MERCATUS CENTER
George Mason University

TESTIMONY

# STATEMENT REGARDING CFPB DODD-FRANK SECTION 1033 SYMPOSIUM

**Brian Knight**
*Director and Senior Research Fellow, Program on Innovation and Governance, Mercatus Center at George Mason University*

Consumer Financial Protection Bureau

February 26, 2020

Section 1033 of the Dodd–Frank Wall Street Reform and Consumer Protection Act is, at first glance, a relatively noncontroversial section in an otherwise highly controversial title of an extremely controversial law.[1] At the surface, all 1033 seems to do is grant consumers a right to access a portion of the data held by a covered firm related to their transactions and accounts in a usable electronic format. Not a big deal, right? Well, as with seemingly all things Dodd-Frank, the answer is more complex, because this section could dramatically change the balance of power in the market for financial services. Section 1033 poses some significant and challenging questions that policymakers should consider; I would like to highlight a few of them and make some very modest suggestions for next steps the Consumer Financial Protection Bureau (CFPB) should take.

In my opinion Dodd-Frank Section 1033 presents at least three major questions that the CFPB will need to resolve:

1. Does Section 1033 extend only to customers themselves or do the access rights it provides extend to customers' agents? What about data aggregators who are relied upon by agent firms but frequently lack a relationship with customers themselves?
2. If Section 1033 does extend to customers' agents, does it allow covered financial services firms any ability to condition access in order to protect customer data or prevent fraudulent transactions, or must firms take all comers? Can the CFPB place limits on data access, and if so, how much latitude does the CFPB have?
3. How must liability be allocated among customers, their agents, aggregators, and covered financial institutions under existing law? How does this allocation of liability differ from an ideal or appropriate allocation?

## DOES SECTION 1033 EXTEND TO CUSTOMERS' AGENTS?

Because of advances in technology, changing consumer expectations, and legal ambiguity, Section 1033 presents a significant question because it may require banks and other covered financial firms to provide access to records to not only their customers, but to the agents of those customers. These agents include not only "fintech" firms, including some quite large firms, but also aggregators who

1. Dodd–Frank Wall Street Reform and Consumer Protection Act § 1033, 12 U.S.C. § 5533 (2018).

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

operate behind the scenes. These technological innovations offer the possibility to empower consumers to better monitor and control their financial lives and potentially be more effective shoppers for financial services. While this access has the potential to enable significant gains in innovation and competition, there are also real concerns for data security, privacy, and fairness.

Of course, there is debate about just what Section 1033 actually requires. While it is clear that covered firms must provide customers with certain records in a usable electronic format, there is disagreement as to whether the law extends that obligation to customers' agents, such as firms that seeks to serve customers by giving them a consolidated picture of their financial lives across all of their accounts, or by possibly allowing customers to transact with multiple financial services firms through a common platform. Further complicating matters is the fact that many of these agent firms also rely on data aggregators, who lack a direct relationship with customers.

At present one of the methods used by agent firms and data aggregators is "screen scraping," where, at customers' behest, firms use credentials provided by customers to access the website of a financial services firm and obtain account information. This practice is broadly seen as suboptimal and a security risk, since it requires the customer to disclose sensitive account information to a third party that then needs to store it on its servers, presenting an additional and potentially tempting target for criminals.

More recently there have been collaborative efforts between financial services firms and intermediaries to create direct access to customer data through the use of application programming interfaces (APIs). APIs present a more secure and robust method of obtaining data, but concerns have been raised by agent firms and aggregators that financial services firms will unduly limit the type of data available or will cut off access periodically. This highlights why resolving the ambiguity of the scope of Dodd-Frank Section 1033 is important. If agent firms do not have a right to access customer data, then the terms of access will be dictated by contract (where access is granted at all) and the relative contracting power of the parties, which may grant incumbent financial services firms, especially large ones, a significant advantage. If, conversely, agent firms have a right under Section 1033 to access customers' data, then financial services firms will presumably be forced to provide access largely without limitation (save for the limits included in the law) or interruption. The US Department of the Treasury, based on the expansive definition of "consumer" in Dodd-Frank that includes agents acting on behalf of individuals,[2] has taken the position that the law requires agent access and recommends that the CFPB reaffirm as much.[3] However, the CFPB has yet to take a firm position, rendering the exact allocation of rights and obligations ambiguous.

