Capital One Financial Corporation
1680 Capital One Drive
McLean, Virginia 22102

February 18, 2020

Consumer Financial Protection Bureau
1700 G. Street, NW
Washington, DC 20552

Via Electronic Delivery

Re: Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act

Capital One Financial Corporation ("Capital One")[1] appreciates the opportunity to provide a written statement with respect to policy making by the Consumer Financial Protection Bureau ("CFPB") regarding Dodd-Frank Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") Section 1033 and ongoing data aggregation-related market monitoring.

Overview

New technology has enabled the rapid proliferation of non-bank financial technology ("fintech") companies. Much of the U.S. population feels comfortable conducting business online with an entity with which it has little or no prior experience and that does not have any physically accessible locations. Recently, however, the growth of data aggregation services has accelerated the distribution and duplication of consumer financial data, and the risks posed by consumer financial data aggregation services have increased in parallel.

Capital One commends the CFPB for taking its first steps to address this market in the 2017 "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." Capital One participated in the November 2016 Request for Information

[1] Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N.A., had $262.7 billion in deposits and $390.4 billion in total assets as of December 31, 2019. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has branches located primarily in New York, Louisiana, Texas, Maryland, Virginia, New Jersey and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

process that helped inform the creation of the principles.[2] While industry actors have been actively working to move data sharing practices forward, a number of the issues that were characterized by the CFPB's principles remain works-in-progress and, as detailed below, there are areas for improvement.

Effective disclosure and consumer awareness are lacking in the consumer financial data services market, as consumers are often not made fully aware of the costs, benefits, and risks of using consumer financial data aggregator services. For aggregators to provide data services to fintechs, to date, most data aggregators continue to require consumers to divulge their online bank account credentials (usernames and passwords). By disclosing their credentials, consumers are inadvertently subjecting themselves to security and financial risks. Consumers likely do not understand that the credentials they provide to a fintech will be provided to, used, and maintained indefinitely by a third party – the fintech's data aggregator. Data aggregators obtain the consumer's financial data by acting as the consumer to enter the consumer's secure online financial account environment.

Consumers may not be aware that data aggregators will copy and store their data, may use the data for other purposes, or will create new products and services using the consumer's data.[3] Similarly, consumers may not be aware that data aggregators collect and transfer as much information as can be obtained, in many cases well beyond the data actually necessary for the consumer to use the new financial product or service. For instance, in the case of screen scraping, a data aggregator has access to and may collect more information than authorized if the consumer credentials provide the data aggregator with access to multiple financial accounts, as is typically the case with multi-relationship customers of a financial institution. Moreover, an aggregator, fintech, or bad actor that obtains a consumer's credentials from an aggregator or fintech has the capacity to take any action as a consumer using the financial institution's website, including initiating electronic funds transfers and account changes.

Consumers have grown to trust that regulated financial institutions are subject to a legal, regulatory, and supervisory regime that requires the safeguarding of consumer financial data. Among numerous other regulatory requirements, financial institutions are subject to periodic examinations for cybersecurity, third party risk management, and consumer protection issues. If a data breach were to occur at a financial institution, the financial institution is expected to notify their federal regulator on a timely basis. Consumers are generally not aware of the differences in the legal and supervisory standards and practices of other participants in the marketplace, and that their financial data may not be subject to the same legal protections when it is removed from the banking system and held by a non-bank aggregator or fintech. Indeed, consumers may incorrectly assume that the fintech with which they are interacting is part of the banking system and is subject to the same standards of practice and information security as a bank. These risks can be further

[2] Capital One requests that its February 21, 2017 letter, enclosed with this written statement, also be entered to the record of this Symposium.

[3] For instance, some data aggregators are marketing identity management products.

exacerbated if downstream fintech clients of data aggregators ("fourth parties") also fail to provide sufficient protections for consumer financial data.

The CFPB has the authority - and a responsibility - to ensure that consumer financial data is subject to adequate safeguards *throughout its lifecycle*. Consumers expect to have a stable and consistent level of protection for their financial data, regardless of where the data originated, where it has been transferred, and the type of entity that is using or storing the data. As described further below, the CFPB can and should take steps to simultaneously enhance the legal protections afforded to consumer financial data and promote fintech innovation that increases competition and delivers consumer benefits.

Accordingly, Capital One respectfully recommends that:

- the CFPB prescribe disclosures that, pursuant to its authorities under Section 1032 of the Dodd Frank Act, ensure consumers' control over their data, adequately convey who has their data, and allow consumers to effectively manage how that data is used;

- the CFPB support secure methods for consumers to access their financial data that do not require consumers to share their account credentials with third parties, such as through application programming interface ("API") agreements between banks and data aggregators;

- the CFPB collaborate with its prudential counterparts and affirm that, notwithstanding the CFPB's Principles regarding Consumer-Authorized Financial Data Sharing and Aggregation, financial institutions should not depart from the FFIEC's guidance regarding multi-factor authentication;

- the CFPB exercise its authority under Dodd-Frank Act Section 1024(a)(1)(C) to provide notice of its intent to require reports and conduct supervisory examinations of specific data aggregators, given the risks they pose to consumers and the consumer financial services market; and

- that any such examination of data aggregators be accompanied by clear expectations from the CFPB regarding disclosure, consumer control, data security, and oversight relating to data aggregators' sharing consumer data with third parties, as well as any fourth parties that third parties may then share consumer data with.

The CFPB should prescribe disclosures that ensure consumers' control over their data, adequately convey who has their data, and allow consumers to effectively manage how that data is used.

In 2017, the Bureau articulated a vision in which "[c]onsumers are informed of, or can readily ascertain, which third parties that they have authorized are accessing or using information regarding the consumers' accounts or other consumer use of financial services." Further, the Bureau described an environment in which consumers were able to reasonably ascertain the "security of each such party, the data they access, their use of such data, and

the frequency at which they access the data" throughout the time that the data is accessed, used, or stored by any such party.[4] Beyond transparency, the Bureau envisioned actual consumer control and consent regarding how their data is used. This would include that "[c]onsumers understand data sharing revocation terms and can readily and simply revoke authorizations to access, use, or store data," among other protections.

Unfortunately, two years later, consumers continue to lack a sufficient understanding of aggregator and fintech data sharing practices and are not offered a meaningful opportunity to consent or object to the privacy and data sharing practices of these services. Moreover, the ability of consumers to understand rapidly evolving market practices is being outpaced by the proliferation of new actors, technologies, and techniques to monetize consumer financial data. The environment described by Federal Reserve Governor Lael Brainard in late 2017 continues to persist:

> It is often hard for the consumer to know what is actually happening under the hood of the financial app they are accessing. In most cases, the log in process does not do much to educate the consumer on the precise nature of the data relationship . . . . In reviewing many apps, it appears that the name of the data aggregator is frequently not disclosed in the fintech app's terms and conditions, and a consumer generally would not easily see what data is held by a data aggregator or how it is used. The apps, websites, and terms and conditions of fintech advisors and data aggregators often do not explain how frequently data aggregators will access a consumer's data or how long they will store that data.[5]

Indeed, in November 2019, The Clearing House published the results of a survey of nearly 4,000 U.S. banking customers.[6] The survey found that 80% of fintech app users were not fully aware that fintech apps or third parties may store their bank account username and password. Once they realize this, more than two-thirds of consumers (68%) were uncomfortable with the level of access they had shared. Similarly, less than a quarter of fintech app users knew that financial apps often continue to have ongoing access to their data until consumers revoke their bank account credentials.

---

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

[5] Lael Brainard, Governor, Federal Reserve System, Speech at the Univ. of Mich., "*Where Do Consumers Fit in the Fintech Stack?*," (Nov. 16, 2017), https://www.federalreserve.gov/newsevents/speech/brainard20171116a.pdf.

[6] The Clearing House, *Consumer Survey: Financial Apps and Data Privacy* (Nov. 2019), https://www.theclearinghouse.org/-/media/New/TCH/Documents/Data-Privacy/2019-TCH-ConsumerSurveyReport.pdf.

