CONSUMER FINANCIAL PROTECTION BUREAU | JULY 2020

Bureau Symposium: Consumer Access to Financial Records

A summary of the proceedings

Consumer Financial Protection Bureau

Introduction

In February of this year, the Bureau of Consumer Financial Protection (Bureau) held a symposium on "Consumer Access to Financial Records" (Symposium).[1] This event marked the fourth in the Bureau's ongoing series of symposia aimed at stimulating a proactive and transparent dialogue to assist the Bureau in its policy development process, including possible future rulemakings.

Dodd-Frank Section 1033 (section 1033), 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…in an electronic form usable by consumers."[2] The Bureau has consistently noted that consumers' ability to access their financial records in electronic form empowers them to better monitor their finances, and that their ability to permission a third party to access those records may enable consumer-friendly innovation in financial services. Companies or other third parties that consumers permission to access their digital financial records can aggregate and use those records to offer new products and services aimed at making it easier, cheaper, or more efficient for consumers to manage their financial lives. At the same time, this kind of expanded access to consumer financial records raises a number of concerns, particularly with respect to data security, privacy, and unauthorized access.

The Bureau's activities to better understand and inform the developing market around consumers' ability to access and permission access to their data prior to the Symposium included, most notably:

- Solicitation of feedback from market participants and observers in a public Request for Information (RFI);[3]

[1] https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/

[2] 12 U.S.C. § 5533(a).

[3] https://www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records

- Publishing a summary of the responses to that RFI with other insightful stakeholder input;[4] and
- Developing a set of "Consumer Protection Principles" intended to help foster the development of innovative financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives.[5]

As the Bureau considers and develops its next steps following the Symposium, it has carefully reviewed the written and oral views provided by Symposium participants. To facilitate further dialogue around these issues and increase transparency, the Bureau is here summarizing its understanding of key facts, issues, and points of contention raised at the Symposium. Specifically, the Bureau is highlighting views stakeholders provided on the following subject categories:

- Data access and scope;
- Credential-based access and "screen scraping";
- Disclosure and informed consent;
- Privacy;
- Transparency and control;
- Security and data minimization;
- Accuracy, disputes, and accountability; and
- Panelist commentary on legal issues.

Views from the participants' written submissions and all three panels that composed the Symposium are summarized below solely by topic area. When appropriate, reference to specific participants or groups of participants is made according to the following shorthand:[6]

- Six panelists represented non-bank "fintech" companies. Three of these were individual "aggregators," companies that collect information from other providers; one was a trade association that represents aggregators and other companies that rely on consumer-permissioned access to financial data; one was a consumer-facing lender that relies on

[4] https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf

[5] https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

[6] The use of this shorthand is not intended to imply that any views expressed at the Symposium are shared by any other persons or institutions who did not so participate. For example, if this document ascribes certain views to "aggregators" or "banks," it is referring only to those aggregators or banks that participated in the Symposium.

consumer-permissioned financial data; and one was an industry attorney who represents companies that use consumer-permissioned financial data.

- Five of the panelists represented "banks." Four of these represented "large banks" and one represented a "smaller bank."
- Five "others" comprised two "consumer advocates" and three "researchers."

Data access and scope

Consumers access data in two ways. "First-party access" refers to consumers directly accessing data in their accounts. Consumers can also authorize (or "permission") third parties to access data on their behalf ("third-party access"). This report, in line with the terms of discussion at the Symposium, generally focuses on permissioned third-party access to consumer data. Participants generally believed consumers should be able to permit third parties to access consumer data. However, panelists disagreed some as to the scope of data consumers should be allowed to share via authorized third-parties. Bank participants were concerned that sharing certain data, such as personally identifiable information or account numbers, entailed higher risk than other data.

Banks were also concerned with any requirement that they share data they deem proprietary. However, an aggregator asserted that consumers should have the right to share certain data that some banks consider to be proprietary: namely, account cost and pricing data, such as fees incurred or the interest rate on an account. In response, bank participants stated that allowing such data to be accessed by third parties could allow for some third parties to amass a large amount of such data. Banks expressed concern that if third parties could use this data without restrictions, they might be able to obtain or derive confidential and proprietary information related to a bank's business practices.