## IF SECTION 1033 DOES EXTEND BEYOND THE CUSTOMER, WHAT LIMITATIONS ON ACCESS ARE PERMISSIBLE?

If Section 1033 does in fact require agent access, a host of other questions then emerge. First among them is, "On what terms?" Must a covered financial services firm provide access to *any* agent, no matter how incompetent or dubious an agent is? Are aggregators (who generally do not have a direct relationship with the consumer) covered by Section 1033, or is it only those firms who have a direct relationship and receive specific authorization from a covered firm's customer? If the CFPB adopts the agent-access view, what, if any, limits can it place on access rights? While access is "subject to rules prescribed by the Bureau"[4] it is unclear how far that can stretch to potentially interfere with a customer's agent obtaining records. Likewise, while the CFPB can promulgate data standards,[5] it does

2. 12 U.S.C. § 5481(4) (2018).
3. Steven T. Mnuchin and Craig S. Phillips, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation* (Washington, DC: US Department of the Treasury, 2018), 31.
4. 12 U.S.C. § 5533(a) (2018).
5. 12 U.S.C. § 5533(d) (2018).

not appear that it can mandate the use of any specific technology.[6] This leaves open the question of how far the CFPB could go in placing limits on customers'—and by extension the agents of their choices'—right to access records.

## IMPLEMENTATION OF SECTION 1033 NEEDS CLARIFICATION OF SCOPE OF LIABILITY

Further, if Section 1033 does mandate agent access it will potentially exacerbate questions of liability and fairness, since banks will be forced to open up their systems to firms not of their choosing, and they will be forced to do so potentially without the ability to impose reasonable requirements to safeguard customer data. Under existing law banks are frequently required to reimburse customers in the event of fraudulent transfers.[7] While cases of screen scraping may potentially absolve the bank of liability under Regulation E, as a legal matter in certain circumstances,[8] there are numerous cases where liability would likely still apply.[9] Even in cases where covered financial institutions are not technically liable, there would likely still be significant pressure on the covered financial services firm to make the customer whole. Less clear is the liability distribution in cases where covered financial services firms are obligated to make data available to customers' agents via a different method that does not involve customers providing agents with their login credentials.

While banks may be able to currently rely on contractual allocations of liability for firms they have agreements with and tort principles in cases where a breach or fraudulent transaction is the result of an agent firm or aggregator's negligence, it is not clear whether these will be sufficient. First, in a scenario where banks are legally required to provide access to data to the agent of a customer's choosing, it is unlikely that banks will be able to meaningfully contract away liability risk. Second, to the extent that an agent firm or aggregator is insufficiently capitalized to sustain a judgment, the bank may end up bearing the cost of fraudulent transactions even if it prevails in court.

## CONCLUSION

As the CFPB ponders how it must proceed on Section 1033, it should keep these concerns in mind. None of this is to say that the benefits of greater access are on net not worth the costs, but mandatory access does potentially pose significant issues of fairness and liability.

The existing ambiguity may be distorting the market's development. To be clear, this isn't to say that exciting innovation isn't happening or that banks and tech firms aren't responding to market incentives. Rather, given the fact that Section 1033 exists but that its scope is unclear and its resolution may have knock-on effects for other regulatory requirements, it is possible that the market is maladapting, and it risks a shock if the ambiguity is resolved later in a way that unsettles expectations. As such, the CFPB may wish to consider rulemaking to clarify the scope of Section 1033. It should also consider clarifying the extent to which the Electronic Funds Transfer Act and Regulation E exempt covered financial services institutions from liability in cases where customers have provided their account information to a third-party agent. The CFPB may also wish to consider the extent to which it is statutorily permitted to allow covered financial services institutions to condition access in order to provide reasonable and appropriate safeguards for consumer data and prevent fraud. In doing this the CFPB should, as required by law, coordinate with federal bank regulators and the Federal Trade Commission. To the extent the CFPB believes that it lacks appropriate authority, it should highlight this issue for Congress.

---

6. 12 U.S.C. § 5533(e)(3) (2018).
7. Bureau of Consumer Financial Protection, Electronic Fund Transfers (Regulation E), 12 C.F.R. § 1005.6 (2019); Bureau of Consumer Financial Protection, Truth in Lending (Regulation Z), 12 C.F.R. § 1026.12 (2019).
8. Bureau of Consumer Financial Protection, Electronic Fund Transfers (Regulation E), 12 C.F.R. § 1005.2(m)(1) (2019); Ann S. Spiotto, "Financial Account Aggregation: The Liability Perspective," *Fordham Journal of Corporate & Financial Law* 8, no. 2 (2003): 557, 586–87.
9. Spiotto, "Financial Account Aggregation: The Liability Perspective."

The CFPB may also wish to change its principle regarding third-party data retention to not discourage third parties from retaining and using consumer data more broadly, provided that consumers make informed choices to allow third parties to do so and can revoke that permission. This may encourage third parties to offer more diverse products and services with different cost structures to suit more customers' needs. Beyond resolving these ambiguities, however, the CFPB should adopt a wait-and-see posture and observe how the market develops, while relying on traditional consumer protection principles as needed. This will allow market processes to evolve over time to meet customer needs and will minimize risk of the CFPB exceeding its authority.

Section 1033 presents novel issues that will be challenging to resolve. It is incumbent on the CFPB to obey the law, exercise due care and humility while providing regulatory clarity, and avoid undue or excessive regulation while providing appropriate consumer protection.