David L. Portilla
+1-212-474-1410
dportilla@cravath.com

Consumer Data Sharing Under Section 1033 of the Dodd-Frank Act

Originally published October 27, 2021; updated as of December 13, 2021

This outline was originally prepared in connection with the Securities Industry and Financial Markets Association's webinar held on October 27, 2021, titled "Consumer Data Sharing Under Section 1033 of the Dodd-Frank Act." We will update this outline periodically as warranted by further developments.

OVERVIEW OF DODD-FRANK ACT SECTION 1033

- Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") grants consumers rights to access information about their financial accounts and contemplates rulemaking by the Consumer Financial Protection Bureau ("CFPB" or "Bureau") to that end.
- Specifically, Section 1033(a) requires 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."[1] Section 1033 further provides that such information must be in an electronic form usable by the consumer.[2]
- Section 1033 is subject to four enumerated exceptions. A covered person is not required to make available to the consumer:
    - Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;
    - Any information collected by the covered person for the purpose of preventing fraud or money laundering, detecting or making any report regarding other unlawful or potentially unlawful conduct;
    - Any information required to be kept confidential by any other provision of law; or
    - Any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information.[3]
- In addition, Section 1033 does not impose a duty to maintain or keep any information about a consumer.[4]
- When prescribing rules under Section 1033, the CFPB must consult with the Federal banking agencies and the Federal Trade Commission ("FTC") to ensure that the rules:
    - Impose substantively similar requirements on all "covered persons";

- Take into account conditions under which covered persons do business in both the United States and in other countries; and
- Do not require or promote the use of any particular technology in order to develop systems for compliance.[5]

- "Covered persons"
  - Covered persons include any person that engages in offering or providing a consumer financial product or service and any affiliate of any such person if such affiliate acts as a service provider to such person.[6]
- "Consumer financial product or service"
  - Consumer financial products and services include any "financial product or service", defined under the Dodd-Frank Act,[7] that is offered or provided for use by consumers primarily for personal, family or household purposes or provided in connection with such products or services.[8]

BACKGROUND ON CFPB ACTIONS TO DATE

2017 Principles

- In October 2017, the CFPB outlined a set of Consumer Protection Principles (the "2017 Principles") for safeguarding consumer interests when consumer authorized third-party companies access consumer financial information to provide financial products and services. The 2017 Principles did not alter existing consumer protection statutes and regulations or establish binding requirements or obligations.
- The Bureau identified nine key principles summarized below:

1. **Access**. Consumers (and their authorized third parties) should be able to access and obtain information about their ownership or use of financial products and services from the product or service provider in a timely and safe manner that does not require consumers to share account credentials with the third party.
2. **Data Scope and Usability**. Financial data to be made available may include any transaction, series of transactions or other aspect of consumer usage; account terms (such as a fee schedule); realized consumer costs (such as fees or interest paid); and realized consumer benefits (such as interest earned or rewards). Such information should be available in readily usable forms, and authorized third parties should only access the data necessary to provide the product(s) or service(s) selected by the consumer and should maintain such data only as long as necessary.
3. **Control and Informed Consent**. The terms of authorized access, storage, use and disposal of consumer information should be fully and effectively disclosed to and understood by the consumer. Terms of access should include access frequency, data scope and retention period. Consumers should not be coerced into granting third-party access and should be able to readily revoke authorizations to access, use or store their data. The revocation should also provide for third parties to delete personally identifiable information.
4. **Authorizing Payments**. Third parties must obtain a separate and distinct consumer authorization to initiate payments. Providers may reasonably require consumers' authorization for both data access and payment authorization to obtain services.
5. **Security**. Consumer data should be accessed, stored, used and distributed securely. Access credentials should also be secured. Parties that access, store, transmit or dispose of data must have protections and processes in place to mitigate the risks of, detect, promptly respond to, and resolve and remedy data breaches, transmission errors, unauthorized access and fraud, and transmit data only to third parties that also have such protections and processes. Security practices should adapt to new threats.
6. **Access Transparency**. Consumers should be informed of or must be able to readily ascertain which authorized third parties are accessing or using their information, the security of each such party, the data they access, their use of such data and the frequency at which they access data.

7. **Accuracy**. Data access by consumers or authorized third parties should be accurate and current and consumers should have reasonable means to dispute and resolve data inaccuracies.
8. **Ability to Dispute and Resolve Unauthorized Access**. Consumers should have reasonable and practical means to dispute and resolve issues of unauthorized data access and sharing, unauthorized payments and failure to comply with other obligations. Consumers should not be required to identify the party or parties who gained or enabled unauthorized access to receive remediation, and the parties responsible for such unauthorized access must be held accountable for the consequences of such access.
9. **Efficient and Effective Accountability Mechanisms**. The goals and incentives of parties that grant access to, access, use, store, redistribute and dispose of consumer data should be aligned and enable safe consumer data access and deter misuse.

