Davis Polk

CFPB issues long-awaited open banking proposal

Overview and key takeaways

November 15, 2023 | Client update

Table of contents

davispolk.com

Davis Polk

Overview of the proposal

The Consumer Financial Protection Bureau (CFPB) recently proposed a rule to implement Section 1033 of the Dodd-Frank Act.

- Section 1033 requires that "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."
- The proposal would regulate three categories of data collectors and users:
  - **Data Providers** – defined as a "covered person," which would consist of:
    - A "financial institution," defined as "a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services" other than certain motor vehicle dealers that are excluded under Dodd-Frank Act Section 1029;
    - A "card issuer," defined as "a person that issues a credit card or that person's agent with respect to the card"; and
    - Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person.
    - Depository institutions that do not have a consumer interface are excluded.
  - **Authorized third parties** – defined to include an entity that "seek[s] access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer request[s]." This term can include a competing financial institution.
  - **Data aggregators** – defined as "an entity that is retained by and provides services to the authorized third party to enable access to covered data."
- Our client update from July 2023 provided an overview of prior developments leading up to this proposal.
- The proposal is open for public comment until **December 29, 2023**.

davispolk.com
Davis Polk

Key takeaways

The proposal would grant consumers greater access rights to the data their financial institutions hold and could significantly shift the market for financial data.

01

Shift towards data portability

Subject to some limitations, the rule would require that a data provider comply with a consumer's request (or an authorized third party's request on behalf of a consumer) for any of the consumer's personal data collected by the data provider.

02

Emphasis on increasing competition

In proposing the rule, the CFPB discusses its view that large market participants are currently disincentivized from providing open access to consumer data. The CFPB notes that many large incumbents have begun to acquire, or build out, data aggregation services, efforts that may ultimately weaken competition in the data aggregation sector.

03

Focus on "junk fees"

CFPB Director Rohit Chopra echoed a broader initiative by the Biden administration, noting that the proposal would help consumers "escape junk fees." The proposal would prohibit data providers from charging consumers fees to pay for consumer data requests.

04

Inclusion of technical requirements

The proposal would require that a data provider build a consumer interface and a developer interface that meet detailed technical requirements. Both interfaces must make data available to consumers and third parties in a "machine-readable file." Moreover, the rule would prescribe certain performance standards for the developer interface, including the requirement that the developer interface provide a "proper response" to a data request 99.5% of the time. The proposal also would require that data providers publicly release documentation so that authorized third parties can easily understand and access the data providers' developer interfaces.

Key takeaways

05

Preference for application program interfaces (APIs)

The proposal would place limits on data providers allowing third parties to access a user's data with the user's credentials, a practice known as "screen scraping." Instead, the proposal would require that data providers develop consumer and developer interfaces that allow consumers and authorized third parties to access consumer data from data providers.

06

Extending the regulatory perimeter to cover data collectors and aggregators

The CFPB extensively discusses the need to regulate data collection and aggregation practices. It states that some third parties misuse and mishandle consumer data, which sows distrust of third-party data collectors and data aggregators. The CFPB also notes that data collectors and aggregators do not all have sophisticated data security and integrity policies. The proposal would attempt to address all of these perceived shortcomings.

07

Limiting secondary use by data collectors and aggregators

The proposal would prohibit a data collector or aggregator from using a consumer's data for any purpose other than what is "reasonably necessary" to provide the consumer with a financial product or service. The secondary use prohibition will likely impact many data collectors and aggregators, particularly because the prohibition also appears to apply to secondary use of anonymized, or de-identified, data. The CFPB has requested comment on (1) whether third parties should be allowed to use a consumer's data for secondary uses upon receiving the consumer's permission and (2) specifically whether third parties should be allowed to engage in secondary uses with de-identified data upon receiving the involved consumers' permission.

08

Empowering consumer revocation powers while constraining data providers' revocation methods

The proposal would permit a consumer to revoke a third party's access for a particular product or service while continuing to allow the same third party access for a separate product or service. A third party would not be permitted to condition the provision of one product or service on maintaining access to a consumer's data for a separate product or service. In contrast, data providers would not be able to offer to partially revoke a third party's access to the consumer's data held by the data provider. Instead, data providers would only be able to provide a revocation method that fully revokes a third party's access.