As for consumer control over such data, Governor Brainard again explains:

> In examining the terms and conditions for a number of fintech apps, it appears that consumers are rarely provided information explaining how they can terminate the collection and storage of their data. For instance, when a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information. If a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don't have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best.

The Dodd-Frank Act calls upon the CFPB to ensure that "markets for consumer financial products and services are fair, transparent, and competitive."[7] In particular, the CFPB has specific authority under Section 1032 of the Dodd-Frank Act to "prescribe rules to ensure that the features of any consumer financial product or service, both initially and over the term of the product or service, are fully, accurately, and effectively disclosed to consumers in a manner that permits consumers to understand the costs, benefits, and risks associated with the product or service, in light of the facts and circumstances."[8]

Accordingly, we recommend the CFPB use its rulemaking authority under section 1032 of the Dodd-Frank Act to ensure that consumers understand the costs, benefits, and risks associated with their use of consumer financial products and services that are provided through the consumer financial data services market. The CFPB should consider promulgating disclosure requirements to ensure that consumers are provided with timely and understandable information needed to make responsible decisions about the sharing of their consumer financial data with aggregators and fintechs, and that the market for consumer financial data operates transparently and efficiently to support enhanced consumer access and innovation.

The CFPB should support secure methods for consumers to access their financial data that do not require consumers to share their account credentials with third parties, such as through API agreements between banks and data aggregators.

Credential-based access is almost always over-broad and presents security risks. The CFPB's Principles state that authorized third parties should "only access the data necessary to provide the product(s) or service(s) selected by the consumer and only maintain such data as long as necessary." This can generally be characterized as a "data minimization" principle, which recognizes that large data sets present risks to the holders

[7] 12 U.S.C. § 5511.

[8] 12 U.S.C. § 5532.

and subjects of the data. However, the currently-prevalent practice of credential sharing is inherently inconsistent with data minimization: even if consumers only authorize use of their credentials to obtain account data, the aggregator or fintech that obtains a consumer's credentials has the capacity to access *all* of the consumer's information. In other words, even if a consumer provides an aggregator or fintech limited authorization to access information from a financial institution, by asking for the consumer's credentials, the aggregator or fintech obtains access to the full suite of data and services available to the consumer. This practice both misleads consumers about the activity that actually occurs and exceeds the consumer's express authorization.

The CFPB's Principles also state that an authorization to initiate payments is separate and distinct from an authorization to obtain data. ("Authorized data access, in and of itself, is not payment authorization. Product or service providers that access information and initiate payments obtain separate and distinct consumer authorizations for these separate activities.") However, the holder of a consumer's bank account credentials often has the capacity to initiate electronic funds transfers and account changes, even if the consumer never authorizes the aggregator or fintech to take those actions. By way of comparison, European regulations draw a distinction between regulated account information service providers (AISPs) and payment initiation service providers (PISPs), each being subject to different regulations that acknowledge their respective risk profiles. Aggregators and fintech obtaining data using consumer credentials have the capacity to access more data than they need and initiate transactions not requested by a consumer. Moreover, storing credentials presents a substantial threat to consumers because an aggregator or fintech data breach could result in fraudulent access to consumers' online accounts. As a result, credential-based access presents heightened risks and, to the extent credential-based access continues to be allowed, the companies using this access method should be subject to commensurate, heightened regulatory obligations.

Under the Gramm-Leach-Bliley Act ("GLBA"), data aggregators may argue that they are requesting and obtaining data from a financial institution "[w]ith the consent or at the direction of the consumer."[9] However, the exception that permits a financial institution to disclose nonpublic personal information based on consumer consent relates to the specific act of a particular disclosure to a particular third party, and does not provide a financial institution with a general exception to the application of GLBA for unlimited sharing of data to third parties.[10] In other words, the GLBA exception for consumer-directed disclosure is not intended to permit a financial institution to obtain a consumer's blanket consent to avoid GLBA restrictions on third party sharing altogether.[11] Rather, consumer consent or direction to disclose information under GLBA should be expressed by the consumer directly to the financial institution and identify parameters of the disclosure for each particular use case.

---

[9] 12 C.F.R. § 1016.15(a)(1) (2019).

[10] See 12 C.F.R. §§ 1016.14(a)(1), 1016.15(a)(1).

[11] In addition, under GLBA, reuse and disclosure obligations continue to apply to any subsequent third-party sharing of the customer's nonpublic personal information after a customer receives notice and opt-out rights from the originating financial institutions, and are controlled by the privacy policy of the originating financial institution. 15 U.S.C. § 6802(c); 12 C.F.R. § 1016.11.

This consent can be adequately captured via a financial institution's OAuth authentication protocol.

For similar reasons, Capital One recommends that the CFPB collaborate with its prudential counterparts and affirm that, notwithstanding the CFPB's Principles regarding Consumer-Authorized Financial Data Sharing and Aggregation, financial institutions should not depart from the FFIEC's guidance regarding authentication in an internet banking environment.[12] In particular, that "where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risk." Among other concerns, fraudulent attempts to access consumer accounts may look similar to account access attempts by aggregators and fintechs via shared credentials, or third-party fraudulent actors may use data aggregators to "stuff" illicitly obtained login-password combinations, hoping to bypass protections used for general consumer access.

APIs are a viable alternative with several benefits relative to credential-based access. First, an API that facilitates the transfer of consumer financial data coupled with authentication technology, such as OAuth, allows consumers to authenticate with a financial institution data provider, who would in-turn give the aggregator or fintech a token to access data in lieu of credentials, removing credentials from the aggregator/fintech ecosystem. Second, data transferred via API can be tailored to the consumer's authorization and subject to enhanced security including encryption. Third, APIs are a far more efficient and scalable platform for the distribution of data. Fourth, Capital One provides access to its APIs for free and, as APIs become more ubiquitous, consumer access will continue to grow.

Because credential-based access is almost always overbroad and APIs are a viable alternative, we urge the CFPB to require aggregators and fintechs seeking consumer-permissioned access to data from financial institutions to use API-based connections when they are available.

The CFPB should exercise its authority under Dodd Frank Act Section 1024(a)(1)(C) to provide notice of its intent to require reports and conduct supervisory examinations of specific non-bank data aggregators, given the risks they pose to consumers and the consumer financial services market.

Although financial institutions and data aggregators store similar data, the substantive expectations that guide financial institutions' data security practices set a significantly higher bar than what is currently expected of data aggregators. In that regard, financial institutions and data aggregators are both subject to the data security requirements established in GLBA. Banks and non-banks, however, are subject to quite different sets of implementing regulations and regulatory guidance.

Banks are subject to extensive regulatory, supervisory and enforcement scrutiny as articulated in the Interagency Guidelines Establishing Information Security Standards,

[12] Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment*, https://www.ffiec.gov/pdf/authentication_guidance.pdf.

adopted jointly by the federal financial regulators (the "Interagency Guidelines").[13] The Interagency Guidelines include numerous expectations regarding data security. For example, a bank's Board of Directors, or an appropriate committee thereof, must "oversee the development, implementation, and maintenance" of the bank's information security program, ultimately approving the program.[14] This includes reviewing regular reports on the overall status of the bank's compliance with the program, including issues such as service provider arrangements; results of testing; security breaches and management's responses; and recommendations for changes.

