most transactions over added privacy protections.[49] Consumers are then better served by full disclosure and a continuing ability to revoke their consent, such an option encourages transparency and gives those who are privacy-conscious the ability to exercise choice.

Privacy advocates, on the other hand, argue that the ability to consent should be subject to inherent limits.[50] Proposed limits include a mandatory period after which consent expires requiring it be granted again, and limits on the number of data fields or data uses that may be consented to at once.[51] Their argument comes out of two concerns. First, consent may be insufficient to safeguard consumer privacy.[52] Even if the disclosure is provided, Fintechs and data aggregators potentially have an incentive to obfuscate

[45] Kate Rooney, *PNC's fight with Venmo highlights bigger issue over who owns your banking data,* CNBC (Dec. 16, 2019), available at https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.htmlhttps://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html.

[46] *See* Knight, *supra* note 1, at 3.

[47] Another ongoing debate concerns whether or not Section 1033 of the DFA is self-executing. If it is self-executing, then consumers already enjoy the rights mentioned in the statute, even absent a CFPB rulemaking. If not, then financial institutions do not have enforceable obligations under this section absent CFPB action. This question is relevant if a new administration wants to enforce this right before rulemaking is complete. Notably, the CFPB announced that Section 1071 of the DFA, which has some similar language to Section 1033, is not self-executing.

[48] *See, e.g.*, Plaid Technologies, *Plaid response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048,* 1-2 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0058https://www.regulations.gov/document?D=CFPB-2016-0048-0058.

[49] *See* Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality in Decision Making*, 3(1) IEEE, Security and Privacy Magazine 26-33 (Jan. 2005), accessible at https://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdfhttps://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.

[50] *See, e.g.*, NCLC Symposium Statement, *supra* note 10, at 4-5.

[51] *Id.*

[52] *See generally* Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013), accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

them. As such, consumers are unlikely to fully appreciate what data they are sharing, with whom it is shared, and how that data may be used. Access may also last longer than expected by a consumer who only intended it for a one-time transaction.[53] Second, consumer consent may only represent a limited act of autonomy. Structural power imbalances between data subjects and data controllers mean that consumer consent does not always mean consumer choice.[54] Consent provisions are included as non-negotiable terms in contracts of adhesion, in which the average consumer does not have the capacity or the competency to change. If general consent is an option, it will then become the norm. The mandated parsing of consumer consent, whether by time, data field, etc., gives consumers more effective opportunities to exercise choice.

- Should the CFPB impose limits on the power of consumers to grant permissioned access to their data?
- If yes, what forms of limitations would be appropriate?
    - *Time bounds* - should permissioned access be time limited, requiring periodic renewal for continued access? Should consent be self-expiring, requiring Fintechs to renew consent or delete a consumer's permissioned data after a set period?
    - *Use* - should consumers be able to provide access to data for general use or without specifying a use?
    - *Permissioned data fields* - should consumers be able to grant a Fintech permission to access all of their data held by another entity? Or should consumers need to consent to the sharing of individual data elements? What if the data transfer involves transferring a relationship to a new service provider (e.g. switching banks)?
    - Other?

Issue Three: Can banks deny an entity's access to financial data in spite of a proper consumer request?

Returning to the text of Section 1033 of DFA, the CFPB will also need to grapple with the limits of which third parties properly qualify as an "agent, trustee, or representative acting on behalf of an individual." Most parties agree that the ability of a consumer to grant permission to a third party is not unlimited. Financial institutions should have some latitude to ensure that their clients' data is not transferred to untrustworthy providers. For example, it seems logical that they should be able to condition access on adequate security measures being in place. In their previous statements on this topic, the CFPB alluded to this limitation and specified that permissioned access should occur "in a safe manner."[55]

At the same time, Fintech startups and data aggregators complain that financial institutions are likely to abuse this kind of discretion.[56] As a result of their size, financial institutions often enjoy a bargaining advantage relative to small Fintech startups. These kinds of discretionary rights to revoke access exacerbate that issue and give financial institutions leverage in any negotiations. Some financial institutions also use this kind of logic as a shield to deny properly permissioned access to Fintech applications and evade the spirit of Section 1033.[57] Determining the shape of any such discretionary right will have a major impact on any potential rule.

[53] NCLC Symposium Statement, *supra* note 10, at 4-5.

[54] *See* Rhoen, *supra* note 15.

[55] Consumer Protection Principles, *supra* note 36, at 3.

[56] *See, e.g.*, Plaid Symposium Statement, *supra* note 28.

[57] *See, e.g.*, *PNC's fight with Venmo*, *supra* note 40.

- Should financial service providers be able to decline transfers to certain parties despite customer consent (e.g. if they find that a company has insufficient security protocols in place to protect the transferred data)? If so, who gets to determine the criteria for disqualification:
    - Individual financial institutions?
    - A self-regulatory organization or other industry-level group?
    - The CFPB (through rulemaking, guidance, etc)?
    - A hybrid approach?

Issue Four: What type of data must be shared?

Section 1033 of the DFA states that covered persons must provide access to "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, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[58] The scope of the data that must be provided is further limited by several exceptions, including one that provides that covered persons need not share "any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors."[59]

Regulators in other countries have conceptualized consumer data as falling into three categories: volunteered, observed, and inferred.[60] Volunteered data includes information that is readily and knowingly provided by the consumer to the service provider, e.g. one might share their social security number when setting up an account. Observed data includes data that is passively collected by the service provider over the course of a relationship, such as a lender tracking whether you prefer to pay your monthly bill through their website or mobile application. Finally, inferred or derived data covers any information generated about you using those other data points, such as a credit score.[61]

The plain language of the statute appears to leave ambiguous whether or not all three of these types of data must be shared upon request. Volunteered, observed, or inferred data may all "concern" the product or service that a bank provides to a customer. The exception for confidential commercial information also notably mentions the algorithms used to generate risk scores, but not the risk scores themselves. The National Consumer Law Center ("NCLC") in particular has argued that the CFPB should interpret this language to allow consumers access to any credit score data that a financial institution may have in its possession.[62]

Such a measure would almost certainly be opposed by financial institutions. They are likely to consider inferred information to be proprietary, even if it does not rise to the same level of confidentiality as the

[58] 12 U.S.C. §5533 (2010).

[59] *Id.*

[60] *See* Article 29 Data Prot. Working Party, Guidelines on the Right to Data Portability, 16/EN WP242 at 10 (April 5, 2017) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[61] *Id.*

[62] National Consumer Law Center, *Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048*, 7 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0072https://www.regulations.gov/document?D=CFPB-2016-0048-0072 (hereinafter "NCLC RFI Response).

algorithm used to determine a credit score. Such data also seems at odds with the volunteered data listed in the first paragraph of Section 1033 of the DFA ("costs, charges, and usage data"). In foreign contexts, academics have also questioned whether such a right to inferred information is a privacy-oriented overreach that limits innovation and competitiveness objectives of data access rules.[63] The CFPB will need to provide clarity on the scope of the data fields that a consumer may request.