Critiques and concerns with the proposal

Increasing liquidity risk for retail deposits

CFPB Director Rohit Chopra stated that the proposal would "make it much easier [for consumers] to switch" between financial firms and would "jumpstart competition." Acting Comptroller of the Currency Michael Hsu similarly noted that open banking would empower consumers but also warned that "in isolation [account portability] would likely increase the liquidity risk of retail deposits for banks."

High cost of compliance

Any data provider with a consumer interface would need to comply with the proposal, meaning financial institutions of all sizes would need to develop APIs that allow consumers and developers access to consumer data. Rob Nichols, President and CEO of the American Bankers Association, expressed concern "with the significant implementation costs our members will face."

Data security concerns

Lindsey Johnson, President and CEO of the Consumer Bankers Association, noted that "[m]any of these entities that are collecting, storing, and selling this consumer information are not subject to the same rigorous data security and privacy standards as well-regulated and supervised financial institutions, putting consumers and their sensitive financial information at risk."

Comments from policy makers

CFPB Director Rohit Chopra and White House National Economic Council Director Lael Brainard delivered remarks in conjunction with the rollout of the proposal.

Consumer protection and encouraging competition

"With the right consumer protections in place, a shift toward open and decentralized banking can supercharge competition, improve financial products and services, and discourage junk fees. Today, we are proposing a rule to give consumers the power to walk away from bad service and choose the financial institutions that offer the best products and prices."

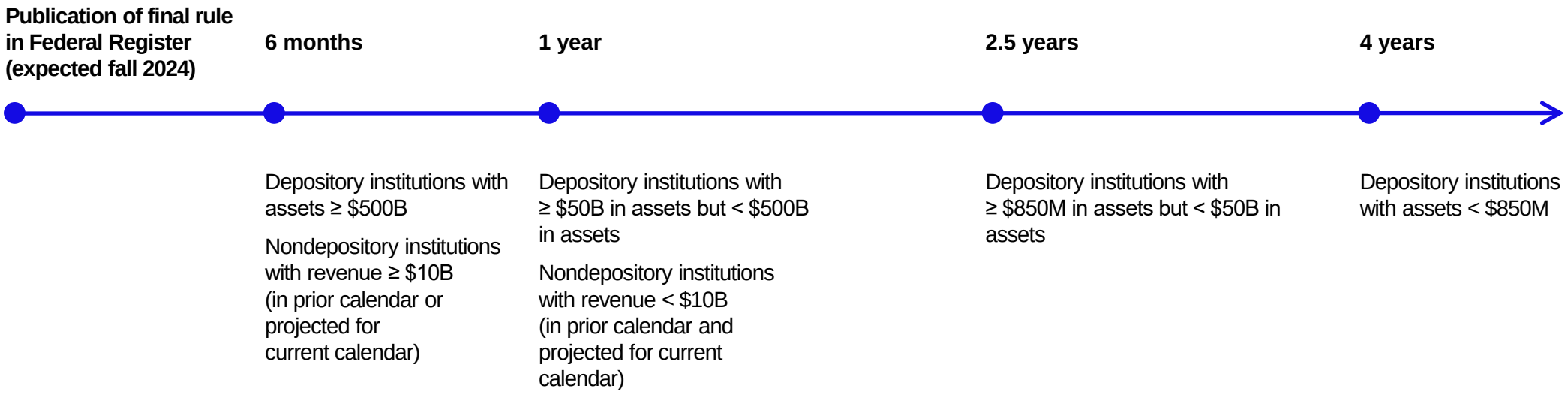
– Rohit Chopra

Improving quality of financial services by forcing more competition

"It is often really daunting for a consumer to switch banks, in part because it's difficult to take their financial transaction history data to a new bank. Today's rule will help ensure financial companies compete based on service quality and pricing."

– Lael Brainard

Proposed compliance timeline



Consumer data rights

Under the proposal, a consumer would be able to request that a data provider produce any "covered data" within the data provider's control or possession and that concerns "a covered consumer financial product or service that the consumer obtained from the data provider."