Banks are expected to conduct regular risk assessments, as well as to periodically gauge the sufficiency of their policies, procedures, customer information systems, and other arrangements to control such risks. In so doing, banks are expected to consider and, where appropriate adopt, a number of detailed recommendations ranging from: (a) access controls on customer information systems; (b) similar restrictions for physical locations; (c) encryption of electronic customer information; (d) procedures designed to ensure that customer information systems are consistent with the financial institution's information security program; (e) dual control procedures, monitoring systems, and procedures for intrusions; (g) response programs that specify actions to be taken in the event of unauthorized access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and (h) measures to protect against the loss of customer information due to potential environmental hazards (e.g., fire/water or technological failure).[15]

Importantly, banks are expected to exercise "appropriate due diligence" in selecting service providers and to require that such service providers "implement appropriate measures designed to meet the objectives" of the GLBA guidelines. Banks are expected to monitor their service providers, where indicated by the banks' risk assessments, including by requiring audits, summaries of test results, or other equivalent evaluations.[16]

In contrast, data aggregators and fourth party fintechs -- which seek access to the very same consumer data safeguarded by banks -- are not subject to the Interagency Guidelines. Rather, as non-bank financial institutions, they would be subject to the more flexible regulations promulgated by the Federal Trade Commission ("FTC").[17] As one industry expert described the FTC's Safeguards Rule, a non-bank "that is subject to an investigation and/or potential enforcement action by the FTC could quite reasonably argue that there are no specific requirements for the technical controls they are required to employ to control identified risks."[18] Last year, the FTC announced that it was seeking comment on

---

[13] Interagency Guidelines, 12 C.F.R. Pt. 30, App. B (as incorporated into the OCC regulations for national banks). The Interagency Guidelines also apply to members of the Federal Reserve System, as well as banks and savings associations insured by the Federal Deposit Insurance Corporation, federally-insured credit unions, and broker-dealers, investment companies, and investment advisors.
[14] *Id*. §III.A.
[15] *Id*. §III.C1(a)-(h).
[16] *Id*. §III.D.
[17] FTC Safeguards Rule, 16 C.F.R. Pt. 314.
[18] Rob Hunter, Ensuring Consistent Consumer Data Protection, The Clearing House,

proposed changes to the GLBA Safeguards Rule.[19] If the FTC finalizes the elements of its proposal, the revisions would create substantive expectations for non-banks that are closer to the Interagency Guidelines but whether parity will exist with banks is yet to be determined.

In addition to the different substantive expectations for non-banks under GLBA, the *process* differences between the two regimes are stark. Banks are regularly examined by prudential regulators, including data-security related inquiries. In contrast, data aggregators and fintechs are generally not subject to regular examinations and other oversight by prudential regulators. Accordingly, even under a revised GLBA Safeguards Rule, if a data aggregator maintained sub-par data security practices and suffered an actual data breach, regulators and consumers may never know.

The CFPB has statutory authority that can bring greater oversight to non-bank data aggregators that now hold data on over twenty million consumer accounts.[20] In our response to the November 2016 Request for Information, Capital One recommended that the CFPB exercise its authority under Dodd-Frank Act Section 1024(a)(1)(B) to promulgate, after consultation with the FTC, a rulemaking delineating the CFPB's supervisory and enforcement authority over larger participants in the data aggregator market.

Dodd-Frank Act Section 1024, however, also sets out CFPB supervisory authority over a number of other market participants that do not require an additional rulemaking. In particular, Sections 1024(a)(1)(C) and 1024(b) direct the Bureau to require reports and conduct examinations on a periodic basis of non-depository covered persons that "the Bureau has reasonable cause to determine, by order, after notice to the covered person and a reasonable opportunity for such covered person to respond," based on information that such person is "engaging in, or has engaged, in conduct that poses risks to consumers with regard to the offering or provision of consumer financial products or services."

Given the growing concentration in the data aggregation market,[21] the Bureau should initially bring oversight to the data aggregation marketplace by focusing on a small handful of specific firms engaging in conduct that poses risks to consumers, rather than undertake a lengthy rulemaking process to define the "larger participants" in this market. Data aggregators hold an enormous volume of consumer data and have the potential to cause large-scale negative externalities to millions of consumers and the financial institutions that

---

https://www.theclearinghouse.org/banking-perspectives/2015/2015-q3-banking-perspectives/articles/ensuring-consumer-data-protections (last visited Feb. 13, 2020).

[19] Federal Trade Commission, *FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules* (Mar. 5, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules.

[20] *See*, *e.g.*, Kate Rooney, *Meet the start-up you've never heard of that powers Venmo, Robinhood and other big consumer apps*, CNBC(Oct. 4, 2018) https://www.cnbc.com/2018/10/04/meet-the-startup-that-powers-venmo-robinhood-and-other-big-apps.html.

[21] *See*, *e.g.*, Donna Fuscaldo, *Plaid Buys Quovo In Its First Major Acquisition* Forbes, (Jan. 8, 2019), https://www.forbes.com/sites/donnafuscaldo/2019/01/08/plaid-buys-quovo-in-its-first-major-acquisition/#55a1f6dc648d.

consumers have entrusted with their financial lives. Accordingly, Capital One recommends that the CFPB conduct regular examinations of high-profile data aggregation firms, coordinating where appropriate with prudential regulators, pursuant to the CFPB's authority under Dodd-Frank Act Section 1024(a)(1)(C). Further, Capital One recommends that any such examination of non-bank data aggregators begin with the CFPB articulating clear expectations regarding appropriate disclosure, consumer control, data security, and oversight relating to data aggregators' sharing consumer data with fourth parties.

Conclusion

We recommend that the CFPB continue to work with industry, consumer, and regulatory stakeholders in an open and transparent manner to continue to inform the CFPB on issues specific to section 1033, inclusive of the issues discussed above.

While we believe that the CFPB should act on the recommendations above prior to considering whether to impose any new regulations or binding standards under section 1033 of the Dodd-Frank Act, we recommend that if the CFPB does so, it begins by collaborating with Federal banking agencies and the FTC to ensure consistent treatment across the industry. In particular, the Federal banking agencies would be able to share their perspectives on safety and soundness, reputational risk, and trust in the banking industry with respect to practices in the consumer financial data services marketplace.

Respectfully,

Becky Heironimus

Rebecca "Becky" Heironimus
Managing Vice President
Digital Enterprise Customer

Capital One Financial Corporation
1680 Capital One Drive
McLean, Virginia 22102

February 21, 2017

Via Electronic Delivery

Monica Jackson, Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, D.C. 20552

Re: Docket No. Bureau-2016-0048; Request for Information Regarding Consumer Access to Financial Records

Dear Ms. Jackson:

Capital One appreciates the opportunity to comment on the Request for Information Regarding Consumer Access to Financial Records ("RFI") by the Consumer Financial Protection Bureau ("CFPB").[1] Capital One applauds the CFPB for issuing the RFI, as Capital One supports innovations that empower consumers to manage their finances in a safe and convenient manner.

Technology allows consumer financial data to be broadly accessed and rapidly disseminated. Innovations that rely on consumer financial data can provide significant benefits, but also can put at risk legitimate consumer interests, including the security of and control over such data. It is vital, therefore, to ensure that long-standing consumer protections apply to consumer financial data across the data services sector.

Accordingly, we respectfully suggest that, in examining consumers' access to their own financial data, the CFPB take the opportunity to assess how best to protect consumer financial data throughout its lifecycle. In that spirit, in sections I-II of the discussion below, we provide the CFPB with information pertinent to its analysis. In addition, in section III of the discussion, we offer recommendations intended to ensure that industry participants can continue to bring consumers new and innovative products and services within a resilient market structure that advances and protects their interests.

---

[1] Capital One Financial Corporation (www.capitalone.com) is a financial holding company whose subsidiaries, which include Capital One, N.A., and Capital One Bank (USA), N.A., had $236.8 billion in deposits and $357.0 billion in total assets as of December 31, 2016. Headquartered in McLean, Virginia, Capital One offers a broad spectrum of financial products and services to consumers, small businesses and commercial clients through a variety of channels. Capital One, N.A. has branches located primarily in New York, New Jersey, Texas, Louisiana, Maryland, Virginia and the District of Columbia. A Fortune 500 company, Capital One trades on the New York Stock Exchange under the symbol "COF" and is included in the S&P 100 index.

Executive Summary

Consumers have long received special protections for their financial data due to its inherently sensitive nature and its value to third parties. The Gramm-Leach Bliley Act of 1999 ("GLBA") is the bedrock law that provides consumers with privacy and data security protections over their financial data.

While all financial institutions are required by GLBA and its implementing regulations to deliver privacy and security protections on behalf of consumers, some companies that store and use consumer financial data believe that those requirements are inapplicable to their activities.