2017 Stakeholder Insights

- After issuing a request for information soliciting public input in November 2016,[9] the CFPB published a separate document concurrently with the 2017 Principles highlighting the feedback from stakeholders on market practices regarding consumer access to financial information (the "2017 Stakeholder Insights").
- Notably, the 2017 Stakeholder Insights identified three main categories of stakeholders:
  - "Aggregators"
    - Aggregators are entities involved in providing aggregation services and collecting information from other providers.
  - "Account data users"
    - Account data users use aggregators to offer various (often digital) consumer financial products and services.
  - "Account data holders"
    - Account data holders hold account and other data about consumers and are often banks or credit unions.
- While there was general agreement among the stakeholders on many of the topics outlined in the 2017 Principles, the 2017 Stakeholder Insights also revealed conflicting opinions between aggregators and data users on the one hand and data holders on the other.
  - For instance, some aggregators and data users raised concerns that data holders may restrict or control, in an unreasonable and anti-competitive manner, the type of data they permit consumers to authorize third parties to access. Conversely, data holders and consumer advocates expressed concerns that aggregators may be accessing more data than necessary to deliver the consumer financial products and services that consumers request.
  - The 2017 Stakeholder Insights also observed that there were varying views about how to establish a secure data sharing ecosystem, including what role, if any, the government and the Bureau should play. Aggregators and data users tended to believe that current levels of oversight (when combined with existing market incentives) were adequate and noted that they were already subject to information security rules. On the other hand, data holders and consumer advocates suggested for the Bureau to take steps to extend formal oversight over aggregators and data users.

2020 Symposium

- In February 2020, the CFPB held a symposium on "Consumer Access to Financial Records" and published a document summarizing its understanding of key facts, issues and points of contention raised at the symposium ("2020 Symposium"). Participants at the 2020 Symposium included aggregators, lenders, banks, consumer advocates and researchers. Issues were discussed under the topics of 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 legal issues.

- The panelists disagreed on a number of points, including the scope of data authorized third parties should be able to access. Some participants raised concerns regarding sharing certain higher risk data with aggregators, such as personally identifiable information or account numbers. Other participants called out the reluctance of some banks to share data they considered to be proprietary.
- The panelists also discussed three different methods of accessing consumer data:
  - "Credential-based access"
    - Credential-based access is 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"
    - Screen scraping is 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 a third party or other third parties (generally on an automated basis).
  - "API"
    - An application programming interface, or API, is a set of rules or software instructions that allow different types of machines to communicate.
- The CFPB understood credential-based access and screen scraping to be the predominant means by which authorized third parties accessed and retrieved data at the time, with some banks and aggregators shifting towards substituting APIs as both a means of data access and retrieval. According to the Bureau, all symposium participants shared the view that moving toward API-based access would benefit consumers and all market participants.
- Bank participants and consumer advocates also asserted that significant privacy issues arise from credential-based access and screen scraping and raised concerns regarding compromised consumer privacy without adequate disclosure of the risks to consumers.
- Finally, panelists raised a number of legal questions including:
  - Whether Section 1033 is "self-executing" (*i.e.*, whether its mandates on covered persons have been effective since the passage of the Dodd-Frank Act or would only be effective upon the CFPB issuing rules);
  - Whether consumers' agents are consumers for the purposes of Section 1033, whether fintechs and aggregators are acting as consumers' agents and, more generally, whether the consumer rights under Section 1033 can be extended to third parties; and
  - Whether the CFPB has authority under Section 1033 to allow for data field exclusions or denials of a consumer's or third party's access rights due to security concerns.
- In cases of unauthorized access, the participants asserted that the law is unclear as to:
  - Which parties are liable and when (primarily relating to the applicability of the Electronic Fund Transfer Act ("<u>EFTA</u>") and Regulation E);
  - If and how the Fair Credit Reporting Act ("<u>FCRA</u>") applies to permissioned data in some cases and how that obligates stakeholders; and
  - The manner in which the Gramm-Leach-Bliley Act ("<u>GLBA</u>") and its implementing regulations regarding privacy and security apply to aggregators.

