Section 1033 of Dodd-Frank—A Decade of Waiting for the Green Flag to Drop

Thomas P. Brown[1]

Most style guides recommend against titling a paper with an allusion to a sports analogy. Sports analogies often reflect cultural biases and may not convey information as clearly as the author intends. But recommendations about writing fall in the category of what the the noted pirate and philosopher, Hector Barbossa, describes as "guidelines" rather than "rules."[2] And the image of financial institution logos crowding a race track waiting for the Green Flag to drop so that they can start racing under a new set of rules captures, from my perspective, the dilemma around Section 1033. The consumer financial services industry has been waiting a long time for the Consumer Financial Protection Bureau ("CFPB" or the "Bureau") to drop the flag and signal that yes, in fact, every consumer financial institution in the United States is required, as a matter of federal law, to make information about consumers and their accounts available to identified third parties in electronic form upon consumer request. I am writing to urge the Bureau to take that step.

Before laying out precisely what I believe the Bureau should do and explaining why I believe the Bureau should do it, I want to thank Director Kraninger, Assistant Director Wade-Gery, and the rest of the team at the Bureau for pulling together this Symposium and inviting me to speak. The issue of consumer permissioned data is one in which I have been interested since I stumbled upon Section 1033 a decade ago as I, like every other lawyer with an interest in the consumer financial services industry, was parsing the massive text of Dodd-Frank. I remember being surprised to see it. Unlike the other major provisions of the statute, it had received almost no attention in the lead up to the enactment of bill. Indeed, when I reached out to friends whom I believed had played a part in drafting the broader text, no one could identify the inspiration for Section 1033. But I thought then, and still think today, that the legislative fragment could be as consequential for U.S. consumers of financial services as anything else in the statute. I recognize that this is a bold assertion given that Dodd-Frank was the most significant overhaul of the regulatory framework for financial services in this country since the Great Depression. I also recognize that the questions posed by the Bureau about Section 1033 do not, at least directly, seek comment on whether consumer-permissioned data access is an important issue. But I think that answering the questions posed by the Bureau about 1033, particularly those directed at the third panel, requires at least some discussion of why the issue matters.

Consumer-permissioned data access matters, from my perspective, because it has the potential to address the core conundrum that makes consumer protection such a difficult problem in the consumer financial services industry—that in many parts of the sprawling consumer financial services industry, consumers are not customers but are, instead, the product that is being served up. This means that although consumers are a key constituent of many markets that make up the industry, their choices do not directly impact the behavior of many of the industry's key service providers. Consumer protection concerns are, thus, a chronic problem. Economists long ago recognized that voice in the sense of complaint is a substitute for exit.[3] Consumers complain about financial service providers because they

---

[1] Mr. Brown is a partner at a major international law firm. He and the firm represent a number of companies with an interest the issues raised by Section 1033 of Dodd-Frank. The views expressed in this submission are his alone, however, and they do not represent the views of the firm or any of its clients. Mr. Brown wants to thank his colleague, Ms. Shreya Gupta, for her help in preparing this submission.

[2] *PIRATES OF THE CARIBBEAN*. (DK Publishing 2003).

[3] Albert O. Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (1970).

often have no alternative. Exit is not an option either as legal matter or a practical matter. However, consumer-permissioned access to information provides an alternative to both exit and complaint.

The remainder of this submission proceeds as follows. Part 1 provides a high level sketch of why competition does not work to protect consumer interests in all segments of the consumer financial services industry. Part 2 explains how consumer-permissioned access to information serves as a partial substitute for exit. Part 3 discusses the information security and privacy issues raised by consumer-permissioned access. Part 4 addresses the specific questions identified by the CFPB for the third panel at its upcoming symposium.

I. Competition in the Consumer Financial Services Industry Does Not Always Work To Benefit Consumers

Consumers may be the axis around which the consumer financial services industry revolves, but they are not always the dimension on which rival service providers compete. Moreover, even where consumers may initiate a relationship with a financial services provider, they may find themselves with little recourse to discipline the behavior of a chosen service provider once a relationship has been established.

The classic example of a financial relationship that is much easier to initiate than exit is the relationship between a consumer and her checking account provider. As consumer groups have documented, once a consumer establishes a deposit relationship with a bank, it is very difficult for the consumer to exit that relationship.[4] Direct deposit relationships and auto-pay transactions do not immediately transition from one institution to another. The problem becomes even more severe for joint accounts. The process of switching a core deposit relationship from one institution to another can take months and cost the consumer hundreds of dollars in fees.