- Does the statutory text of Section 1033 of the DFA indicate whether consumers may access observed and/or inferred data regarding the consumer under their financial service provider's control?
- Specifically regarding inferred data, if the text is ambiguous, what stance should the CFPB take?
    - Should the CFPB prescribe a regulatory right to access some or all kinds of inferred data?
    - Should the CFPB explicitly exclude some or all kinds of inferred data from the scope of Section 1033 of the DFA?
    - Should the CFPB remain silent on this issue for the time being?

Issue Five: To what extent should the CFPB regulate the method of transfer and try to move the industry away from screen-scraping?

As discussed above, there is near-universal acknowledgement among industry stakeholders that screen-scraping is a risky and suboptimal practice, and that APIs are a safer, more reliable method that also allow consumers more control over how their data is shared.[64] Recognizing these arguments, a number of foreign jurisdictions have taken affirmative steps to promote the use of APIs for the transmission of consumer financial data.[65] With its open banking initiative, the United Kingdom mandated that the largest banks in the country had to establish APIs and provided an opt in regime for smaller banks to join the program. The European Union adopted the Revised Payment Service Directive, requiring banks to give licensed parties access to account data. It did not mandate the use of APIs, but encouraged their use and provided standards to make APIs more interoperable where implemented. Singapore has also issued guidance encouraging the use of bank APIs but has not made any regulatory mandate on the subject.[66]

Industry efforts in the US to move toward greater API use have had little success outside of the largest financial institutions.[67] Part of this reflects a general reluctance on the part of financial institutions to make it easier for consumers to shift their business to other companies. At the same time, there has been concerted opposition from small and mid-sized banks who do not want to take on the added burdens of implementing this technology.[68] Any mandate to adopt the technology would need to account for their needs and take affirmative steps to prevent this requirement from becoming a barrier to entry for new banks.

[63] Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay & Ignacio Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, COMPUTER L. & SECURITY REV. 193 (2018).

[64] Treasury Fintech Report, *supra* note 8, at 34-5.

[65] *Id.*

[66] *Id.*

[67] Fidelity Investments, *Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048*, 6-8 (Feb. 21, 2017), available at https://www.regulations.gov/document?D=CFPB-2016-0048-0053https://www.regulations.gov/document?D=CFPB-2016-0048-0053.

[68] ICBA RFI Response, *supra* note 27, at 7.

The CFPB has rulemaking authority under Section 1033 of the DFA to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information…"[69] The CFPB should explore whether or not it should use this authority to follow the lead of other countries to resolve the industry logjam in this area.

- Should the CFPB take any steps to encourage API adoption and discourage the use of screen-scraping?
    - Should the CFPB provide any regulatory mandate for the use of APIs (e.g. through rulemaking)? If so, should it be targeted at only large banks and should there be any relief to help smaller banks adopt the technology?
    - Should the CFPB provide regulatory guidance to encourage and standardize API implementation?
    - Should the CFPB take a more conservative approach and wait to see how other changes impact the direction of the industry on this point?

Applying Existing Regulations to Data Aggregation

The above issues relate to Section 1033 of the DFA and how the CFPB should implement it. Regardless of the approach taken on that topic, regulators will need to also grapple with how to apply existing regulations to data aggregators, Fintech startups, and other new participants in the financial sector. In general, these new players have resisted the application of existing financial regulatory regimes. Financial institutions, meanwhile, claim that the underenforcement of existing regulation is allowing Fintechs to practice a form of regulatory arbitrage and that they should be brought under the same regulatory umbrella.[70]

Fair Credit Reporting Act ("FCRA")

The FCRA is one of the other pieces of the patchwork of privacy regulations that apply to the US financial sector.[71] Among other things, the FCRA gives consumers access to the data in their consumer reports, gives them the opportunity to restrict the use of those reports, and requires financial institutions to conduct reasonable investigations if a consumer disputes the accuracy of the information therein.[72]

Crucially, the FCRA is the primary tool that provides American consumers with a right to rectify incorrect data that is being used to judge their creditworthiness.[73] This right is arguably even more important in the

[69] 12 U.S.C. §5533 (2010).

[70] *See, e.g.*, ABA RFI Response, *supra* note 11.

[71] For a general summary of the rights contained within this statute, see the Federal Trade Commission's *A Summary of Your Rights Under the Fair Credit Reporting Act*, accessible at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdfhttps://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

[72] *See* Regulation V, 12 C.F.R. § 1022 https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1022/1/https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1022/1/ (hereinafter "Reg V").

[73] Carlo Kostka and Sam Adriance, *The Effects of GDPR on U.S. Financial Institutions*, Covington and Burling (blog post), available at https://www.cov.com/-/media/files/corporate/publications/2018/08/the_effects_of_gdpr_on_us_financial_institutions.pdfhttps://www.cov.com/-/media/files/corporate/publications/2018/08/the_effects_of_gdpr_on_us_financial_institutions.pdf.

context of Fintech applications. Screen scraping and other suspect data gathering techniques make alternative data more likely to be inaccurate than traditional data.[74] The CFPB's post-RFI statements also stressed the importance of accuracy as one of their key principles in protecting consumers in the new data sharing economy, stating that consumers should have a reasonable expectation that the data regarding them is accurate and that they'll have a meaningful opportunity to dispute inaccuracies.[75]

As a legal matter, there has been an ongoing debate over whether or not data aggregators fall under the FCRA's regulatory boundaries.[76] The FCRA's primary obligations are imposed on "consumer reporting agencies." A consumer reporting agency is any person that regularly assembles or evaluates consumer credit information for the purposes of providing consumer reports. A consumer report is defined as any information that relates to an individual's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, and mode of living, or that is otherwise collected to be used in assessing someone's eligibility for credit.[77] By these terms, a consumer report encompasses broad categories of information that are not limited to credit-based data. Consumer advocacy groups point to the apparent breadth of this language and the important policy goals advanced by the statute to argue that it should apply to Plaid and other data aggregators in the new financial ecosystem.[78]

However, many data aggregators continue to argue that they should not be subject to the FCRA's requirements.[79] One of their main arguments rests on the requirement that a consumer reporting agency "regularly engage[]… in the practice of *assembling or evaluating* [consumer reports] (emphasis added)."[80] The Federal Trade Commission, which had regulatory authority over this statute before the establishment of the CFPB, has interpreted this language relatively narrowly. It defined "assembling" to mean "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."[81] On the other hand, "evaluating" means "appraising, assessing, determining or making a judgment on such information."[82]

Some data aggregators, including Plaid, have argued that they do neither and merely function as a "pipe" for data.[83] In this telling, the aggregator is merely a piece of software that serves as a data conduit, allowing Fintechs themselves to assemble and evaluate data from financial institutions. The Ninth Circuit found a similar argument persuasive in *Zabriskie v. Federal National Mortgage Association*, holding that Fannie Mae was not a consumer reporting agency because it merely provided a software tool that allowed mortgage lenders to assemble or evaluate consumer information themselves.[84] On the other hand, a few aggregators, including Finicity, feel that their activities constitute more than functioning as a conduit and

[74] NCLC Symposium Statement, *supra* note 10.

[75] Consumer Protection Principles, *supra* note 36.

[76] NCLC Symposium Statement, *supra* note 10.

[77] Reg V, *supra* note 71, at § 1022.130(c)-(d).

[78] NCLC Symposium Statement, *supra* note 10, at 6-9.