Many consumers who use new services that pull their financial data from a bank end up losing the safe and secure environment where their financial data is accorded the longstanding protections provided by law, by releasing their data into a relatively unfettered data services marketplace that may not grant privacy protections or adequately safeguard the sensitive data from security risks. Consumers are not sufficiently informed or given meaningful choice to consent or object to the privacy and data sharing practices of these new services. Moreover, the ability of consumers to understand rapidly evolving market practices is being outpaced by the proliferation of new actors, technologies, and techniques to monetize consumer financial data.

Despite the risks to consumers, much of the public dialogue concerning innovative services using consumer financial data ignores the loss of consumer privacy, transparency, and control over uses for the data. These risks are greatly exacerbated when the data is moved to a business that does not feel constrained by the requirements of the GLBA. Nor has the debate about these services focused on the security risks that consumers face when they part with their banking credentials, which, when stolen, provide a fraudster with control over the consumer's entire financial account and enables identity theft and theft of funds. Instead, many nonbank companies providing new services assert interests that stand in direct conflict to consumer interests, by calling for third parties to have *unfettered* access to bank systems in order to obtain consumer financial data and by employing a *caveat emptor* philosophy of use and disclosure.

Given the current status of this market, we respectfully recommend:

- The CFPB should work with stakeholders to produce overarching principles governing consumer financial data that can guide the marketplace to develop solutions that address consumer privacy and security risks. These principles should encompass the long-standing protections provided by GLBA, and address: (i) consumer transparency; (ii) restrictions on the sharing of data; (iii) restrictions on use of data; (iv) consumer accessibility; (v) consumer control; and (vi) cost.

- The CFPB and its sister regulatory agencies should use their existing powers to make clear that GLBA's consumer protections apply to consumer financial

data held by all financial institutions, including non-bank innovators that seek to play a role in this ecosystem.

- The CFPB should bring the financial aggregator and consumer financial data market under its direct supervision by designating larger participants for this market.

These recommendations would prevent the continued growth of a shadow financial system in which consumers, with one click, can unwittingly transfer their data from a safe environment into a largely unfettered and unprotected marketplace.

Discussion

I. Consumer Financial Data Has Long Been Given Special Status and Accorded Special Protections

Consumer financial data has long been accorded special status under U.S. law due to its sensitive nature and value to potential bad actors.[2] The policy and regulatory basis for special treatment of financial data is reflected in a comprehensive set of well-settled laws and regulations that form the foundations of consumer protections in both privacy and data security for nearly two decades.

The main federal laws that regulate the treatment of consumer financial data are the GLBA, the Fair Credit Reporting Act ("FCRA"), and the Fair and Accurate Act Credit Transactions Act ("FACTA"). The special protections provided to consumer financial data in the United States, as a result of these laws, fall into five categories: privacy; sharing of data; use of data; security; and accessibility. These categories share an expectation that institutions provide consumers with transparency into their data practices, permit consumers choice about how their data is used, and provide consumers with the ability to correct inaccuracies when that data will be used for eligibility or employment purposes.

In addition, many consumer transactional accounts require periodic disclosure of certain information related to the consumer's account. Regulation Z (implementing the Truth in Lending Act with respect to periodic statements for credit cards),[3] Regulation E (implementing the Electronic Fund Transfer Act with respect to periodic statements for traditional bank accounts and other consumer asset accounts),[4] and Regulation DD (implementing the Truth in Saving Act with respect to periodic statements for deposit

---

[2] This letter generally uses the terms consumer financial data and nonpublic personal information interchangeably but when referring to legal requirements, generally uses the term nonpublic personal information.

[3] 12 C.F.R. §§ 1026.5(b)(2), 1026.7(b).

[4] 12 C.F.R. § 1005.9(b).

accounts held at depository institutions),[5] are among the requirements imposing periodic disclosure of a consumer's financial account information.

Section 1033 of the Dodd-Frank Act, upon implementation through rulemaking, provides a consumer right to access information in the control or possession of a covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, or series of transactions, to the account including costs, charges, and usage data.[6]

II. The Fast-Evolving Consumer Financial Data Services Market is not According Special Status to Consumer Financial Data and the CFPB Should Take Action to Ameliorate this Failure

Current market practices undermine the long tradition of consumer trust in banks to keep their data safe, secure, and private, and within the consumer's control through opt-out mechanisms. By providing third party access to their data, consumers may unknowingly be pulling their non-public, personal, financial data from a safe and secure environment where it is accorded the protections of the law, and releasing it into a relatively unregulated data services market where providers may not grant the data the special protections required by law.

A. Data Aggregators Avoid Longstanding Data Privacy and Data Security Protections

Data aggregators are a class of businesses that gather and present consumer financial data in a new format for the consumer or provide services themselves or through "fintech" companies based on the consumer's financial data. Some companies in the consumer financial data services market appear to take the position that GLBA does not apply to them. Whether they argue that they do not meet the definition of a "financial institution" under GLBA, or that section 1033 allows them to avoid the GLBA safeguards for consumer financial data because they stand in the shoes of the consumer when they use the consumer's credentials to access the consumer's personal information,[7] these companies contend that they can avoid GLBA's data security and privacy requirements applicable to financial institutions. Without GLBA coverage, these companies are not obligated to provide the transparency and use limitations observed by banks and may freely develop products for third parties that exploit the consumers' data.[8]

---

[5] 12 C.F.R. § 1030.6(a)(3).

[6] 12 U.S.C. § 5533. We do not believe that section 1033, as a matter of law, requires covered persons to provide "direct and unfettered" access to bank systems in order to permit any unconfirmed third party to access consumer financial data, without having first secured adequate contractual protections, as a matter of safety and soundness and to protect consumers from risk of harm. For further information, please refer to the comment letter on this RFI by the Clearing House Association L.L.C.

[7] 12 U.S.C. § 5481(4).

[8] For instance, the Wall Street Journal reported on Yodlee's sale of credit card and debit card data to investors and research firms. See Wall Street Journal, *Provider of Personal Finance Tools Tracks Bank*

Moreover, because many data aggregators incorrectly conclude that they are free of GLBA's rules regarding reuse and redisclosure of non-public financial information, they do not limit their use of consumer financial data for purposes beyond the specific consent to receive the service that the consumer sought when she provided her credentials.[9] The additional uses are generally ones that will allow the data aggregator to monetize the data through consumer identification, risk management (like fraud analytics), or aggregated insights.

Overall, these companies have built their business model around a legal theory that allows them to treat consumer financial data as data that carries no special legal protections. Effectively, these companies are choosing to treat consumer financial data as though it were any other data, like the webpages that the consumer viewed.

B. Data Aggregators Are Financial Institutions Subject to GLBA

GLBA provides a set of protections for the "nonpublic personal information" of a "consumer" that is held by a "financial institution." GLBA regulates the collection, use, protection, and disclosure of consumer nonpublic personal information by financial institutions. As noted above, GLBA protects nonpublic personal information by, among other things, requiring financial institutions to implement appropriate safeguards to protect the consumer's nonpublic personal information, and requiring financial institutions to satisfy an exemption or various conditions prior to sharing the consumer's nonpublic personal information, including providing a consumer with notice of the institution's privacy practices and the right to opt-out of certain types of sharing.

Congress included an intentionally robust and expansive definition of "financial institution" in the GLBA. The definition of a "financial institution" incorporates by reference any business that engages in financial activities identified by the Board of Governors of the Federal Reserve System ("Federal Reserve Board") pursuant to section 4(k) of the Bank Holding Company Act of 1956 (12 USC 1843(k)).[10] Section 4(k) incorporates the § 225.28 of the Federal Reserve Board's Regulation Y, which is a list of nonbanking activities that are so closely related to banking "as to be a proper incident thereto" and a bank may engage in them.[11] This list includes "data processing, data storage and data transmission services, facilities (including data processing, data storage and data transmission hardware, software, documentation, or operating personnel), databases, advice, and access to such services, facilities, or data-bases by any technological means, if the data to be processed, stored or furnished are financial,

---

Cards, Sells Data to Investors (Aug. 6, 2015), available at http://www.wsj.com/articles/provider-of-personal-finance-tools-tracks-bank-cards-sells-data-to-investors-1438914620.