Although the checking account may be the consumer's most important financial relationship, it is not the only one. Over the course of their financial lives, consumers will have relationships with financial institutions that were chosen *for* them not *by* them. Consumers do not choose the firms that service their mortgages, collect their debts, maintain their credit files, or collect their online bill payments. In each instance, those service providers are chosen by a third-party with an independent interest in the interaction with the consumer. The interest of those parties may overlap with the interests of the consumer, but they do not always align. And in some instances, such as debt collection and mortgage servicing, the interests of the service provider may conflict with the interests of the consumer.[5]

Not surprisingly, many segments of the consumer financial services industry exhibit the characteristics of industries in which consumers have little choice. The two classic indicia of industries that suffer from

---

[4] *See generally*, *Trapped at the Bank: Removing Obstacles to Consumer Choice in Banking*, Consumers Union (May 30, 2012), http://consumersunion.org/wp-content/uploads/2013/09/TrappedAtTheBank1.pdf; Kevin Wack, *The Big Switch: Just How Hard Is It to Change Banks?* AM. BANKER, Oct. 25, 2011, http://www.americanbanker.com/issues/176_207/debit-card-fees-Bank-of-America-BofA-interchange-1043494-1.html.

[5] Ron Lieber, *Don't Like Your Mortgage Servicer? Good Luck Trying to Switch*, (Feb. 16, 2018) (available at https://www.nytimes.com/2018/02/16/your-money/wells-fargo-mortgage-switch.html?referringSource=articleShare).

some kind of market failure are complaints and lock-in. Many, many segments of the consumer financial service industry display both indicia.

First, consumers complain consistently and in great numbers about firms in the industry—namely debt collectors, credit bureaus, and mortgage servicers.[6] They also pay billions of dollars in nuisance fees. The $17 billion to $34 billion in overdraft fees and insufficient funds fees that banks and credit unions collect from consumers are the single best example, but they are just an example.[7] Banks, according to a McKinsey study of the FinTech boom, generate a higher percentage of their profits and a much greater return on equity from fee based income than they generate from making their balance sheets available.[8]

Second, the general regulatory framework for the industry—particularly banks and credit unions—purposely inhibits consumers from easily moving financial relationships from one institution to another. Bank business models are built around the time lag between when a consumer places a deposit at a financial institution and when the consumer seeks to use the funds associated with the deposit. This, as I have noted elsewhere, means that competition has a double edge within the industry.[9] Competition in the financial services industry has the same salutary effects as in other industries—e.g., increased output, lower prices—but it also makes individual institutions less stable. Under certain circumstances, institutional instability can become systemic. To a large extent, the entire bank regulatory system is designed to protect banks from too much competition among themselves and with non-banks.[10]

II. Consumer-Permissioned Data Access Provides Consumers With An Alternative To Both Complaint And Exit

Consumer-permissioned access to data provides an alternative to voicing complaint on the one hand and unbridled competition on the other hand. By allowing third parties access to information about their accounts, consumers can provide third parties with real time access to the information that arises from the interaction with service providers in the space. Those third parties may be able to help ensure that consumers receive the services to which they are entitled at the time of their interaction with those service providers rather than having to obtain a remedy after the fact. Permissioned access to data is not a perfect substitute for exit. Debt collectors, for example, are unlikely to ever act wholly in the interest of the consumer that has not paid an outstanding debt. But it is a partial one. It also enables consumers to take greater control of their financial lives.

---

[6] CFPB, Consumer Complaint Database (visited February 12, 2020) (noting that the top three sources of consumer complaint data are debt collection, credit bureaus, and mortgage servicing) (available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?from=0&searchField=all&searchText=&size=25&sort=created_date_desc).

[7] *See* A Closer Look: Overdraft and the Impact of Opting-In at 1, CFPB (Jan. 2017), https://files.consumerfinance.gov/f/documents/201701_cfpb_Overdraft-and-Impact-of-Opting-In.pdf (estimating annual consumer overdraft and insufficient funds fees to be $17 billion); Maria Lamagna, "Overdraft Fees Haven't Been this Bad Since the Great Recession", MARKETWATCH, Apr. 2, 2018, https://www.marketwatch.com/story/overdraft-fees-havent-been-this-bad-since-the-great-recession-2018-03-27 citing Moebs Services research (estimating consumer overdraft fees in 2017 to be over $34 billion).

[8] McKinsey Global Banking Practice, *Cutting Through The FinTech Noise: Markers of Success, Imperatives For Banks* 4 (2015).

[9] Thomas P. Brown, *Of Bitcoin and Banks*, Concurrences, Comp. L. Rev. 34 (2019).