[79] *See, e.g.*, John Pitts, *Statement before the Senate Committee on Banking, Housing and Urban Affairs* (Mar. 15, 2019), accessible at https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Plaid1.pdf.

[80] Federal Trade Commission, *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations* 29, July 2011, https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting- act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

[81] *Id.*

[82] *Id.*

[83] *See* NCLC Symposium Statement, *supra* note 10, at 8.

[84] 912 F.3d 1192 (9th Cir. 2019).

have already registered as consumer reporting agencies.[85] Consumer groups argue that most, if not all, aggregators fall into this latter category and differences in the business models of Plaid and Finicity do not justify different treatment.[86] Resolution of this debate will significantly impact the coverage of the rights in the FCRA.

If data aggregators are determined to be consumer reporting agencies, a secondary debate asks whether or not all of their sources of data then become data furnishers under the FCRA. A data furnisher is an entity that furnishes information relating to consumers to one or more consumer reporting agencies for provision in a consumer report.[87] The FCRA imposes various obligations on these entities including avoiding the transmission of data it suspects may be incorrect. Again, consumer advocates point to the apparent breadth of the language and need for consumer protections to argue for a broad application of this language.[88] However, other groups have argued that the term furnish requires an "affirmative undertaking to provide information."[89] If data is collected from a financial institution via screen scraping, that financial institution arguably does not "furnish" the data to the aggregator. On a more hotly contested point, some financial institutions argue that providing an API is a passive activity that does not constitute furnishing. An API is merely a piece of software that allows external systems to interact with a group's software in clearly defined ways. It defines calls and requests that external users can make to a company's systems and may be available on an open or permissioned basis. Under such a system, the data recipient simply inputs a command which is automatically fulfilled by the data source. In the case of public APIs, a consumer reporting agency may draw data from a source without directly contacting employees. Whether or not this constitutes "furnishing" will also significantly impact the scope of the FCRA going forward.

- Are data aggregators consumer reporting agencies under FCRA?
- Is a financial institution a data furnisher if it provides an API through which aggregators access data?

Electronic Funds Transfer Act ("EFTA")

Screen-scraping has created a string of liability disputes between financial services companies and new Fintech startups. Data aggregators and downstream Fintech applications may both store consumer account credentials in order to gather consumer financial data absent an API. If those providers experience a data breach, the hackers may then use those credentials to log into the impacted consumer's financial accounts and conduct fraudulent transactions.[90] There is an ongoing legal dispute regarding whether the EFTA and Reg E obligate the financial institution, the Fintech, or neither, as responsible to repay the consumer for the unauthorized transaction under these circumstances.

[85] *See* Finicity, *Consumer Reporting Agency*, accessible at https://www.finicity.com/consumer-reporting-agency/.

[86] *See* NCLC Symposium Statement, *supra* note 10, at 8.

[87] Reg V, *supra* note 71, at § 1022.41(c).

[88] *See* NCLC Symposium Statement, *supra* note 10, at 8.

[89] Kwamina Williford and Brian Goodrich, Why Data Sources Aren't Furnishers Under Credit Report Regs, HK Law (blog post Sep. 25, 2019), available at https://www.hklaw.com/-/media/files/insights/publications/2019/09/whydatasourcesarentfurnishersundercreditreportregs.pdf?la=en.

[90] Treasury Fintech Report, *supra* note 8, at 35-6.

Banks strongly maintain that they are not liable under Reg E for any losses that result in this manner.[91] Under Reg E, an "unauthorized transfer" does not include transactions performed by a person furnished with an "access device" by the consumer.[92] Under the banks' reading, a consumer furnishes an access device to a data aggregator when they provide them with account credentials and thus the transaction is not an unauthorized transaction at all.[93] Banks thus have no liability and if a data aggregator is unable or unwilling to compensate the consumer, the consumer suffers the loss.[94] Several banks have started including disclosures to this effect in their terms of service, partially as a method to dissuade their users from giving their credentials to Fintech applications.[95]

Consumer groups, on the other hand, strongly contest this argument. They argue that even if the account credentials constitute an access device, the consumer does not furnish it to the party that makes the transaction.[96] Even if the consumer furnishes this information to a data aggregator and that data aggregator then experiences a breach, one could not reasonably claim that the consumer furnished the access device to the hacker. They further argue that, as a policy matter, it's difficult to trace the origins of unauthorized charges and it will often be difficult to establish fault under these circumstances.

These arguments are compelling but, as a policy matter, there is also force to the banks' claim. It appears unfair to force them to share consumer account data with third parties, then be penalized if that data is breached if those same parties underinvest in security. Reducing the use of screen-scraping, increasing the data security obligations of Fintechs, or providing for some liability sharing could all help resolve this issue. The CFPB should clarify this ongoing legal dispute and provide policy guidance to ensure that all parties are properly incentivized to protect consumer financial data and that consumers have adequate means to seek relief if and when unauthorized transactions occur.[97]

- As a legal matter, do banks remain liable under the Reg E for unauthorized charges made in their systems that result from a consumer data breach at a Fintech company?
- As a policy matter, how should liability be apportioned between Fintechs and traditional financial institutions in such cases?
    - Should the two parties be jointly liable?
    - Should the apportionment depend on the respective fault of the parties?
    - If the Fintech alone should be liable, should the consumer still be able to bring a claim for reimbursement through their bank? Would the bank be liable to pay the claim in the first instance with a right to recover against the Fintech or should the bank not be forced to pay at all?

[91] *See, e.g.*, ABA RFI Response, *supra* note 11.

[92] Regulation E, 12 C.F.R. § 1005, available at https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/14/#14-b-Interp-1https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/14/#14-b-Interp-1.

[93] ABA RFI Response, *supra* note 11, at 9.

[94] *Id.*

[95] NCLC RFI Response, *supra* note 62.

[96] *Id.*

[97] *Id.*

Research Note on Financial Data Protection and Consumer Privacy in the United States
(Optional Reading)

Prepared by Nafisa Adama, HLS LLM 2020

June 3, 2020

The United States (U.S.) does not have a single overarching data protection law. Instead, separate sector-specific data protection laws have been enacted to regulate the use of data and consumer information in limited contexts. This memorandum provides background to the primary data protection laws applicable in the U.S. financial services industry and draws a distinction with comparable legislation in other jurisdictions, such as the General Data Protection Regulation (GDPR) in the European Union and the European Economic Area. It also discusses the key features of the recently enacted California Consumer Protection Act and the ensuing deliberations on the adequacy of the existing U.S. financial data protection and consumer privacy legal framework.

THE GRAMM-LEACH-BLILEY ACT

At the federal statutory level, the main legislation that protects consumers' personal financial data, albeit in a limited fashion, is the Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, enacted in 1999. A crucial aspect of the GLBA is the Title V which makes provisions for financial privacy protection. The safeguards provided under the GLBA can be broken down into the following:

a. Safe storage and sharing of consumer confidential information with affiliated third parties;
b. Provision of privacy notices to consumers; and
c. Securing consumer confidential information from unauthorized third-party access.