[9] 15 U.S.C. § 6802(c).

[10] 15 U.S.C. §§ 6809(c), 6809(3)(A); 12 C.F.R. § 1016.3(l)(1).

[11] 12 C.F.R. § 225.28.

banking or economic.[12] Section 225.28 lists other activities that would qualify aggregators as financial institutions if they engage in one of those activities. These activities include "acting as investment or financial advisory to any person, including… [f]urnishing general economic information and advice, general economic statistical forecasting services, and industry studies…[p]roviding education courses, and instructional materials to consumers on individual financial management matters; and [p]roviding tax-planning and tax-preparation services."[13] In addition, any entity "[a]cting as a certification authority for digital signatures and authenticating the identity of persons conducting financial and nonfinancial transactions," may also be a financial institution.[14]

Also, the FTC determined that data aggregators qualify as "financial institutions" under the GLBA.[15] In the preamble to the FTC's regulation implementing privacy provisions of the GLBA, the FTC explained that the broad language used to describe "data processing" in section 225.28 "brings into the definition of financial institution an Internet company that compiles, or aggregates, an individual's on-line accounts (such as credit cards, mortgages, and loans) at that company's web site as a service to the individual, who may then access all of its account information through that Internet site."[16] The FTC's regulation implementing the GLBA has been incorporated in Regulation P, issued by the CFPB post-Dodd-Frank.[17] The CFPB has stated that it generally will follow the guidance issued by other agencies whose regulations CFPB has restated. Thus, given their fundamental data processing activities, data aggregators fall within the expansive definition of financial institution in the GLBA. Data aggregators' other activities may also independently fall under the GLBA definition of "financial activities" as well.

"Financial institutions" under the GLBA have certain obligations for the nonpublic personal information that they obtain.[18] Congress defined "nonpublic personal information" ("NPI") as personally identifiable financial information either provided by a consumer[19] to **a** financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by **the** financial

---

[12] 12 C.F.R. § 225.28(b)(14).

[13] See 12 C.F.R. § 225.28(b).

[14] 12 C.F.R. § 225.86(a)(2)(iii).

[15] See The Clearing House *et al.*, *Risks Regarding Data Aggregation Services that Access Consumer Bank Accounts / Information Through Use of Consumers' Login and Password Credentials* at 12–13 (April 2016) ("TCH Whitepaper").

[16] 65 Fed. Reg. 33,646 (May 2000).

[17] See 76 Fed. Reg. 79,026 (Dec. 21, 2011).

[18] 15 U.S.C. § 6809.

[19] Congress defined the term "consumer" as "an individual who obtains, from **a** financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." 15 U.S.C. § 6809(9) (emphasis added).

institution.[20] GLBA does not apply only when a consumer has a continuing relationship with the financial institution, and is therefore a customer under Regulation P of the GLBA.[21] Rather, a consumer's nonpublic personal information has certain rights and protections when it is being held by a financial institution. In other words, data aggregators have obligations for any personally identifiable financial information of a consumer that the data aggregator has obtained in any manner.

When a data aggregator receives the consumer's permission to obtain the consumer's personally identifiable financial information from another financial institution, and the data aggregator stores that consumer's personally identifiable financial information, the information falls within the definition of nonpublic personal information under GLBA and carries with it all accordant rights and protections applied by GLBA. Because of the broad scope of the GLBA, data aggregators have obligations for any personally identifiable financial information of a consumer that the data aggregator has obtained in any manner. Therefore, GLBA applies to data aggregators despite many data aggregators purportedly not having ongoing customer relationships with consumers.

Congress's intent is abundantly clear from its use of the term *consumer* rather than *customer* in describing the category of nonpublic personal information subject to the most extensive regulation. In particular, except as otherwise provided, a financial institution may not disclose to a "nonaffiliated third party" any nonpublic personal information of a "consumer," unless such financial institution provides or has provided to the consumer a notice that complies with the section requiring disclosure of the institution's privacy policy.[22] Moreover, this section (with certain enumerated exceptions), prohibits a financial institution from disclosing nonpublic personal information to a nonaffiliated third party unless the financial institution clearly and conspicuously discloses to the consumer that such information may be disclosed to such third party; the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such third party; and the consumer is given an explanation of how the consumer can exercise that nondisclosure option.[23] And, a nonaffiliated third party that receives nonpublic personal information from a financial institution "shall not, directly or through an affiliate of [that] third party, disclose such information to any other person that is a nonaffiliated third party of both the financial institution and [that] receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution."[24] Finally, a financial institution is required to impose adequate safeguards

---

[20] 15 U.S.C. § 6809(4).

[21] 12 C.F.R. § 1016

[22] 15 U.S.C. § 6802(a); see also 12 C.F.R. § 1016.4(a)(2) (2017) (initial privacy notice to consumers).

[23] 15 U.S.C. § 6802(b); see also 12 C.F.R. § 1016.7 (2017) (opt out notice to consumers).

[24] 15 U.S.C. § 6802(c); see also 12 C.F.R. § 1016.11 (2017) (limits on redisclosure and reuse of information).

over the security and confidentiality of nonpublic personal information.[25] The implementing regulations and guidance concerning the safeguarding of nonpublic personal information is extensive for financial institutions subject to the safeguards regulations promulgated by the Federal Reserve Board, OCC, and FDIC.[26]

As noted above, some of GLBA's notice and opt-out requirements do not apply if the financial institution is disclosing the consumer's nonpublic personal information with the consent or at the direction of the consumer.[27] Data aggregators may argue that they have the consumer's consent or are operating at the direction of the consumer. The exception for consumer consent, however, pertains to the specific act of a particular disclosure to a particular third party, and does not provide a financial institution with a general exception to the application of GLBA for unlimited sharing of that data to other third parties.[28] Under the GLBA's implementing regulations, a financial institution must provide a revised notice before the financial institution begins to share a new category of nonpublic personal information or shares information with a new category of nonaffiliated third party in a manner that was not described in the previous notice under which the initial data sharing occurred.[29] In other words, the exception for a consumer's consent is not intended to permit a financial institution to obtain a consumer's blanket consent to avoid GLBA restrictions on third party sharing altogether. In addition, under GLBA, reuse and disclosure obligations continue to apply to any subsequent third-party sharing of the customer's nonpublic personal information after a customer receives notice and opt-out rights from the originating financial institutions, and are controlled by the privacy policy of the originating financial institution.[30]

Given the clarity of the statute and implementing regulations, we are concerned that some data aggregators are embedding into their practices a data regime that declines to provide nonpublic personal information with special protections, ostensibly by using consumer consent as a way to "opt out" of the GLBA in its entirety. This practice is not only wrong as a matter of law, but also because consumers are not knowingly consenting to the loss of privileges for their nonpublic personal information when they consent to its transfer out of the regulated banking system.

---

[25] See 15 U.S.C. § 6801(b) (requiring agencies, other than the CFPB, to establish standards for the protection of consumer information).

[26] Interagency Guidelines Establishing Standards for Safeguarding Customer's Information, 12 CFR Part 30, App. B. See also TCH Whitepaper at 13-14 ("there is currently no notification requirement imposed by the FTC on non-bank financial institutions that experience a breach resulting in the unauthorized disclosure of customer data"); The Clearing House, *Ensuring Consistent Consumer Protection for Data Security: Major Banks vs. Alternative Payment Providers* (August 2015).

[27] 15 U.S.C. § 6802(e)(2); see also 12 C.F.R. § 1016.15(a)(1) (2017)

[28] See 12 C.F.R. §§ 1016.14(a)(1), 1016.15(a)(1) (2017).

[29] 12 C.F.R. § 1016.8(b)(1)(i) (2017).

[30] 15 U.S.C. § 6802(c); 12 C.F.R. § 1016.11.