2020 ANPR

- In October 2020, the CFPB issued an advance notice of proposed rulemaking ("ANPR") soliciting comment on ways the Bureau may develop regulations to implement Section 1033 and seeking information regarding the scope of data access, other terms of access (such as those relating to security, privacy, consumer control over access and accessed data, accountability for data errors and unauthorized access) and legal uncertainty over the interaction of Section 1033 with the GLBA, FCRA and EFTA.
- Specifically, the Bureau sought comment on nine topics:
  - Benefits and costs of consumer data access
  - Competitive incentives and authorized data access
  - Standard-setting
  - Access scope
  - Consumer control and privacy
  - Legal requirements other than Section 1033
  - Data security
  - Data accuracy
  - Any other information that would help inform the Bureau
- Notable among these topics is the focus on competition (which was not directly addressed in the 2017 Principles), with the Bureau highlighting in the ANPR preamble that "Authorized data access holds the potential to intensify competition and innovation in many, perhaps even most, consumer financial markets . . . One notable aspect of the competition fostered by consumer-authorized data access is that in many cases data users may compete for customers with the data holders from which they have obtained data . . . These competitive dynamics mean that data holders may have an incentive to restrict access by certain data users or to seek greater clarity about the purposes to which particular accessing parties may put accessed data. By the same token, data users may have incentives not to be forthcoming about such purposes."[10]

2021 EXECUTIVE ORDER ON PROMOTING COMPETITION

- In July of this year, President Biden signed an Executive Order on Promoting Competition in the American Economy affirming the administration's policy to enforce antitrust laws and directing federal agencies to consider using their authorities in furtherance of such policies.
- Among its exhortations, the order called on the Director of the CFPB to consider commencing or continuing a rulemaking under Section 1033 of the Dodd-Frank Act to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products.

2021 CFPB ORDERS TO PROVIDE INFORMATION ON PAYMENTS PRODUCTS

- On October 21, 2021, the CFPB ordered a number of technology companies to provide the agency with information regarding their payments products, pursuant to Section 1022(c)(4)(B)(ii) of the Dodd-Frank Act.[11]

- In a statement accompanying the orders, Director Rohit Chopra noted that the inquiry will "yield insights that may help the CFPB to implement other statutory responsibilities, including any potential rulemaking under Section 1033."

2021 CFPB PRESS CALL

- On December 1, 2021, Director Chopra held a press call regarding checking account overdraft fees. In the prepared remarks for the call, Director Chopra alluded to Section 1033, stating that the "CFPB will be looking to harness technology in ways that give American families the power to more easily fire poor-performing banks. We can only accrue the benefits of competition if customers can vote with their feet. Unfortunately, switching bank accounts isn't easy. It involves new account numbers, new debit cards, updating direct deposit, updating auto-debits, and much more. If America can shift to an open banking infrastructure, it will be harder for banks to trap customers into an account for the purpose of fee harvesting".

BACKGROUND ON CONSUMER DATA ACCESS

APIs

- Broadly speaking, the industry has been moving away from screen scraping and credential-based data access towards data sharing through APIs. An API facilitates the transfer of consumer data through tokenized access, thereby removing credential sharing and allowing users to be authenticated at their own financial institution.
- Data sharing through API tends to be more accurate and secure than screen scraping and credential-based access. APIs also provide data holders with more control in managing data access as compared to screen scraping, including by allowing them to restrict the scope of data transferred to aggregators or data users.
- APIs require bilateral access agreements between a data holder and aggregator outlining the terms of the data sharing that must be negotiated.

Screen Scraping and Credential-Based Data Access

- Screen scraping requires consumers to turn over their log-in credentials to data aggregators or data users to access consumer data. Some industry participants have argued that this creates significant security and privacy concerns. For example, there are questions regarding whether data aggregators and data users have in place the same data security protocols or fraud monitoring systems that are commonplace for regulated financial institutions.
- Screen scraping has been criticized for being more susceptible to inaccuracy than APIs.

KEY CONCERNS EXPRESSED IN INDUSTRY ANPR COMMENT LETTERS

- The CFPB received around 100 comments to the ANPR from banks, aggregators, fintechs and industry trade groups, among others. Below, we provide a few highlights from the comment letters to help outline the debate and the key issues at stake.

Bank Trade Associations' Comment Letters

- One of the key concerns expressed in the comment letters from the bank trade associations is the regulatory uncertainty surrounding aggregator and data user practices. Some commenters argued that there was not enough clarity around the application of the security and privacy provisions of the GLBA to aggregators and other authorized entities[12] and whether Regulation P obligations applied once a financial institution has allowed access to consumer data in compliance with any Section 1033 implementing regulations. The commenters proposed designating data aggregators as "larger participants" of the consumer financial data services marketplace to provide for their direct oversight and regular supervision and examination by the CFPB.[13] The commenters also argued for the CFPB to clarify the allocation of liability, in particular for unauthorized transactions under Regulation E, as consumers may turn to their banks whenever a data breach or unauthorized account transaction occurs, even if the bank was not responsible for the incident.