The GLBA imposes several obligations on financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—regarding the handling or storing of what it terms "consumer nonpublic personal information."[98] This subjects all information personal to the consumer such as their names, home addresses, social security numbers, or any additional information that a financial institution requires to provide financial services or sell a product to the data sharing restrictions of the GLBA. The GLBA places limited obligations on affiliated third parties that have received nonpublic personal information from GLBA regulated financial institutions. In the absence of an applicable exception, financial institutions are prohibited from sharing nonpublic personal information with non-affiliated parties unless consumers are first issued a notice containing the privacy policy of the financial institution with an opportunity to "opt-out."[99] The notice is issued only when an individual first becomes a customer of the bank and then annually thereafter. Each opt-out notice to a consumer must

[98] A "consumer" under the GLBA is an "individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes" or "the legal representative of such an individual." 15 U.S.C. § 6809(9). 70. "Nonpublic personal information" is defined as "personally identifiable financial information — provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution."

[99] § 6802; 12 C.F.R. § 1016.10(a).

be clear, conspicuous, and provide a reasonable means to exercise the opt-out right, such as through designated check boxes or providing a toll-free telephone number that consumers may call to opt-out.[100] Even though the GLBA specifies the type of information to be contained in the privacy notices,[101] the exact language of the notice is left to be determined by the financial institution thereby giving them some leeway to decide on the complexity and transparency of language in a manner that best serves their interests. It is no wonder why most privacy policies are considered convoluted, technical, and difficult to understand, further diminishing the power of the consumer to effectively control how their information is shared. Notably, the GLBA takes away from the consumer the power to control the sharing of their information among affiliate companies of the financial institutions. As such, the opt-out right is inapplicable in affiliate information sharing scenarios and this presents the risk of information being collected by an indeterminable number of affiliated companies who may even be non-financial institutions.

Even though the opt-out strategy gives the consumer the opportunity to permit or object to the sharing of their information with unauthorized parties, financial institutions will not be bound by the requirements for notification and the consumer's exercise of opt-out rights where they disclose nonpublic personal information:

a. to nonaffiliated third-party service providers, such as promoters of the financial institution's own products, provided that such nonaffiliated third parties are contractually bound to maintain the confidentiality of the consumer's information.[102]
b. to service or process transactions requested by the consumer.[103]
c. (i) to protect the confidentiality or security of their records on the consumer, service, product, or transaction; (ii) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; (iii) for required institutional risk control or for resolving consumer disputes or inquiries; (iv) to persons holding a legal or beneficial interest relating to the consumer; or (v) to persons acting in a fiduciary or representative capacity on behalf of the consumer.[104]
d. to provide information to applicable rating agencies, the institution's attorney's accountants, auditors, and other organizations assessing the financial institution's compliance with industry standards.[105]
e. to law enforcement agencies, self-regulatory organizations, or in connection with an investigation on a matter of public safety.[106]
f. to a consumer reporting agency in accordance with the Fair Credit Reporting Act (FCRA) or from a consumer report by a consumer reporting agency.[107]

[100] 12 C.F.R. § 1016.7(a)).

[101] The notices must include, among other things, the categories of information collected and disclosed, the categories of third parties with which the financial institution shares information, and policies and practices with respect to protecting the confidentiality and security of the information. *Id. § 1016.6(a)).*

[102] 15 U.S.C. § 6802(b)(2); 12 C.F.R. § 1016.13.

[103] 15 U.S.C. § 6802(e); 12 C.F.R. § 1016.14.

[104] 15 U.S.C. § 6802(e)(3)(A); 12 C.F.R. § 1016.15(a)(2)).

[105] 15 U.S.C. § 6802(4); 12 C.F.R. § 1016.15(a)(3)).

[106] 15 U.S.C. § 6802(5); 12 C.F.R. § 1016.15(a)(4)).

[107] 15 U.S.C. § 6802(6)(A) - (B); 12 C.F.R. § 1016.15(a)(5)(i)-(ii)).

g. in connection with the sale, transfer, or merger of all or a portion of the institution's business or operating unit, where the disclosure relates solely to the nonpublic personal information of consumers of that business or unit.[108]
h. to comply with all legal requirements including federal state and local laws, subpoenas, summons, judicial processes or government regulatory authorities having jurisdiction over them.[109]

Part of the enforcement framework of the GLBA is the Safeguards Rule[110] issued by the Federal Trade Commission (FTC). Together, the GLBA and the Safeguards Rule require all financial institutions under FTC jurisdiction to ensure the security and confidentiality of customers'[111] (as opposed to consumers as with the disclosure requirements) information. In implementing this provision, the law requires that the financial institutions put in place "administrative, technical, and physical safeguards" to secure the customers' information against "any anticipated threats or hazards" or "unauthorized access" to such information.[112] In this regard, the law anticipates the development and implementation of an "information security program" that contains safeguards that are suitable to the "size and complexity, the nature and scope" of the company's activities as well as the "sensitivity of the customer information".[113] Finally, the companies must, in maintaining the information security system, among other things, designate an information security program coordinator, put in place a risk assessment process, and regularly monitor the effectiveness of the safeguards procedure.[114] Regulatory authorities such as the Securities and Exchange Commission as well as the federal banking agencies impose other supervisory standards with respect to cybersecurity safeguards at regulated firms, which provides additional protections for consumer data.[115]

THE CALIFORNIA CONSUMER PRIVACY ACT

Effective January 2020, the California Consumer Privacy Act (CCPA), compared to title V of the GLBA, provides a much more extensive and comprehensive framework for the protection of consumer's personal information, despite being state law. The CCPA does not restrict its application to any industry in particular but rather applies to all companies that collect the personal information of Californians – provided the company is a for-profit, carries on business activities in California, and qualifies as a CCPA covered business., e.g., any company with more than $25 million in annual gross revenues, or that engages in the buying, selling, or receipt of the personal information of 50,000 or more California residents, or that

[108] 15 U.S.C. § 6802(7); 12 C.F.R. § 1016.15(a)(6)).

[109] 15 U.S.C. § 6802(8); 12 C.F.R. § 1016.15(a)(7)).

[110] *See*, e.g., Financial Institutions and Customer Information: Complying with the Safeguards Rule, Federal Trade Commission (Apr. 2006), Available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[111] Customer is defined as someone who has a continuing relationship with the financial institution, such as someone who has obtained a loan or who has opened a credit or investment account. 16 C.F.R. § 313.3(h)–(i); see also 12 C.F.R. § 1016.3 (i)–(j)).

[112] 15 U.S.C. § 6801(a) – (b)).

[113] 16 C.F.R. § 314.3.

[114]; 16 C.F.R. § 314.4.