[10] *See* M. C. Keeley, *Deposit Insurance, Risk and Market Power in Banking*, 80 Am. Econ. Rev. 1183 (1990) (discussing the "franchise value" paradigm in bank regulation).

By providing third parties with access to information about their accounts, consumers can protect themselves against the nuisance fees imposed by their providers. With access to information about a user's core deposit account and the ability to move funds instantly into a consumer's account, a company like Digit can, for example, move money from an emergency savings account to the consumer's core deposit account to protect the consumer against an anticipated overdraft.[11]

The benefits of such services go beyond avoiding nuisance fees, however. Over the course of the last decade, a raft of companies have sprouted on the periphery of the financial services industry to enable consumers to better manage their financial lives. Some of these services help consumers save money automatically. Others help consumers match the timing of their bill payments to the delivery of their paycheck. Others have expanded access to credit by allowing consumers to supplement information visible on a credit report with direct visibility into their income and expenses. Still others, as in the debt collection example above, provide consumers with help in the course of the interaction with service providers for which the consumer is not a customer.[12]

All of these companies are premised on consumer access to financial data. Autonomous personal financial advisers require access to consumer deposit accounts to advise on savings and spending decisions. Digital investment management services require access to investment accounts to determine when consumers should make changes to their portfolios. Lenders hoping to underwrite individuals overlooked by FICO need income and expense data that is only visible through a checking account.[13]

The benefits of data access are not lost on the banking industry. Banks share detailed transaction data with one another through services that they manage on a cooperative basis but that are closed to non-banks. Indeed, the entire retail payment infrastructure built and maintained by Visa and MasterCard operates on a bank-permissioned basis. And a number of depository institutions have sought to enhance the services that they offer by adding features that require access to information about accounts provided by other depository institutions.

Other regulators have recognized the competitive benefits that flow from third-party data access. In advocating for the creation of a consumer-permissioned data access regime in the United Kingdom, HM Treasury observed that such a regime

> will further increase consumer engagement by making it even easier for customers to see where they could get a better deal, meaning banks will have to work harder to win and retain customers. It will also increase competitive intensity by supporting the growth of technology that can be adopted by banks and non-bank providers to compete to offer new products.[14]

III. Existing Technology and Law Provide Ways to Address the Information Security And Privacy Issues Raised by Consumer-Permissioned Data Access

---

[11] Hello Digit, Inc., https://digit.co/.

[12] *See* e.g., Even Responsible Finance, Inc., https://even.me/; Acorns Grow, Inc., https://www.acorns.com/; FinRegLab, *The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings* (2019) (available at https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf).

[13] FinRegLab, *The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings* (2019) (available at https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf).

[14] *Banking for the 21st Century: Driving Competition and Choice* at 6, HM Treasury, (Mar. 2015), http://www.finextra.com/finextra-downloads/newsdocs/Banking_for_the_21st_Century_17.03_19_40_FINAL.pdf.

Allowing third parties to access to sensitive consumer information does raise issues. The two most significant, at least for present purposes, are information security and privacy. Financial institutions have deployed technology in other segments of the financial services industry that could address the security issues that arise around consumer-permissioned data access. And The Gramm-Leach-Blilely Act ("GLBA"), provides a well-established framework for managing the privacy issues that arise from the movement of sensitive financial information. There may be room to improve that framework, but the passing of information between institutions with consumer permission does not raise new issues.

The chief risk presented by expanding access to financial data is the possibility of an unauthorized transaction. Based on anecdotal reports, credential sharing remains the predominant way that consumers permit third parties to access information about their accounts. In many instances, the account identifying information and passwords that consumers share with third parties can be used both to access information and initiate a transaction.

This practice, under existing regulations, creates risks for both the consumer and her financial institution. The consumer risk arises if the person to whom the consumer gave her account credentials uses them outside of the permission granted by the consumer. Although the Electronic Funds Transfer Act generally protects the consumer against unauthorized transactions, that protection does not extend to situations in which the consumer gives a third party the underlying credentials but purports to limit what the recipient can do with them.[15] The risk to the underlying financial institution arises from the possibility that some third party might obtain the credential from the consumer's original designee. If, for example, the party authorized by the consumer to use her credential suffered a security breach and the thief then used the credentials to initiate transactions, the financial institution would be on the hook.[16]

Technology can mitigate and possibly eliminate these risks. The credential that a consumer uses to delegate access to information does not need to be the same as the one she uses to initiate a transaction. Banks could give consumers an alternate credential—or token—that consumers could then pass to parties that they want to have information access but not transaction access. In fact, banks have already deployed sophisticated tokenization systems in the payment industry to protect against precisely these types of risks. Banks in Europe, including Agricole Bank and Fidor Bank, are testing the OAuth specification which enables banks to keep ownership of customer log-in data but requires them to make available an API for third party developers.[17]

Data sharing also raises privacy concerns. Banks are generally forbidden from sharing a consumer's personal financial data with third parties without the consumer's express consent/authorization. Under the GLBA, the restrictions on the use of financial data generally run with data, meaning that a party that receives sensitive financial data about a consumer generally must abide by the same rules as a bank.[18]

---

[15] See 12 CFR 1005.2(m)(1); 12 CFR Part 1005, Supp. I, Cmt. 2(m)(2).