C. Data Practices in the Consumer Financial Data Services Marketplace

New technology has enabled the rapid proliferation of fintech companies to emerge during a time when the population feels comfortable conducting business with an entity with which it has little prior experience, and that does not have any physically accessible location. Recently, however, the risks of consumer financial data aggregation services have increased in parallel with the growth of the market. The Clearing House and the Financial Services Roundtable published a paper in April 2016 that described these risks and explained how banks are beginning to use rules and standards agreed to and enforced by contract to mitigate them.[31]

Consumer risks are especially concerning. Effective disclosure and consumer awareness are lacking in the consumer financial data services market, as consumers are not made fully aware of the costs, benefits, and risks of using consumer financial data aggregator services because the nature and scope of these services often are not fully, accurately, and effectively disclosed to consumers.[32]

In order to provide their data services to end-user fintech companies, to date, most data aggregators require consumers to part with their credentials. In so doing, consumers are inadvertently subjecting themselves to security and financial risks, as they do not have full transparency about the consequences of that decision. They likely do not understand that the credentials will be provided to a third party – the data aggregator – who will employ screen scraping to obtain the consumer's financial data by acting as the consumer in order to enter into the consumer's secure online financial account environment. Consumers are not made aware that these practices can shift loss protections under Regulation E, nor that providing their credentials may be a violation of the terms and conditions of their financial account.[33]

Consumers have long grown to trust that regulated financial institutions are subject to a strict legal, regulatory, and supervisory regime to safeguard consumer data. Consumers are generally not aware of the differences in the legal and supervisory standards and practices of other participants in the marketplace, and that their consumer data may not be as safe and secure once it is removed from the banking system.

Consumers may not be aware of the full range of activities of data aggregators when they provision an innovative application to obtain their financial data, including that the data aggregator will copy and store their data, will use the data for other purposes, or will create new products and services using the consumer's data.[34] Consumers are not made aware that data aggregators collect and transfer not only the data

---

[31] TCH Whitepaper.

[32] See 12 U.S.C. § 5532.

[33] See TCH Whitepaper at 6-11.

[34] For instance, some data aggregators are marketing identity management products.

necessary for the consumer to use the new financial product or service, but also as much information as can be obtained. For instance, in the case of screen scraping, the data aggregator may obtain more information than authorized if the consumer credentials provide the data aggregator with access to additional financial accounts of the consumer, as is typically the case with the deployment of single sign-on capability.

Despite these concerns, fintech companies, data aggregators, and large technology companies have been increasingly vocal in asserting interests that stand in conflict to consumer interests. Brian Peters, Executive Director of Financial Innovation Now (a new fintech industry trade group), has articulated that these technology companies employ a philosophy of *caveat emptor*: "It's up to the consumer to decide what technology they want to use and what level of privacy and security they want."[35] Indeed, the current privacy policies and data practices of data aggregators reveal the potential consequences of such a philosophy – a lack of sufficient transparency and the reservation of full institutional discretion to make changes to privacy practices without notice to the consumer or any opportunity to opt out of such changes, including any changes to practices relating to the sharing of the consumer's personal financial information.

Overall, under the regime envisioned and exercised by these companies, risks are shifted to the consumer and the consumer can, with one click, opt out of all the special protections that have traditionally applied to the consumer's financial data. Without the application of the special safeguards to consumer financial data, data aggregators are unconstrained in their ability to transfer data into the broader market, or to utilize data in their possession for new activities and new sources of revenue. These risks can be further exacerbated when downstream clients of the data aggregators also lack sufficient protections for consumer financial data.

Arguably, in today's marketplace, absent reasonable rules of the road for the collection, use and dissemination of consumer data, consumers are left with two unattractive choices: relinquish control over the safety of their personal data or elect not to take advantage of any new and innovative products and services outside of the banking industry for fear such data will not be protected. That is not true consumer choice.

The CFPB has the authority to ensure that consumer financial data is safeguarded throughout its lifecycle, thereby ensuring consumers have a stable and consistent level of protection for their financial data, regardless of where the data originated, where it has been transferred, and the type of financial institution using or storing the data.

D. Bank Operational Risk Management

In light of the changing risk environment, many financial institutions have determined that, as a matter of consumer protection and safety and soundness, protecting consumers' data through contractual rights and obligations is both prudent and necessary.

---

[35] See Lalita Clozel, American Banker, *Why Silicon Valley Is Watching the Screen Scraping Debate* (Dec. 29, 2016), available at https://www.americanbanker.com/news/why-silicon-valley-is-watching-the-screen-scraping-debate.

More recently, consumer data security risks have required the marketplace to move away from sharing credentials and screen scraping to more secure and modern mechanisms for authentication and transmission of data. In addition to the consumer issues specified above, some market participants are concerned about the significant reputational costs that would be faced if trust in the banking system were affected by practices and failures in the broader consumer financial data services market.[36]

In the risk discussion within the RFI, the CFPB speaks to these issues but from a different perspective:

> "The Bureau believes, however that such market participants do not necessarily share common views about consumer protection and other consumer interests. More fundamental still, the Bureau does not believe that consumer views have been adequately represented in this area. The Bureau is concerned, therefore, that some market participants may decide to restrict consumer-permissioned access to data in ways that undermine consumer interests identified in section 1033 – and that are broader than necessary to address legitimate privacy and security concerns."[37]

We agree with the CFPB that the market is not aligned on the consumer's best interests. In particular, we do not believe that any marketplace participants should ignore (or that the CFPB would want any entities to waive) legitimate consumer privacy and security considerations. We also believe that, absent such efforts, market participants risk eroding the slowly-built and long-standing consumer trust in the financial system.

Therefore, we urge the CFPB to address legitimate consumer interests in the consumer financial data services marketplace by using the various authorities that have been granted to the CFPB through the GLBA and the Dodd-Frank Act, as specified in section III below. This will enable marketplace participants to have confidence that consumer interests will be protected across the entire consumer financial data ecosystem, and thereby enable market participants to responsibly shift resources away from the safeguarding of legitimate consumer interests through contracts and other mechanisms.

III. Recommendations

We respectfully offer the CFPB the following recommendations that are intended to ensure that industry participants can continue to bring consumers new and innovative products and services within a resilient market structure that protects and advances the interests of consumers.

---

[36] OCC Bulletin 2001-12 includes reputation risks among the risks that national banks are exposed to in offering aggregation services. OCC Bulletin 2001-12: Bank-Provided Account Aggregation Services (Feb. 28, 2001).

[37] 81 Fed. Reg. 83809.

A. CFPB Should Clarify and Strengthen Regulatory Oversight of Data Aggregators Using Its Existing GLBA and Dodd-Frank Authority

We recommend that the CFPB work with stakeholders to develop overarching principles governing consumer financial data. These principles can guide the marketplace by describing the CFPB's approach to consumer access to their own financial data, the responsibilities of financial data services under section 1033 of the Dodd-Frank Act and the other data and privacy protection laws enforced by the CFPB. This approach would be consistent and complimentary to international efforts to protect consumer data privacy and security, and to the efforts of the FTC, which has enforcement authority under certain of these statutes applicable to non-financial institutions.[38]

We recommend the CFPB work together with other regulatory stakeholders to define principles for consumer financial data that encompass the long-standing protections provided by GLBA, and include at least the following categories: transparency, restrictions on the sharing of data, including the required consent needed from the consumer prior to sharing data, restrictions on use of data, consumer accessibility, consumer control, and cost.

B. We Recommend the CFPB Close Identified Gaps Using GLBA Authority and Dodd-Frank Act Authorities

In parallel with the efforts to define principles for consumer financial data, we recommend that the CFPB use its existing regulatory authorities to address shortcomings in the consumer financial data marketplace, to make clear that GLBA applies to consumer financial data across the entire financial institution marketplace, and to bring this marketplace under direct supervision. Ensuring that consumers do not lose their long-standing protections when their nonpublic personal information moves away from the banks' servers, will enable consumers to both benefit from technological innovation and remain protected. Moreover, the data aggregators and fintech companies accessing the data will not build their business models around consumers sacrificing protection so their data can be sold, but rather around consumers choosing services.