[115] *See* Brian Neil Hoffman, Romaine Marshall And Matt Sorensen, Federal and State Cybersecurity Regulation of Financial Services Firms, Law Journal Newsletters, June 2017, Available at http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/06/01/federal-and-state-cybersecurity-regulation-of-financial-services-firms/.http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/06/01/federal-and-state-cybersecurity-regulation-of-financial-services-firms/. *Also see* Cybersecurity regulation and best practice in the U.S. and UK, Lexis Nexis, Available at https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practicehttps://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice.

derives more than 50% of its annual revenues from the sale of California residents' personal information.[116] Accordingly, the CCPA may be enforced against all companies (including affiliates and subsidiaries) that fit these criteria, irrespective of the industry or location. It has been suggested that these thresholds have been set in such a way that it is easily fulfilled by even small to medium businesses, who merely collect personal data (IP addresses, cookie IDs, etc.) through a website accessible by California residents.[117] It is instructive to note that even though the CCPA provides a partial carve-out for financial institutions concerning information collected pursuant to the GLBA,[118] financial institutions whose activities go beyond the scope of the GLBA and fit within the business threshold will still need to comply with the provisions of the CCPA as it relates to data collection activities not governed by the GLBA.[119] Therefore, all personal information not covered by the GLBA and collected by financial institutions that qualify as a business will now be subject to the CCPA. This is also enabled by the fact that the GLBA does not exempt regulated entities from complying with data and privacy issues not covered under the GLBA.[120]

The CCPA defines "personal information" just as broadly as it defines businesses. Unlike the GLBA, which implies specific personal identifiers, the CCPA broadly construes personal information to include, with the exception of publicly available information[121] and "de-identified" or "aggregate consumer information,"[122] all information of California residents that "identifies, relates to, describes, or is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household".[123] This applies regardless of how the collection is done or the type of industry in which the business operates. In fact, the CCPA illustrates further that personal information can include "electronic network activity such as browsing or search history, and information regarding a consumer's interaction with an internet website, application, or advertisement" and "inferences drawn from any of" this information.[124]

The CCPA regime affords California consumers three primary "rights" with respect to the disclosure of their personal information. The rights include the "right to know", the "right to opt-out" similar to the GLBA, and the "right to delete or be forgotten".

a. The Right to Know/Disclosure of Personal Information

As the name implies, the California based consumer has the right to know all information collected, stored, and/or shared about them. Accordingly, the CCPA requires that a business must, in advance

[116] CAL CIV. CODE § 1798.140(c)(1)).

[117] *See,* Christopher A. Ott, Q&A: Privacy and Security Partner Christopher Ott on the California Consumer Privacy Act of 2018, Davis Wright Tremaine LLP Privacy & Security Law Blog, August 6, 2018, Available at https://www.dwt.com/blogs/privacy--security-law-blog/2018/08/qa-privacy-and-security-partner-christopher-ott-on.

[118] CAL CIV. CODE § 1798.145(e)).

[119] *See,* Mathews, Fleisher & Foester, Financial Institutions and the CCPA: What Remains After the Law's Exceptions, Bloomberg Law, Available at https://media2.mofo.com/documents/191025-financial-institutions-ccpa.pdf.

[120] 15 U.S.C. § 6807.

[121] CAL CIV. CODE § 1798.140(o)(2)).

[122] *Id. Also see,* CAL CIV. CODE § 1798.145(a)(5)).

[123] CAL CIV. CODE § 1798.140(O)(1)).

[124] *Id.* § 1798.140(O)(1)(A)–(K)).

of collecting a consumer's personal information, inform the consumer (via mail or electronically) the categories of personal information to be collected and purposes for which such information will be used.[125] This is similar to the privacy notice under the GLBA regime, except the latter does not burden financial institutions with the responsibility of disclosing the specific usages for collected information. This presumably gives the CCPA an edge over the GLBA, especially in terms of transparency of privacy policies. Predictably, GLBA regulated financial institutions will need to change their privacy policies and data protection mechanisms in order to fulfill the more stringent compliance requirements of the CCPA.

b. The Right to Opt-Out of Sale of Personal Information

Under the CCPA, the consumer shall have the power to restrict the sale of their information by expressly exercising the right to opt out of such sale by the business. In this regard, the CCPA mandates the business to inform consumers of their right to opt-out, after which the business shall be barred from selling such consumer's information until such a time when the consumer provides express authorization for sale.[126] This provision of the CCPA supplements the GLBA, as it allows the consumer to retroactively direct the business on the sale of its information or otherwise and, in this regard, the law requires the business to act promptly. This strengthens the consumer's ability to retain control over the use of their information to a considerable extent.

c. Right to Request Deletion of Personal Information

Lastly, under the CCPA, the consumer enjoys the right to have previously collected information deleted or forgotten by the business and the latter must, at the time of collection, disclose this right to the consumer.[127] Once a consumer makes such a request, the business and its service providers are obligated to proceed and delete such information. The GLBA does not accord the consumer the right to request the deletion of their information. Any opt-out directives or request to delete the information by the consumer will not be complied with when the disclosure of the information is necessary to detect illegal activity, to comply with legal obligations, or to perform contracts between the business and the consumer. This is reflective of the exceptions under the GLBA where financial institutions may disclose consumer information without prior authorization. Also worthy of note is the fact that the CCPA makes provision for additional anti-discrimination safeguards of consumers' data which goes beyond the scope of the GLBA. Accordingly, businesses handling consumer data shall not discriminate against consumers based on rights exercised within the confines of the CCPA.[128] Therefore, all consumers of CCPA covered businesses must be treated fairly in a manner that does not indict the good-faith practices of the businesses.[129]

[125] CAL CIV. CODE § 1798.100.

[126] CAL CIV. CODE § 1798.120.

[127] CAL CIV. CODE § 1798.105.

[128] CAL CIV. CODE § 1798.125.

[129] *See,* Cynthia J. Larose, Analysis of Modified Attorney General Regulations to CCPA – Part 5: Discriminatory Practices and Financial Incentives, February 21, 2020, Available at https://www.natlawreview.com/article/analysis-modified-attorney-general-regulations-to-ccpa-part-5-discriminatory.

The CCPA is enforced by the Attorney General of California who also has the power to impose non-compliance fines. In addition, and unlike the GLBA, the CCPA provides consumers with a private right of action concerning data breaches such as unauthorized access, theft, and/or disclosure of certain types of personal information including the right to seek statutory damages.[130] Although the CCPA goes well beyond the requirements of the GLBA, the GLBA, as amended, explicitly provides that states may provide greater privacy protections.[131]

Since the passage of CCPA, some analysts have questioned whether a federal privacy law should be enacted and include new preemption provisions with respect to state privacy.[132] Calls have been made in Congress and both Republicans and Democrats have explored a comprehensive federal data privacy law that would not only serve as a national-wide privacy law in the U.S., but also would preempt to a considerable extent the application of inconsistent provisions of state privacy laws. These efforts have, however, remained stalled as there is a divergence of opinion with respect to state preemption, amongst other issues. On the one hand, it is argued that without the preemption of state laws, businesses and consumers will suffer due to the patchwork of regulations with which they will need to comply. On the other hand, there are those who believe that federal legislation should do no more than lay the foundation for states to build on as preemption will stifle state innovation in this area.[133] The California Attorney General, Xavier Becerra, has specifically argued that a federal law should not undermine state protections urging that Congress "favor legislation that sets a federal privacy–protection floor rather than a ceiling" so as to allow states provide protections tailored to their residents.[134] The debate over federal preemption in this area remains unresolved.[135]

THE EUROPEAN GENERAL DATA PROTECTION REGULATION (GDPR)

The CCPA is arguably the U.S. version of the GDPR, because of their similarities in terms of their broad scope of application. Just like the GLBA and the CCPA, the purpose of the GDPR is to regulate how personal data is processed by regulating those persons that collect and process that data, while ensuring that it

[130] Cal. Civ. Code § 1798.150(a) (as amended by Assembly Bill 1355 effective October 11, 2019)).