Credential-based access and "screen scraping"

Panelists discussed different methods for accessing consumer data. "Credential-based access" refers to the practice of a third party accessing a consumer's permissioned financial data by obtaining the consumer's credentials and logging into the consumer's online financial account management portal as though it were the consumer (generally on an automated basis). "Screen scraping" refers to the practice of a third party retrieving a consumer's permissioned financial data by using proprietary software to convert the data presented in a consumer's online financial account management portal into standardized machine-readable data able to be utilized by that

third party or other third parties (also generally on an automated basis).[7] An API is a set of rules or software instructions that allow different types of machines to communicate. The Bureau understands that credential-based access and screen-scraping are the predominant means by which third parties currently access and retrieve permissioned consumer data, with some banks and aggregators shifting towards substituting APIs as both a means of data access and retrieval.

Participants generally agreed that an industry move away from credential-based access and screen scraping and towards application programming interfaced (API)[8]-based access would benefit consumers and all market participants. No participant stated any opposition to this view. A broad array of market participants with an interest in consumer-permissioned financial data sharing have long asserted that replacing credential-based access and screen scraping with API-based access to consumer-permissioned financial data would mitigate or obviate many of the risks and challenges associated with the former.

Symposium participants differed, however, in the degree to which they prioritized this step over others. Fintechs generally supported API-based access in the context of a broader data right that ensured ongoing, reliable access to consumer data. Banks urged adoption of APIs without these kinds of preconditions.

Other panelists also identified challenges related to transitioning to API-based access. One researcher participant noted that onboarding an API was an expensive and technically daunting task for small financial institutions. The aggregator trade group participant noted that existing API penetration was small, and that while broadly superior to collecting data via credential-based access and screen scraping, existing API implementations are not always reliable.

Disclosure and informed consent

A variety of panelists invoked informed consent as a critical consumer protection element in consumer-permissioned data sharing. However, panelists disagreed to some extent about the present adequacy of consumer disclosure and consent management. Generally, banks and consumer advocates criticized the visibility, informativeness, and consistency of disclosures offered by companies seeking consumer authorization for permissioned data sharing. Fintechs generally defended their practices and noted relevant recent improvements.

[7] Often, credential-based access and screen scraping are conflated and jointly referred to as "screen scraping." While the two practices are often linked, they are both theoretically and practically severable, and each raises distinct consumer protection issues.

[8] *See* https://hmdahelp.consumerfinance.gov/knowledgebase/s/article/What-is-an-API.

Many participants cited consumer-facing data sharing controls and dashboards as potentially useful tools for aligning treatment of consumer data with consumer preferences. Participants suggested that these tools reduce the onus on upfront disclosures to serve as a primary means of protecting against consumer harm. Consumer advocates pointed towards certain harms, generally privacy risks, that they viewed as not effectively addressable by any regime of informed consent (see "Privacy" below).

Privacy

Bank participants asserted that significant privacy risks arise from credential-based access and screen scraping and suggested that increased regulatory oversight of aggregators and other fintechs could mitigate these risks. Consumer advocates asserted consumers engaged in permissioned data sharing consent frequently to sharing data, or sharing data with certain third parties, that may compromise consumer privacy and that disclosure was inadequate to address these risks. The advocates called specifically for Bureau action to mitigate those privacy risks (see "Considerations regarding the law and future Bureau actions" below). Aggregators focused primarily on issues other than privacy.

Transparency and control

Participants generally agreed that consumers should have control over the data they permission, with a focus on consumers' ability to monitor and regulate data flows, revoke access, and request retroactive deletion of data. Participants also generally agreed that the flows and uses of data should be transparent to the consumer. Several participants asserted specifically that data flows should be traceable; *i.e.*, consumers should be able to see not just what data are being shared or how frequently, but which entities are handling it at various points in its journey from holder to end user. No participants disagreed with this assertion.