"Covered consumer financial product or service" is defined to mean a consumer financial product or service (as that term is defined in Section 1002(5) of the Dodd-Frank Act) that is:

- An "account" as defined in Regulation E, meaning "a demand deposit (checking), savings, or other consumer asset account (other than an occasional or incidental credit balance in a credit plan) held directly or indirectly by a financial institution and established primarily for personal, family, or household purposes."
- A "credit card" as defined in Regulation Z, meaning "any card, plate, or other single credit device that may be used from time to time to obtain credit."
- A facilitation of payments from a Regulation E account or Regulation Z credit card.

The CFPB intends to include mortgages, auto loans, student loans and other consumer financial products or services within the scope of "covered data" through supplemental rulemaking.

Consumer data rights

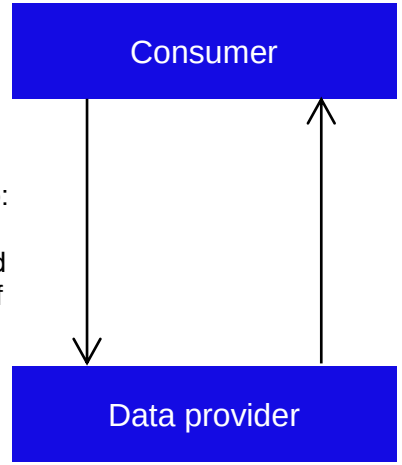
Categories of covered and exemptive data

Covered data	Exempted data (a data provider is not required to make available)
At least 24 months of transaction information (e.g., amount, date, payee, etc.)	Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors
Account balance	Information collected for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding unlawful or potentially unlawful conduct
Information to initiate a payment to or from a Regulation E account (including an ACH transaction)	Information required to be kept confidential by any other provision of law
Account terms and conditions (e.g., fee schedule, rate, etc.)	Information the data provider cannot retrieve in the ordinary course of business
Upcoming bill information (e.g., minimum payment information)	
Basic account verification information (name, address, email address and phone number)	

Regulation of data providers

A data provider would have to make available to the consumer or authorized third party "the most recently updated covered data that it has in its control or possession at the time of a request."

Data request from consumer



Authorizes data request, providing:

Information sufficient to:
(1) authenticate consumer's identity and
(2) identify the scope of the data requested

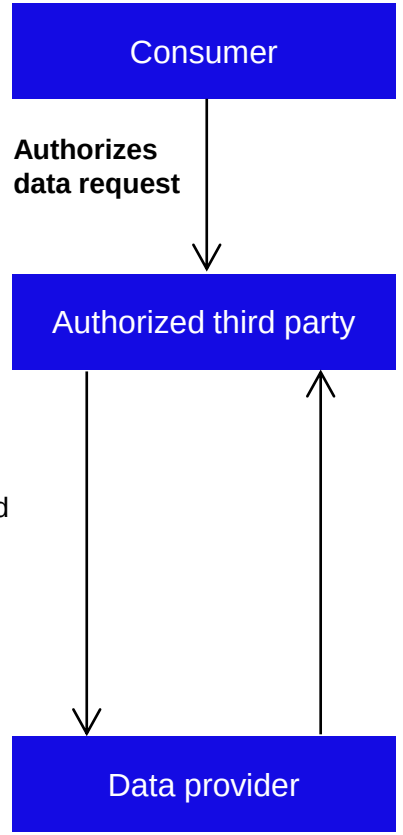
Generally:

Data in an electronic form usable by consumer

Upon specific request:

Information provided in a "machine-readable file" that can be retained by consumer and transferred for processing into a separate information system that is reasonably available to and in control of the consumer

Data request from authorized third party



Authorizes data request

Information sufficient to:
(1) authenticate the consumer's identity
(2) authenticate the third party's identity
(3) confirm the third party has followed specified authorization procedures and
(4) identify scope of data requested

Generally:

Data in an electronic form usable by the third party

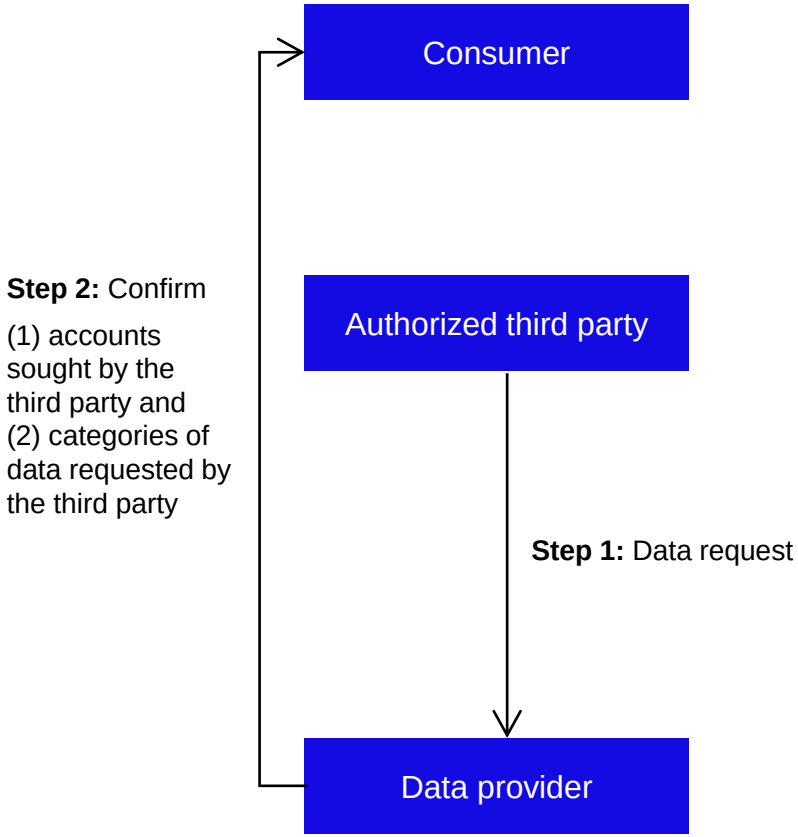
Upon specific request:

Information provided in a "machine-readable file" that can be retained by the third party and transferred for processing into a separate information system that is reasonably available to and in control of the third party

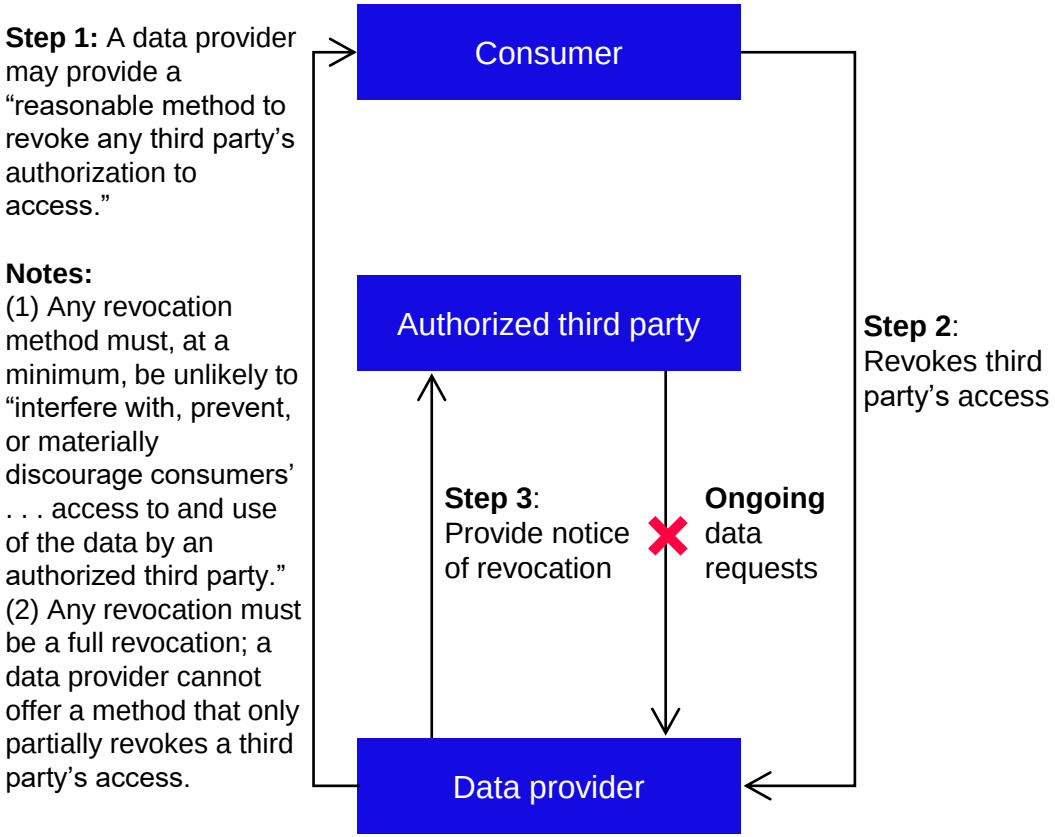
Regulation of interaction between data providers and consumers regarding authorized third party access