[131] *See* 15 U.S.C. § 6807:

(a) In general: This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency.

(b) Greater protection under State law: For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter, as determined by the Bureau of Consumer Financial Protection, after consultation with the agency or authority with jurisdiction under section 6805(a) of this title of either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party.

[132] The GLBA preempts provisions of state statute, regulation, order or interpretation that areinconsistentare inconsistent with its provisions and such preemption is only to the extent of the inconsistency. State statutes, regulations, orders or interpretations will not be considered inconsistent if they provide greater consumer privacy protection as compared to the GLBA. Therefore, the GLBA does not preempt the enforcement of the CCPA for providing stricter consumer privacy safeguards.

[133] *See* Robert E. Slavkin, Is A Federal Privacy Law In the Cards for 2020?, December 12, 2019, Available at https://www.healthlawrx.com/2019/12/is-a-federal-privacy-law-in-the-cards-for-2020/.

[134] *See* Sara Merken, California Attorney General Asks Congress to Shield Privacy Laws, Bloomberg Law, February 25, 2020, Available at https://news.bloomberglaw.com/privacy-and-data-security/california-attorney-general-asks-congress-to-shield-privacy-laws.

[135] *See* Alysa Zeltzer Hutnik, Michael Lynch, Paul A. Rosenthal & Jewel Tewiah, Potential Constitutional Challenges to the CCPA, AD Law Access, December 12, 2019, Available at https://www.adlawaccess.com/2019/12/articles/potential-constitutional-challenges-to-the-ccpa/.

moves freely throughout the E.U..[136] Any personal data or information relating to an identified or identifiable person such as their name, address, employment history, income, IP address, etc., subject to any applicable exception,[137] cannot be collected, recorded, organized, structured, stored, used, transferred, adapted, altered, or otherwise processed unless such processing is in compliance with the GDPR.[138] The CCPA's conceptualization of personal information is slightly broader as it considers information traceable, directly or indirectly, to a household and not just an individual. The GDPR categorizes holders of personal data into the controller and processor such that a controller determines the purposes and means of processing personal data,[139] and a processor is responsible for processing data on behalf of a controller.[140] Similar to the CCPA, the GDPR is extraterritorial in its application and offers a comprehensive data protection framework that applies throughout the European Union and in other jurisdictions that process personal data of persons resident in the E.U..[141] Therefore, U.S. companies, acting as either controllers or processors, that have an "establishment"[142] in the E.U. and/or (a) process personal data in the E.U.; (b) are established outside the E.U., but are offering goods and services in the E.U.; or (c) monitor behavior of individuals in the E.U. will be required to comply with the data protection requirements of the GDPR.

The key rights provisions of data subjects under the GDPR can be summarized under six headings, some of which are also provided for under both the CCPA and the GLBA. These are as follows:

a) Right to be informed

Individuals have a right to be informed about the collection and use of their personal data[143] and controllers have a corresponding right to provide them with privacy notices clearly stating the purposes for processing, retention periods, and with whom the data will be shared.[144] This transparency is also seen with the CCPA.

b) Right of access

Individuals have the right to access and obtain copies of their personal data and controllers must respond to a request for access within one month.[145] This provides certainty of obligation to the controllers and manages the expectations of the data subject.

c) Right to rectification

[136] GDPR, Art. 1.

[137] The GDPR does not apply to the processing of personal data: (1) in the course of an activity that "falls outside the scope of E.U. law"; (2) by E.U. nations carrying out certain -E.U.-wide foreign policy and national security objectives; (3) by an individual in the course of a purely personal or household activity; and (4) by competent authorities conducting criminal investigations and prosecutions, including safeguarding against preventing threats to public security - GDPR Art. 2(2).

[138] GDPR Art. 4(2)).

[139] *Id.* Art 4(7)).

[140] *Id.* Art 4(2)).

[141] GDPR, Art. 3.

[142] The GDPR does not define "establishment," but states that it "implies the effective and real exercise of activity through stable arrangements." – GDPR recital 22.

[143] GDPR Art 12 – 14.

[144] *Id.*

[145] *Id.* Arts. 12(3), 15.

Individuals have the right to require personal data controllers to correct inaccurate information or complete incomplete data.[146]

d) Right to erasure (also known as the "right to be forgotten")

This provision is largely similar to the consumer's right to have their personal information deleted under the CCPA, save that the CCPA broadly guarantees this right subject to the applicability of certain exceptions. Under the GDPR, controllers are only obliged to comply with an erasure request without undue delay when, among others: (1) the data is no longer necessary for the purposes for which it was collected; (2) the controller relied on consent as its legal basis for processing and such consent has subsequently been withdrawn; or (3) the controller relied on the "legitimate interests"[147] basis for processing, the individual objected to processing, and there was no overriding legitimate interest.[148] In the absence of an applicable exception, the individual's right to be forgotten also applies when: (1) the controller is processing personal data for direct marketing purposes and the individual objects to the processing; (2) the data was processed unlawfully; (3) E.U. law or the law of an E.U. member nation requires the data to be erased; or (4) the data was collected in connection with the offering of internet services to a child.

e) Right to restrict processing

Individuals may exercise the right to restrict data processing in certain circumstances, within a limited period of time. In this regard, the right to restrict the data processing activities of the controller will apply when: (1) the accuracy of personal data is contested and the controller is in the process of verifying whether the data is accurate; (2) the processing is unlawful, but the data subject prefers restriction instead of erasure; (3) the controller no longer needs the personal data, but the data subject requires the data to be maintained in relation to its legal claims; or (4) the controller is considering whether the data subject's objection to processing overrides the legitimate interests in the processing while the controller evaluates a broader objection to its data processing activities.[149]

f) Right to data portability

This right allows data subjects to obtain their personal data that they provided to a controller in a commonly used, automated form that can be transmitted to another controller without affecting the data's usability.[150] This allows data to be transferred between controllers irrespective of the controller that originally collected or compiled the data. The portability of such data shall be based on the express consent of the data subject, or in fulfillment of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.[151]

[146] *Id.* Art 16.

[147] Legitimate interests for data processing include, among other things, processing for direct marketing purposes, transmission within a group of affiliated entities for internal administrative purposes, ensuring network and information security, and reporting of possible criminal acts or threats to public security. GDPR, recitals 47–50.

[148] *Id*. Art. 17.

[149] *Id.* Art. 18(1).

[150] GDPR Art. 20(1)(a) – (b)).

[151] *Id.*

The rights conferred by the GDPR and the CCPA, particularly the rights to data portability and the right to request the deletion of information, respectively constitute some of the most prominent distinguishing features from the standard protections provided under the GLBA. Financial institutions have had to grapple with making the necessary infrastructural adjustments to their data collection and preservation practices[152] to ensure maximum compliance with the requirements of all three legislations. No matter the data security measures employed, the nature and scope of its security must be appropriate to the severity of the risks of infringement on individual rights if data security were to be violated.[153] This is particularly important given the rise of new industry players, such as Fintech firms and data aggregators, whose business activities are wholly automated with attendant risks of cyber intrusions and data theft, which may sometimes go undetected due to under regulation.