- Bank trade associations generally called for CFPB coordination with other federal financial regulators, including the U.S. Securities and Exchange Commission ("SEC"), on issues specific to broker-dealers, investment advisers and other regulated entities not subject to CFPB supervision, and the Office of the Comptroller of the Currency ("OCC"), for confirmation on whether arrangements with aggregators or data users constitute third-party vendor relationships subject to the issued guidance on third-party relationships.[14]
- Bank trade associations continued to be concerned about the types of data consumers should be able to access and share with aggregators and account data users. The commenters asserted that not all personal information collected by financial institutions is within the scope of data covered by Section 1033. In addition, some commenters argued that certain consumer data can reveal market movements and contain sensitive information when aggregated and urged for such data to also be excluded.
- Some bank trade associations argued for improved transparency of the consumer consent process and specific disclosure requirements, asserting that consumers may still be unaware that (1) they are providing their credentials to a third-party data aggregator, rather than directly to a financial institution, and (2) their credentials or data could be further shared and/or used beyond their initial authorized access. The commenters also claimed that consumers could be confused about which party they are entering into an agreement with and which party is holding their data.
- Bank trade associations generally highlighted the market-driven solutions that have been developing to unify the industry around common contractual and technical standards and maintained that the Bureau should avoid setting specific technical standards.
- Some commenters encouraged the inclusion of an exception to authorized access during times of market stress or volatility as financial institutions may experience significant stresses on their systems due to increased data access during those times.

Aggregator Comment Letters

- Aggregator commenters generally agreed with bank trade associations that the CFPB should clarify of Section 1033's interaction with existing law. For instance, some commenters claimed that the FCRA does not apply in the context of Section 1033 consumer-permissioned data and that consent authorization under Section 1033 for certain student loan data should satisfy Family Educational Rights and Privacy Act ("FERPA") requirements. The commenters also maintained that the Bureau should work with the OCC to clarify that Section 1033 applies regardless of the level of business relationship between banks and aggregators. Commenters argued that the Bureau should address how Regulation E applies to unauthorized transactions that occur in the context of data sharing.
- Some aggregators acknowledged that they have reached a size at which supervision would provide helpful oversight and assurances to the ecosystem. In such cases, aggregators proposed two avenues for supervision, (1) the Bureau may exercise its existing supervisory authority over certain aggregators that provide services to banks[15] and (2) the Bureau may exercise authority to designate some aggregators as "larger participants" subject to direct supervision.[16]
- One of the broader arguments made by aggregators was that Section 1033 was enacted to allow consumers to benefit from access to their own financial data by providing autonomy over its use and portability for use by different financial service providers. Some commenters also argued that data holders should be supervised for compliance with Section 1033 and that remedies should be provided for consumers when data holders improperly burden or impede authorized access to their data.
- Commenters generally agreed with bank trade associations that the Bureau should use principles-based guidelines rather than mandates for technical standards.

New York
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

London
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com

---

[1] 12 U.S.C. § 5533(a).

[2] *Id*.

[3] 12 U.S.C. § 5533(b).

[4] 12 U.S.C. § 5533(c).

[5] 12 U.S.C. § 5533(e).

[6] 12 U.S.C. § 5481(6).

[7] 12 U.S.C. § 5481(15).

[8] 12 U.S.C. § 5481(5).

[9] 81 Fed. Reg. 83806 (Nov. 22, 2016).

[10] 85 Fed. Reg. 71006 (Nov. 6, 2020).

[11] 12 U.S.C. § 5512(c)(4)(B)(ii). An example order is available here.

[12] Commenters stressed that the CFPB should coordinate with the FTC to expand the safeguards rule to expressly address data aggregators' security practices. The Bureau has no supervisory, enforcement or rulemaking authority with respect to GLBA section 501(b) (15 U.S.C. § 6801(b)) or its implementing rules, which require financial institutions to develop, implement and maintain comprehensive information security programs.

[13] 12 U.S.C. § 5514(a)(1)(B). For Federal consumer financial protection laws, Section 1024 of the Dodd-Frank Act provides the CFPB with *exclusive* authority to supervise certain non-banks that provide mortgage-related products or services and payday and private student loans, among others, as well as larger participants of other consumer financial service or product markets as defined by CFPB rules, plus their service providers. 12 U.S.C. §§ 5114(c), (d). The CFPB has prescribed larger participant rules with respect to the consumer reporting, consumer debt collection, student loan servicing, international money transfer and automobile financing markets. 12 C.F.R. §§ 1090.104-1090.108.

[14] In March 2020, the OCC updated its Third Party Guidance FAQs to specify that if a formal relationship between a bank and an aggregator exists, banks must engage in due diligence and ongoing monitoring of the aggregator commensurate with the risk to the bank. But even when no business relationship exists, banks should conduct due diligence to evaluate the business experience and reputation of the aggregator to gain assurance that the aggregator maintains controls to safeguard sensitive customer data. *See* OCC Bulletin 2020-10 (Mar. 5, 2020), available here. *See also* SIFMA Response to Proposed Interagency Guidance on Third-Party Relationships: Risk Management (Oct. 4, 2021), available here.

[15] *See* 12 U.S.C. §§ 5515(d), 5516(e), 5481(26)(A).

[16] *See supra* n. 13.