No panelists asserted that any one segment of market stakeholders should be solely responsible for ensuring consumer control. Some participants stated that control capabilities should be available to consumers at the origination and ultimate receipt points of the data flow as well as at points in between. Some panelists also suggested controls should be interoperable; *i.e.*, if a consumer provides instructions for changing his or her data sharing at one point in the flow, these instructions should be applied throughout the flow without further action by the consumer.

Consumer advocate panelists stated that even the strongest consumer controls should not be seen as a panacea for other issues, including informed consent, dispute resolution, and privacy. One consumer advocate panelist suggested that consumer controls should extend to "secondary

uses"[9] of the data and that consumers need to have some rights against being required to provide data as a condition to achieve certain ends (such as employment, or to procure a loan where traditional data sources are sufficient to underwrite the applicant).

Security and data minimization

Participants generally agreed that transitioning from credential-based access and screen scraping to API-based authentication and access would improve security. Banks and some other participants believed that more oversight, including cybersecurity oversight, of aggregators and other nonbank handlers of consumer-permissioned data was needed to ensure parity of oversight commensurate with the amount and sensitivity of consumer data accessed.

Participants also agreed that robust data minimization would mitigate security risks inherent in permissioned data sharing. However, as some participants noted, minimization is not always straightforward and implicates access, security, privacy, competition, and innovation. Fintechs expressed concern that banks would attempt to condition whether fintechs could access data, and which data they could access, based on the fintech's representation of the service for which they are using consumer-permissioned data (*i.e.*, the service use case). Fintechs generally preferred the ability to determine which data fields are necessary to support their use cases.

Accuracy, disputes, and accountability

Participants generally agreed that accuracy of shared data was important. Bank participants generally asserted that screen scraping is susceptible to inaccurate capture of data and thus inferior to API-based access.

Participants disagreed about whether or in what circumstances the Fair Credit Reporting Act (FCRA) applies or should apply to credit-related uses of permissioned data. Participants focused primarily in this respect on whether aggregators, by collecting and then sharing third-party data to permissioned, downstream users, would count, at least in some circumstances, as "credit reporting agencies" under the statute.[10] However, several participants stated that a broader dispute resolution mechanism was necessary for all uses of permissioned data, including uses to which the FCRA would not apply.

---

[9] The term "secondary uses" in this context generally refers to uses of consumer-permissioned data beyond those that directly support the service being offered to the consumer.

[10] For example, one consumer advocate participant made the argument that if a company is collecting and sharing third-party data that is used or expected to be used as a factor in determining eligibility for credit, insurance, employment, or other purposes authorized under the FCRA, that company should be considered a "consumer reporting agency" subject to the FCRA under 15 U.S.C. § 1681a(f).

Panelists discussed stakeholder liability, including in the context of the Electronic Fund Transfer Act and Regulation E. Generally, consumer advocates and one researcher panelist agreed that consumers should not be liable for unauthorized transactions associated with permissioned use of data, and other panelists did not contest this proposition. Some participants disagreed about which non-consumer party should bear the ultimate economic cost of a consumer's Regulation E error dispute. Several panelists asserted that in practice, consumers will go to their account-holding institution to initially raise a problem with their accounts.

Panelist commentary on legal issues

Symposium panelists raised a number of issues relating to the meaning and applicability of present statutes and regulations, as well as whether and how the Bureau should interpret and apply them. Panelist commentary on those issues are summarized according to topic below.

THE APPLICABILITY OF DODD-FRANK SECTION 1033 AND OTHER FEDERAL CONSUMER FINANCIAL LAWS

Section 1033 of the Dodd-Frank Act was central to participants' views of both the current obligations of market participants as well as the authority and scope for future Bureau action.

Participants discussed whether section 1033 is "self-executing"; *i.e.*, whether the core mandate of section 1033(a) on covered persons to make information available to consumers has been effective since the passage of the Dodd-Frank Act or would only be effective upon the Bureau issuing rules. Participants also discussed whether consumers' agents are considered consumers for the purposes of section 1033, whether fintechs and data aggregators are acting as consumers' agents, or more generally whether consumer rights to data can be extended to third parties. Further, participants discussed whether section 1033 provides any authority for the Bureau to allow for data field exclusions from a consumer's right to access, or for the denial of data access to third parties relating to security concerns (more on which is in the "Security" subsection below).