Although both the CCPA and the GDPR have the extra-territorial effect, the GDPR appears to have farther applicability as its data protection provisions extend to protect the personal data of consumers temporarily in the E.U.. In reality, many financial institutions in the U.S. are able to comply with both the CCPA and the GDPR due to the scope and size of their operations transcending geographical boundaries. E-commerce businesses, firms providing Fintech solutions such as Apple Pay, PayPal etc., also carry similar burdens to ensure compliance with the CCPA, GDPR, and the GLBA because of the large amount of personal data processed as part of their routine business activities.

Who truly owns/controls consumer financial data and how should it be used?

The GLBA makes an effort to protect consumer financial data by giving them the power to control how their financial information is collected and shared with third parties. However, the broad list of excepted circumstances where financial institutions may act without notifying or obtaining the consumer's consent demonstrates in practical terms that consumers do not have real control over their financial data and any resulting third party disclosures or onward transfers. A recent report by the Federal Reserve of San Francisco (SF Fed) advocates for the reframing of the construct of consumer 'data ownership' to a more realistic notion of consumers having 'active data rights '.[154] The argument here is that this shift does not diminish the proprietary relationship between consumers and their data but rather "provides a broader framing that…acknowledges the inherent complexity of data as an intangible resource that is shared between individuals, businesses and the broader society."[155] This is understandable as, today's interconnected data economy makes it increasingly difficult for consumers to track who has access to their data and how it is being used. Therefore, consumers are limited in their capacity to actively take steps to protect collected data in the traditional sense of exercising ownership. This issue is further aggravated in instances where consumers authorize financial institutions to share their data with named third parties. Such authorized data sharing arrangements provide very limited means for the consumer to determine with certainty how often their data are being accessed, how long their data are being retained,

[152] *See* Lauren Davis, *The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation*, 24 N.C. BANKING INST. 499 (2020), Available at https://scholarship.law.unc.edu/ncbi/vol24/iss1/22.

[153] GDPR Art 32(1)).

[154] Kaitlin Asrow, The Role of Individuals in the Data Ecosystem: Current debates and considerations for data protection and date rights in the United States, Fintech Edge Special Report, Federal Reserve Bank of San Francisco (June 3, 2020), Available at https://www.frbsf.org/banking/files/The-Role-of-Individuals-in-the-Data-Ecosystem-Full-Report.pdf, Pages 17 – 22;

[155] *Id.* page 18

with whom their data are being shared, and the risks associated with sharing their data and account credentials.[156]

It is also difficult to ensure that such third party's access is limited to the express purpose for which the consumer authorized access to their data. Discussions around the attendant privacy risks stemming from such authorized access have been on the rise owing to the proliferation of the financial market by new industry players, such as Fintech startups. They can access consumer information from financial institutions based on consents obtained from consumers directly or through alternative means, including the consumer's use of services provided by Fintech applications to track spending, set monthly budgets, apply for loans, or manage investments. Financial institutions and consumer privacy advocates are particularly concerned that the ease of portability of such sensitive data to largely unregulated industry actors will not only pose privacy risks for the consumers but also expose their data system safeguards to risks of cybersecurity breaches that could ultimately lead to unintended and unauthorized access to consumer's financial data. In essence, stakeholders are concerned about how informed consumers really are when providing such authorized access and whether financial institutions should out rightly honor them or exercise some discretion.

The CFPB attempted to address some of these issues and also assuage concerns around data security in its non-binding Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation, without creating new rules. The principles deal with the pressing issues of informed consumer consent, data scope, and usability, noting that third parties' authorized to access consumer's financial information should ensure that the authorization obtained addresses access frequency, data scope, and retention period so as to limit the third parties' access to the extent of the consent provided. Essentially, third parties with authorized access should only access the data necessary to provide the specific services for which access was granted and only maintain such data for as long as it is necessary.[157] Notwithstanding, these issues remain contentious and campaigns for a more substantive regulation on the matter persist.[158]

Should the U.S. Implement a Federal GDPR-styled privacy law?

Another question that has arisen since the coming into effect of the CCPA is whether the U.S. should adopt an overarching data protection and privacy law as opposed to leaving the field open for states to create their respective privacy laws. The wide reach and stringent conditions of the CCPA raise concerns about other states following suit. The federal government's approach to privacy and data protection has been industry-focused with its provisions limited to specific industry participants and certain types of data leading to duplicity of regulations and in some instances, contradictions. Consequently, financial institutions in the U.S. have the burden of complying with both the CCPA and the GLBA, while adjusting their procedures to ensure full compliance in circumstances where the laws diverge. This fragmented

[156] *See* Michael S. Barr, Abigail Dehart and Andrew Kang, Consumer Autonomy & Pathways to Portability in Banking and Financial Services, Centre of Finance and Policy, University of Michigan, Available at https://www.cio.com/article/3379036/the-united-states-needs-a-federal-privacy-law.html, Page 8.

[157] CFPB, Consumer Protection Principles: Consumer Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017), http://files.consumerfinance.gov/f/documents/cfpb_cons umer-protection-principles_data-aggregation.pdf.

[158] Brian Knight, *Statement Regarding CFPB Dodd-Frank Section 1033 Symposium* (Feb. 26, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf.

regulatory framework places undue burdens on business as they strive to avoid penalties for breaches or non-compliance.

Stakeholders in the financial industry have canvassed for Congress to consider creating protections in a federal law similar in spirit to the GDPR (and the CCPA) as it puts consumers in charge of their personal data.[159] Accordingly, several Senate Committee hearings to examine proposals for an overarching consumer privacy legislation have been held over the last 18 months. Participants at these hearings, which range from internet service providers to consumer privacy organizations, have made proposals to the Senate for a comprehensive federal privacy legislation highlighting the benefits that would come from such a law especially in today's highly digitally integrated world. Should Congress consider a comprehensive national data protection law, its legislative proposals would involve numerous legal considerations including, amongst others, the scope of application and nature of the information to be protected, enforcement agency/authority, issues of statutory overlap, and preemption of state laws.

[159] America Should Borrow from Europe's Data-Privacy Law, The Economist, April 5, 2018, Available at https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

Appendices

APPENDIX I - CFPB MEMO

1. U.S. Dep't of Treasury, *A Financial System that Creates Economic Opportunity: Nonbank Financials, Fintech, and Innovation* 22-44 (2018) (hereinafter "Treasury Fintech Report"), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

2. Michael Barr et al, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, University of Michigan Center on Finance, Law and Policy 1-2 (November 3, 2019), available at http://financelawpolicy.umich.edu/files/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

3. Plaid Technologies, *Plaid response to CFPB regarding Consumer Access to Financial Records Docket No. CFPB-2016-0048* (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0058.

DODD FRANK S. 1033

General

4. 12 U.S.C. §5533 (2010) (Dodd Frank Act, Title X generally and Section 1033 specifically), accessible at https://legcounsel.house.gov/Comps/Dodd-Frank%20Wall%20Street%20Reform%20and%20Consumer%20Protection%20Act.pdf.

5. CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

6. CFPB, *Stakeholder Insights that Inform the Consumer Protection Principles* (October 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

Issue 1

7. Brian Knight, *Statement Regarding CFPB Dodd-Frank Section 1033 Symposium* 3-5 (Feb. 26, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_knight-statement_symposium-consumer-access-financial-records.pdf.

8. American Bankers Association, *Request for Information Regarding Consumer Access to Financial Records Docket No.: CFPB-2016-0048, 13*-14 (Feb. 21, 2017) available at https://www.regulations.gov/document?D=CFPB-2016-0048-0041.

9. Plaid Technologies, *Written Statement for the Symposium on Consumer Access to Financial Records* (Feb. 19, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf.

Issue 2

10. National Consumer Law Center (on behalf of its low income clients), *Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act* (Feb. 12, 2020), accessible at https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf.

11. Alessandro Acquisti and Jens Grossklags, *Privacy and Rationality in Decision Making*, 3(1) IEEE, Security and Privacy Magazine 26-33 (Jan. 2005), accessible at https://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.

12. Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harvard Law Review 1880 (2013), accessible at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018.

Issue 3

13. ABA RFI Response, see appendix 8.

14. Kate Rooney, *PNC's fight with Venmo highlights bigger issue over who owns your banking data,* CNBC (Dec. 16, 2019), available at https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html.

Issue 4

15. Article 29 Data Prot. Working Party, Guidelines on the Right to Data Portability, 16/EN WP242 at 10 (April 5, 2017) available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

16. National Consumer Law Center, *Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048*, 7 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0072.

17. Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay & Ignacio Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, COMPUTER L. & SECURITY REV. 193 (2018), accessible at https://www.sciencedirect.com/science/article/pii/S0267364917303333.

Issue 5

18. Treasury Fintech Report (see appendix 1)

19. Written Statement of Petal Card, Inc., Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act (Feb. 12, 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_gross-statement_symposium-consumer-access-financial-records.pdf.

20. Independent Community Bankers of America, *Docket No. CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records*, 6 (Feb. 21, 2017), accessible at https://www.regulations.gov/document?D=CFPB-2016-0048-0035.

21. Fidelity Investments, *Request for Information Regarding Consumer Access to Financial Records; Docket No. CFPB-2016-0048*, 6-8 (Feb. 21, 2017), available at https://www.regulations.gov/document?D=CFPB-2016-0048-0053.

FCRA

22. Regulation V, 12 C.F.R. § 1022 https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1022/1/.

23. Kwamina Williford and Brian Goodrich, *Why Data Sources Aren't Furnishers Under Credit Report Regs*, HK Law (blog post), available at https://www.hklaw.com/-/media/files/insights/publications/2019/09/whydatasourcesarentfurnishersundercreditreportregs.pdf?la=en.

24. NCLC Symposium Statement, 6-9 (see appendix 10)

25. Plaid RFI Response, 11-14 (see appendix 3).

26. Federal Trade Commission, *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations* 29, July 2011, https://www.ftc.gov/sites/default/files/documents/reports/40-years-experience-fair-credit-reporting- act-ftc-staff-report-summary-interpretations/110720fcrareport.pdf.

EFTA

27. Regulation E, 12 C.F.R. § 1005, available at https://www.consumerfinance.gov/policy-compliance/rulemaking/regulations/1005/14/#14-b-Interp-1.

28. NCLC RFI Response (see appendix 16)

29. ABA RFI Response (see appendix 8)

APPENDIX II - PRIVACY

1. Juliana De Groot, What is GLBA Compliance? Understanding the Data Protection Requirements of the Gramm-Leach-Biley Act in 2019, Digital Guardian's Blog (July 15, 2019) https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

2. Debevoise & Plimpton, The California Consumer Privacy Act: Compliance Strategies for Financial Institutions, Debevoise Update, (May 2, 2019) file:///C:/Users/User/Downloads/20190502_California_Consumer_Privacy_Act_.pdf

3. Juliana De Groot, What is the General Data Protection Regulations? Understanding and Complying with the GDPR Requirements in 2019, Digital Guardian's Blog (December 2, 2019) https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

4. Helen Goff Foster, Exempt or Not Exempt? California Consumer Privacy Act and the Gramm-Leach-Biley Act, Davis Wright Tremaine LLP, Privacy & Security Law Blog (April 15, 2019) https://www.dwt.com/blogs/privacy--security-law-blog/2019/04/exempt-or-not-exempt

5. Ropes & Gray, GDPR vs CCPA (2019) file:///C:/Users/User/Downloads/GDPR%20vs%20CCPA.pdf

6. Davis Wright Tremaine LLP, Q&A: Privacy and Security Partner Christopher Ott on the California Consumer Privacy Act of 2018, , Privacy & Security Law Blog, (August 6, 2018) https://www.dwt.com/blogs/privacy--security-law-blog/2018/08/qa-privacy-and-security-partner-christopher-ott-on

7. Mayer Brown LLP, Whose Data is it: CFPB Releases Consumer protection Principles for Consumer Authorized Financial Data Sharing and Aggregation (November 2, 2017) https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2017/11/whose-data-is-it-cfpb-releases-consumer-protection/files/updatecfpbprinciplesforfinancialdatasharingandaggr/fileattachment/updatecfpbprinciplesforfinancialdatasharingandaggr.pdf

8. Kaitlin Asrow, The Role of Individuals in the Data Ecosystem: Current debates and considerations for data protection and date rights in the United States, Fintech Edge Special Report, Federal Reserve Bank of San Francisco (June 3, 2020), https://www.frbsf.org/banking/files/The-Role-of-Individuals-in-the-Data-Ecosystem-Full-Report.pdf

9. Lauren Davis, The Impact of the California Consumer Privacy Act on Financial Institutions Across the Nation, 24 N.C. BANKING INST. 499 (2020), https://scholarship.law.unc.edu/ncbi/vol24/iss1/22

10. Kristen Mathews, Adam Fleisher, Morrison & Foester, Financial Institutions and the CCPA: What remains after the Law's Exceptions?, Bloomberg Law, (October 2019) https://media2.mofo.com/documents/191025-financial-institutions-ccpa.pdf

11. America should borrow from Europe's data-privacy law, The Economist, (April 5, 2018), https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law

12. David MacCabe, Congress & Trump Agreed they want a National Privacy Law. It is Nowhere in Sight, The New York Times, (October 2019) https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html

13. Fara Soubouti, Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection, 24 N.C. BANKING INST. 527 (2020) https://scholarship.law.unc.edu/ncbi/vol24/iss1/23

14. Information Technology & Innovation Foundation, Debate: Should the U.S. Copy the E.U.s New Privacy Law, (September 18, 2018), https://itif.org/events/2018/09/25/debate-should-us-copy-eu-privacy-law

15. Carl Schonander, The United States needs a federal privacy law, CIO, (March 22, 2019), https://www.cio.com/article/3379036/the-united-states-needs-a-federal-privacy-law.html

16. Derek Hawkins, The Cybersecurity 202: Why a privacy law like GDPR would be a tough sell in the U.S., The Washington Post, May 25, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/

17. Council on Foreign Relations, Reforming the U.S. Approach to Data Protection and Privacy, January 30, 2018, https://www.cfr.org/report/reforming-us-approach-data-protection