1. GLBA Authority

Congress expressly provided the CFPB with GLBA rulemaking authority. Specifically, the CFPB is permitted to prescribe regulations that "may be necessary to carry out the purposes of this subchapter with respect to financial institutions and other

---

[38] In 2009, the FTC developed self-regulatory principles for online behavioral advertising. FTC Staff Report, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf. In 2012, the White House has developed a Consumer Privacy Bill of Rights and called for Congress to pass legislation that applies the Consumer Privacy Bill of Rights to commercial sectors that are not subject to existing Federal data privacy laws.

persons subject to their respective jurisdiction (the CFPB is not authorized to prescribe regulations with respect to the standards under section 6801 of this title, which covers regulations for the security of consumer nonpublic information).[39] The FTC was provided separate authority from the CFPB to prescribe regulations "as may be necessary to carry out the purposes of this subchapter with respect to any financial institution that is a person described in section 1029(a) of the Consumer Financial Protection Act of 2010.[40] Congress called on the agencies to consult and coordinate with each other with respect to the prescription of regulations pursuant to those authorities.[41]

We recommend that the CFPB consult with the banking agencies and the FTC in the exercise of this authority and prescribe regulations as are necessary to ensure that consumer financial data is accorded its special protections under the GLBA throughout its lifecycle in the consumer financial data services marketplace.

2. Dodd-Frank Act Authority

The CFPB has rulewriting authority under the Consumer Financial Protection Act of 2010 within the Dodd-Frank Act.

a. Section 1021 of the Dodd-Frank Act – Fair, Transparent, and Competitive Markets for Consumer Financial Products and Services

Section 1021 of the DFA calls for the CFPB to implement and, where applicable, enforce existing Federal consumer financial law consistently for the purpose of ensuring that all consumers have access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive.[42] That section specifically authorizes the CFPB to exercise its authorities under existing Federal consumer financial law for the purposes of ensuring that, with respect to consumer financial products and services—

> (1) consumers are provided with timely and understandable information to make responsible decisions about financial transactions;
> (2) consumers are protected from unfair, deceptive, or abusive acts and practices and from discrimination;
> (3) outdated, unnecessary, or unduly burdensome regulations are regularly identified and addressed in order to reduce unwarranted regulatory burdens;
> (4) Federal consumer financial law is enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition; and

---

[39] 15 U.S.C. § 6804(a)(1)(a).

[40] 15 U.S.C. § 6804(a)(1)(c).

[41] 15 U.S.C. § 6804(a)(2).

[42] 12 U.S.C. § 5511.

(5) markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation.[43]

We recommend that the CFPB use its existing Dodd-Frank Act authorities to ensure that consumers are provided with timely and understandable information to make responsible decisions about their financial transactions, and that the market for consumer financial data operates transparently and efficiently to facilitate access and innovation.

b. Section 1032 of the Dodd-Frank Act – Fully, Accurately, and Effectively Disclosed Features of Consumer Financial Products and Services

The CFPB has specific authority under 1032 of the Dodd-Frank Act to "prescribe rules to ensure that the features of any consumer financial product or service, both initially and over the term of the product or service, are fully, accurately, and effectively disclosed to consumers in a manner that permits consumers to understand the costs, benefits, and risks associated with the product or service, in light of the facts and circumstances."[44]

We recommend the CFPB use its rulemaking authority under section 1032 to ensure that consumers understand the costs, benefits, and risks associated with their use of consumer financial products and services that are provided through the consumer financial data services market.

c. Section 1024 of the Dodd-Frank Act – Supervision for Large Participants in the Markets for Consumer Financial Products and Services

Section 1024 of the Dodd-Frank Act provides the CFPB supervisory authority over covered persons that the agency declares as a larger participant of a market for other consumer financial products or services, after consultation with the FTC.[45] The Dodd-Frank Act provides the CFPB with general supervisory authorities, to require reports and conduct periodic examinations to assess compliance with the requirements of Federal consumer financial law; obtain information about the activities and compliance systems or procedures of such person; and detect and assess risks to consumers and to the consumer financial data market.[46]

Given the opaque nature of the practices of many data aggregators, we believe that the CPFB should exercise its authority to collect information from data aggregators about the collection and use of consumer financial information, including information

---

[43] 12 U.S.C. § 5511.

[44] 12 U.S.C. § 5532.

[45] 12 C.F.R. § 5514.

[46] 12 C.F.R. § 5514.

about their subsequent sharing of this information with other data aggregators and data brokers. We also believe that the CFPB's data collection effort should require data aggregators to provide comprehensive information about their privacy policies, consumer disclosures, and all other consumer-facing communications relating to data use and disclosure.

In addition, we recommend that the CFPB exercise its 1024 authority, after consultation with the FTC, to impose supervisory and enforcement authority over larger participants in the data aggregator market. Once the CFPB has exercised supervisory authority over these consumer financial data aggregators, the CFPB can appropriately monitor risks in the consumer financial data market through its supervisory authorities.

C. **Develop Priorities and Policies for Section 1033 of the Dodd-Frank Act**

While the CFPB considers how to address the risks that have emerged in the consumer financial data services market, we believe the CFPB should continue to study and understand the access issues specific to section 1033 of the Dodd-Frank Act. A primary concern of the CFPB, as well as many marketplace participants, is to move away from screen scraping as a data collection tool into a more secure access technology. While we also agree that data security is the fundamental issue to address within section 1033 of the Dodd-Frank Act, there are other questions and considerations specific to section 1033 of the Dodd-Frank Act that warrant the CFPB's attention.

1. *Data Security: How should marketplace participants and the CFPB ensure the security of consumer financial data at transmission?*

We believe data security is one of the primary considerations in affording consumers data access rights under section 1033 of the Dodd-Frank Act, should the CFPB decide to prescribe standards and requirements in accordance with its rulemaking authority.

In that regard, we believe that the CFPB should examine data security at transmission from the perspective of both authentication and data access technologies in determining the potential contours of access requirements under section 1033. While authentication and data access are functionally different, they are combined in order to provide a mechanism for data transfer. We believe that current market practices are inadequate to ensure secure and effective authentication and transmission of consumer financial data. However, given the variability of approaches and the availability of new technologies, we believe that market participants are best situated to decide which authentication and access technologies should be used. Accordingly, we do not believe at this time that the CFPB should prescribe standards or guidance mandating particular access or authentication practices or technologies, as regulatory standards or guidance are invariably outpaced by technological developments. We do, however, welcome the CFPB's promulgation of guidance concerning the need to move away from insecure practices with respect to credential sharing, in order to incentivize market participants to invest in the development of new technologies.

Customer Authentication Technologies: Authentication refers to how data access is permissioned and refers to the act of verifying the identity of the consumer and providing the consumer the ability to access the consumer's accounts. The Federal Financial Institutions Examination Council ("FFIEC") has published guidance on authentication.[47] FFIEC guidance is based on the principle that institutions should use effective methods to authenticate the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information.[48] The prevalent practice in the consumer data services marketplace today is to obtain the consumer's credentials and use them to satisfy the financial institution's authentication requirements. The proliferation of consumer credentials being held by different entities in the data services ecosystem increases the security risks to consumers. New technologies like OAuth offer improvements to this practice by using techniques – such as tokenization – that permit authentication without the need for a data aggregator or other institution to obtain and store a consumer's credentials.

Data Access Technologies: Companies that obtain consumer financial data from their financial institutions have employed one of two approaches: screen scraping and the Open Financial Exchange protocol ("OFX"). New access technologies are being explored and implemented, with a primary focus on Application Programming Interfaces ("APIs").