For issues related to unauthorized access, participants also asserted that the law is unclear as to: (1) which parties are liable and when (primarily relating to the applicability of the Electronic Fund Transfer Act and Regulation E); (2) if and how the FCRA applies to permissioned data in some cases and how that obligates stakeholders; and (3) the manner in which the Gramm-

Leach-Bliley Act and its implementing regulations regarding privacy and security apply to aggregators.[11]

TECHNICAL STANDARDS

Participants were generally supportive of market-led development of API standards. No participant stated that the Bureau should prescribe specific technical standards or approaches, and several participants stated that the Bureau should not do so.[12]

SECURITY

One researcher panelist raised the issue of whether section 1033 allows data holders to refuse access to a permissioned third party for security reasons, either because that party maintains poor security practices or because the consumer's permission was obtained fraudulently or underhandedly. That panelist also raised the intertwined issue of whether the Bureau's section 1033 rulemaking authority allows the Bureau to prescribe rules or standards that would allow data holders to deny access in such circumstances. The panelist recommended that if the Bureau were to determine that it could not resolve these ambiguities in a way that allows permissioned data to be both secure and subject to the language of section 1033, then Congress should revise the underlying statute.

PRIVACY

Consumer advocates stated that the Bureau should limit certain "secondary uses" of consumer-permissioned data. Advocates also called for robust data minimization and to ensure data holders and users provide consumers effective controls, including with respect to secondary uses such as selling data or analytical products premised on consumer data to parties unconnected to the consumer. One advocate stated that the Bureau should provide for the automatic expiration of a consumer's consent to share and an accompanying automatic obligation upon data receivers to delete collected data, including copies of the data that have been purportedly "deidentified" for other uses.

---

[11] While the Bureau has authority with regard to Gramm-Leach-Bliley privacy, the Bureau has no supervisory, enforcement, or rulemaking authority with regard to Gramm-Leach-Bliley Act section 501(b), or its implementing rules, which require that financial institutions develop, implement, and maintain comprehensive information security programs.

[12] The attorney participant broached the language of section 1033(d), which states that "[t]he Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section," but only in asserting that section 1033(d) is a separable mandate from the broader rulemaking authority in section 1033(a) and that the Bureau safely could and should defer any action on technical standards if it elects to issue rules pursuant to section 1033(a).

LIABILITY

Participants were divided as to whether a market-driven equilibrium of ultimate liability allocation for unauthorized transactions relating to permissioned data use would emerge absent regulatory interventions. One bank participant stated that consumers have a general proclivity to bring disputes regarding unauthorized debits to their banks, resulting in banks bearing outsized burden and losses regardless of whether consumers could also raise these issues with other entities. The attorney participant noted that industry has proven adept at resolving these issues with centralized industry standards in the payment card context and with lawmakers and regulators focusing on protecting consumers from ultimate liability. One researcher participant stressed that the Bureau, when addressing liability, should not stretch the parameters of Regulation E beyond what is permitted by the statute.

PANELIST SUGGESTIONS FOR FUTURE BUREAU ACTIONS

Fintechs generally stated, as did some of the other panelists, that the Bureau should prescribe a right for consumers and permissioned third parties to access their data relying on the authority of Dodd-Frank Section 1033. Banks, as well as some other panelists, generally stated that the Bureau should issue a larger participant rule for the data aggregation market under section 1024(a)(1)(B) of the Dodd-Frank Act to establish its supervisory authority over larger participants in this market.[13]

A number of other suggestions were proffered, such as imposing disclosure requirements or disclosure standards; using guidance or other avenues to clarify some of the regulatory ambiguities described above; or taking actions predominately aimed at securing consumer privacy. Several participants did not recommend specific courses of action, but instead suggested criteria and considerations the Bureau should take into account when taking next steps.

[13] 12 U.S.C. § 5514(a)(1)(B). Note, one bank participant suggested the Bureau establish supervisory authority over data aggregators posing risks to consumers under provisions of section 1024(a)(1)(C) (12 U.S.C. § 5514(a)(1)(C)).