[16] 12 CFR § 1005.2(m)(1) (clarifying that the definition of "unauthorized electronic funds transfer" does not include "…an electronic funds transfer initiated:…[b]y a person who was furnished the access device to the consumer's account by the consumer….").

[17] *See, e.g.*, Mary Wisniewski, *Is It Time to End Screen Scraping?* AMERICAN BANKER, (Nov. 7, 2014), http://www.americanbanker.com/news/technology/is-it-time-to-end-screen-scraping-1071118-1.html.

[18] See 15 U.S.C. § 6802(c); 12 CFR 1016.11.

With that said, there are differences between the supervisory regimes for banks and non-banks.[19] Banks are supervised by a raft of regulators. Some non-banks are as well, though others are not. It is not clear that supervision actually leads to better outcomes with regard to information security or privacy issues than enforcement regimes. Moreover, the entity chiefly responsible for protecting consumers from issues arising in their interactions with non-banks and the lead privacy regulator for those institutions, the CFPB, does not have an office dedicated to privacy.[20]

Technology can help here as well. Financial Institutions could share information through APIs. Such a regime could require consumers to provide express consent with regard to the precise data fields accessible by third parties. Indeed, borrowing techniques developed in the payment industry, data sharing could be limited to one-time access.

The larger point is that the United States has an established regulatory framework for dealing with the privacy issues that arise from financial information. There may be room to improve that regulatory framework—e.g., devoting resources to the topic within the CFPB or make other changes to existing law. But the CFPB should not further delay clarifying that Section 1033 is effective now while debates about whether it is necessary to make changes to the generally applicable laws that protect consumer interests in the privacy of their financial information.

IV. Answering the Questions Asked by the Bureau

What areas of regulatory uncertainty persist in this market?

The principal area of uncertainty under Section 1033 of Dodd-Frank is whether financial institutions, as defined by the statue, must share information in electronic form about the products and services provided to a consumer with the subject consumer and her third party agents upon request by the subject consumer. Although the plain language of the statute compels the conclusion that the answer to this question is yes—as the Treasury Department has agreed[21]—financial institutions continue to take the position that they are not obligated to share information with third parties upon consumer request. The recent decision by PNC to deny consumer requests to share information with Venmo received considerable attention in the press,[22] but it is not the only instance of a financial institution denying a consumer request to share information. At least one dispute has resulted in a lawsuit by a consumer-facing financial services provider to prevent a third party from making a bill payment on a consumer's behalf.[23]

---

[19] Rob Hunter, *Leveling the Playing Field: Ensuring Consumers Are Protected When Using Nonbank Payment Services* (available at https://www.theclearinghouse.org/banking-perspectives/2015/2015-q2-banking-perspectives/articles/payments-risk).

[20] *See* Bureau Structure, Aug. 26 2019 (available at https://www.consumerfinance.gov/about-us/the-bureau/bureau-structure/).

[21] A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation, Dep't of the Treasury, Report to President Donald J. Trump (July 2018), https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

[22] See, e.g., Kate Rooney, "PNC's Fight with Venmo Highlights Bigger Issue Over Who Owns Your Banking Data, CNBC.com, Dec. 16, 2019, https://www.cnbc.com/2019/12/16/venmo-and-pncs-fight-over-sharing-consumer-financial-data.html.

[23] Complaint, *SpeedPay, Inc. v. BillGO, Inc*., 2:19-cv-20274 (D. N. J. Nov. 14, 2019).

Are any of these areas retarding the development of a competitive and vibrant market? If so, how?

As explained above, many consumer financial services markets are not responsive to consumer demand and are, thus, not "competitive" or "vibrant" when viewed from the perspective of the consumer. In some instances, the lack of competition is a product of regulatory design. In other instances, service providers answer to parties other than consumers such as mortgage holders in the case of loan services, potential lenders or other users of consumer reports in the case of the credit reporting companies, or holders of unpaid debt in the case of debt collectors. Ensuring that consumers can provide third parties with access to information about the services and products provided to them would help to remedy the regulatory and structural barriers that prevent many consumer financial services markets from responding to consumer demand.