Screen Scraping. Screen scraping refers to the practice of collecting – or scraping – data from the consumer's account information environment. As noted above, in order to enter the consumer's account portal, data aggregators obtain the consumer's authentication credentials, proffer these credentials to the consumer's financial institution as though the data aggregator is the consumer itself, and thereby obtain access to, and scrape out, any data that is available to the consumer through that environment, irrespective of whether the portal is limited to the single financial account that the consumer permissioned, or contains multiple accounts for that consumer. Also as noted above, consumers are not made well aware of the use of screen scraping or how the provision of authentication credentials for use in screen scraping may affect the consumers' legal rights. In addition, the high traffic load that gets placed onto the screen-scraped institution's infrastructure increases the costs for managing its infrastructure, and this traffic and cost load continues to increase as more consumers use data aggregation. Moreover, screen-scraped institutions are required to use inefficient techniques such as IP whitelists for trusted intermediaries to enable consumers to obtain their data through this access technology. Needless to say, given these significant risks, marketplace participants are largely aligned on the need to transition from screen scraping to a more secure, transparent, and efficient access technology.

---

[47] FFIEC, *Authentication in an Internet Banking Environment* (Oct. 12, 2005), available at http://ithandbook.ffiec.gov/media/54001/04-25-11_06-28-11_-_bulletin_and_supplement_combined.pdf; FFIEC, Authentication in an Electronic Banking Environment (Aug. 8, 2001) available at http://ithandbook.ffiec.gov/media/resources/3456/occ-bul_2005-35.pdf

[48] Id.

OFX. OFX is a data transmission specification that has been incorporated by thousands of financial institutions in the United States. OFX recommends the use of OAuth as an authentication technology in its latest standards. While OFX can be more secure than screen scraping, it can be implemented in multiple ways and standards cannot be enforced, which creates areas for improvement. OFX requires technical experts to enable implementation. In addition, OFX standards have not been updated to support all modern technologies and needs. Apart from technical limitations, the commonplace practice through OFX is for data aggregators to obtain and store all data that have access to for that consumer, regardless of whether the consumer and its requesting institution having asked only for a subset of the data.

APIs. API refers to a set of routines, protocols and tools for building software applications. An API for a particular routine can easily be inserted into code that uses that API in the software. APIs are extremely prevalent in technology today. Google Maps is a common example of an API that has been inserted into the software of many other companies. An API that facilitates the transfer of consumer financial data coupled with an authentication technology such as OAuth would provide a far more secure, efficient, and scalable platform over today's methods of obtaining consumer financial data.

2. *Ubiquity: Are existing transfer and authorization technologies mechanisms ubiquitous enough to meet the definition of data in a machine readable format or must the CFPB issue technical standards to meet the definition of machine readable?*

We do not believe the CFPB should issue technical standards. Existing transfer and authorization technologies, such as APIs and OAuth, permit the transfer of information using commonly known systems that are easy to implement by technology system engineers.

3. *Legal Risks: How should the marketplace and the CFPB clarify legal responsibilities for the marketplace participants when consumers have permissioned a third party to obtain its consumer financial data?*

We believe the TCH Whitepaper provides a robust analysis of the legal issues regarding consumer-permissioned data access and legal clarifications that are needed.[49] In addition, we believe that marketplace participants should remain free to clarify legal liabilities by contract to the extent permissible by existing law and regulation.

[49] See, e.g., TCH Whitepaper.

4. *Applicability of Access Right: To whom does section 1033 of the Dodd-Frank Act apply?*

We believe that consumers should have a comprehensive right to access their consumer financial data from their consumer financial product or service provider. Consistent with the TCH comment letter, however, we do not believe that section 1033 mandates that banks provide access to their customers' financial data via data aggregators and other third parties. To the extent that such information is provided, it should be done under written contracts between the bank and the third party to ensure the terms of any such arrangements are fully delineated and undertaken in full compliance with the laws governing consumer protection, privacy and data security. We believe that the CFPB could clarify the scope of section 1033 of the Dodd-Frank Act to identify all entities that fall within the scope of the consumer right of access and ensure that those entities have an opportunity to provide their views to the CFPB on a timely basis.

5. *Section 1033 Data Elements: What are the section 1033 data elements that a consumer has the right to access?*

Financial institutions provide differing levels of information to their customers through their banking technologies. For example, certain financial institutions offer their customers different levels of capabilities for personal financial management tools, such as setting budgets, creating automatic savings tools, and conducting assessments of financial decisions, such as how much of a monthly home mortgage payment could a customer afford. One of the foundational questions for section 1033 of the Dodd-Frank Act concerns which data elements fall within the section 1033 consumer right of access. One potential interpretation is that the section 1033 consumer right of access should include any and all data that a covered entity makes available to the customer. Such an expansive position would create disincentives for institutions to invest in new and innovative capabilities with respect to their customer's data, because the value of their investment would be easily and immediately transferred to other institutions that obtain that data. This would work at cross-purposes to the CFPB's goal to promote innovations in consumer financial product and services. The CFPB should be careful in approaching this question, in order to ensure that all institutions, regardless of size and technical sophistication, will be able to provide a consistent type and amount of data regarding their customers, and will result in all institutions retaining the incentive to continue to provide innovations in data and other services to their customers.

6. *Cost: Must 1033 data elements be transferred for free to the consumer or may they be transferred to the consumer at cost, or on a cost plus basis?*

Consumers have a statutory right to access their data under section 1033 of the Dodd-Frank Act. The statute is silent on the cost of the transmission of that data. In the current marketplace, the transfer of a consumer's financial data begins when the consumer requests a company to access that consumer's data from a different financial institution. The company that receives that request commonly employs a data aggregator

to obtain the consumer's data and provides the data aggregator with the consumer's credentials to enable the data aggregator to screen scrape the consumer's data or obtain the data through a structured feed, like OFX. In each case, financial institutions provide the consumer's data to data aggregators at no cost. Data aggregators, however, charge the original requesting company a fee to obtain the data that the data aggregator obtained for free.

These marketplace characteristics are at risk of rent-seeking behavior at the expense of the consumer's best interests. The cost of the consumer's section 1033 data is completely dependent on the revenue and profit requirements of the data aggregators. In addition, the market could further fracture (for instance, through the emergence of a new class of data aggregator that specializes in personal investment data) and lead to elongated chains of transfer and subsequent "value additions" by companies in the chain of transfer, with the result that consumers may face spiraling costs to obtain their data under the consumer right to access their data in section 1033. We believe the cost dynamics of the marketplace are not in equilibrium, and that the 1033 data elements should be transferred either for free or at cost to the consumer. In this way, consumers never pay more than cost to obtain their data, no matter how long the chain of transfer has become, and market participants will not be incentivized to charge for the data or make "value additions" to the data that are intended solely to capture revenue. Moreover, the CFPB should through advisory opinions and guidance address how to impose that structure equally across all market participants, so that if any market participant is entitled to charge cost for the production of data, then all market participants in the chain of transfer are entitled to charge cost for the production of data.

We recommend that the CFPB continue to work with industry, consumer, and regulatory stakeholders in an open and transparent manner to continue to inform the CFPB on issues specific to section 1033, inclusive of the questions above. While we believe that the CFPB should follow the recommendations above prior to considering whether to impose any new regulations or binding standards under section 1033 of the Dodd-Frank Act, we recommend that the CFPB formally begin consultation with Federal banking agencies (such as the OCC) and the FTC under section 1033(e) of the Dodd-Frank Act. In particular, the Federal banking agencies would be able to share their perspectives on safety and soundness, reputational risk, and trust in the banking industry with respect to practices in the consumer financial data services marketplace.

Conclusion

Once again, Capital One would like to express its appreciation to the CFPB for formally and publicly examining important developments in the market for consumer financial data. We hope that the comments and recommendations provided in this letter are useful to the CFPB. Please do not hesitate to contact the undersigned for any reason.

Sincerely,

Meredith Fuchs, Senior Vice President &
Chief Counsel, Regulatory Advisory
(703) 720-2526

Andres L. Navarrete, Executive Vice
President, External Affairs
(703) 720-2266

cc (by email):

Don Busick, SVP, Digital Product Management
Rebecca Heironimus, VP, Digital Product Management
Al Ciafre, MVP, Regulatory Relations
Sebastian Astrada, Senior Director, Regulatory Relations
Eulonda Skyles, Director, Regulatory Advisory