How should the Bureau tackle such areas? With what regulatory tools? With what substantive content?

The Bureau should issue a rule that does two things: (1) ends the debate about whether Section 1033 of Dodd Frank is effective and (2) makes clear that Section 1033 requires a financial institution to share information about a consumer's account with a third-party when instructed by the consumer.

The Bureau has the authority to issue such a rule without simultaneously prescribing technical standards for standardized data formats. The duty to promulgate a rule, and the duty to provide technical standards, are two separate obligations within the act and do not fall within the same timeline or have any direct dependency on one another.

Section 1033 of the Dodd-Frank Act states that, "[s]ubject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, 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."[24] In another section, the statute also authorizes the Bureau to "prescribe standards … to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section."[25]

An analysis of this language demonstrates that the Bureau can promulgate a rule now that does not include a technical standard. The language "subject to rules prescribed by the Bureau" is not limited by and does not depend on the language in section (d) permitting technical standards. The text thus clearly draws a distinction between the creation of a rule, and the creation of technical standards. There is no command from Congress, anywhere within the statute, that says that any rule issued by the agency pursuant to section (a) must include with it a technical standard.

A simple application of Chevron allows one to reach the same result.[26] Chevron involves a two-step analysis: 1) whether or not the statute's language, and Congress' intent, is ambiguous and, if so, 2) whether the agency's interpretation is reasonable.[27] Here, the statutory language itself is not at all ambiguous. Congress explicitly delegates authority to the CFPB to issue a rule, using the words "subject

[24] *Id.* at 12 U.S.C. § 5533(a).
[25] *Id*. at 5533(d).
[26] *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984).
[27] *Id.* at 843.

to rules prescribed by the Bureau" before providing the requirements of the statute. Therefore, if a rule issued by the Bureau is reviewed, it cannot be found to be an abuse of the Bureau's discretion, because the Bureau is acting under express authority through an unambiguous statute. Any rule issued by the Bureau thus supports Congress's clear intent. As per Chevron, the inquiry must stop there.

However, even to the extent that any such ambiguity exists, such ambiguity can only be as to whether or not this language requires the Bureau to issue a rule in the first place. The Bureau can easily remedy this by clarifying that the language of Section 1033 is self-executing, using the interpretation laid out by the treasury department.

Either way, whether it is issuing guidance that Section 1033 is self-executing, or whether it is promulgating a rule clarifying the duties of financial institutions under the statute, the Bureau need not worry about issuing technical standards at this time.

In what areas can the Bureau continue to rely on non-binding approaches? Does the Bureau need to revise the principles in certain respects?

The Bureau can continue to rely on non-binding approaches to the issue of how financial institutions share information with third parties upon consumer request. There are a number of standards and technologies that financial institutions can use to discharge their responsibilities under Section 1033.[28] The Bureau can also continue to rely on non-binding approaches to govern what types of information falls within the scope of the 1033 obligation.

What should the Bureau's policy-making priorities be in this market over the short term (1 year) and longer term (5 years)?

In the near term, the Bureau's focus should be on ensuring that financial institutions of all kinds comply with the clear mandate expressed in federal law. Ending the debate about whether financial institutions are required to share information with third parties upon consumer request will allow the industry to tackle other issues related to information sharing, including what technology should be used to facilitate consumer-directed data sharing.

Over the longer term, the Bureau should monitor whether other rules need to be updated to reflect risks to consumers that might arise from access to account level information. The near term risks associated with data access are likely associated with the rather informal way that consumers currently permission data access—i.e., screen scraping. As discussed above, technology widely used by consumer financial service providers in other other contexts is capable of solving these problems.

How should other regulators tackle areas of regulatory uncertainty? Do they need to clarify or change their own regulatory standards in this area? In what areas could regulators usefully provide interagency guidance?

The CFPB is not, of course, the only regulator with authority over consumer financial services providers. Other federal and state regulators have broad authority over banks, credit unions, broker dealers, investment advisors, and others that provide or supply consumer financial services to consumers within the meaning of Section 1033. The CFPB should work with those regulators to ensure that covered

[28] See ISO 20022 (available at https://www.iso20022.org/).

financial institutions are discharging their responsibilities under Section 1033. At a minimum, the CFPB should advocate through its role on the FFIEC that the FFIEC examination manual be updated to include a section outlining examination standards to ensure compliance with Section 1033.[29]

[29] About the FFIEC, (available at https://www.ffiec.gov/about.htm).