The proposal regulates how data providers may communicate with consumers regarding authorized third party access.

Third-party data request confirmation



Consumers may revoke third party's access



Regulation of data providers

Requirements for consumer and developer interfaces

Upon specific request, data providers would:

- Have to “make available to a consumer or an authorized third party covered data in a machine-readable file that can be retained by the consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party”;
- Not be permitted to impose fees or charges on a consumer or authorized third party in connection with establishing and maintaining the required consumer and developer interfaces or in connection with receiving requests or making available covered data in response to requests; and
- Only be permitted to restrict access (1) for data that is exempted or (2) based on risk management concerns.

davispolk.com

Davis Polk

Regulation of data providers

Requirements for consumer and developer interfaces

A data provider would be allowed to deny access to a third party for risk management concerns if:

- The third party fails to present evidence that its data security practices are adequate to safeguard covered data; or
- The third party does make the following information available, in human-readable and machine-readable formats, and readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website:
  - The third party's legal name and, if applicable, any assumed name it is using while doing business with the consumer;
  - A link to the third party's website;
  - The third party's Legal Entity Identifier (**LEI**), issued either by a utility endorsed by the LEI Regulatory Oversight Committee or a utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system; and
  - Contact information a data provider can use to inquire about the third party's data security practices.

One indicia of whether a denial is reasonable is whether the denial adheres to a qualified industry standard related to data security or risk management.

- A qualified industry standard related to risk management is one set by a CFPB-approved standard setting body. The proposal does not discuss the reasonableness of denying access to adhere to the Interagency Guidance released on June 6, 2023 relating to banking organizations' management of risks associated with third-party relationships. **Our client update from June 2023 provides more details on the Interagency Guidance on third-party relationships.**

Regulation of data providers

Specific requirements for developer interfaces

A developer interface would have to:

- Be in a "standardized format," meaning that it either:
  - Makes available covered data in a format that is set forth in a "qualified industry standard," or
  - In the absence of a "qualified industry standard," makes available covered data in a format that is widely used by the developer interfaces of other similarly situated data providers with respect to similar data and is readily usable by authorized third parties.
- Demonstrate "commercially reasonable" performance, meaning that it has to provide a "proper response" 99.5% of the time, which doesn't include queries during scheduled downtimes.
  - A proper response is one that occurs within 3500 milliseconds.
  - **Indicia of whether a developer interface's performance is commercially reasonable** include whether it:
    - Meets applicable performance specifications set forth in a qualified industry standard; and
    - Meets applicable performance specifications achieved by developer interfaces established or maintained by peers.
- Cannot unreasonably limit frequency of data requests.
- Meet certain security specifications, including that it:
  - Must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface; and
  - Requires the data provider to apply to the developer interface an information program that satisfies the regulations issued pursuant to section 501 of the Gramm-Leach-Bliley Act **(GLBA).**

Regulation of data providers

Required disclosures

A data provider would have to make the following information readily identifiable to members of the public, which means the information must be (1) at least as available as it would be on a public website and (2) available in both human-readable and machine-readable formats.

Information about data provider:

- Legal name and, if applicable, any assumed name it is using while doing business with the consumer
- A link to the data provider's website
- The data provider's LEI
- Contact information that enables a consumer or third party to receive answers to questions about accessing covered data

Information about developer interface:

- Documentation, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface
- Documentation must:
  - Be maintained and updated as the developer interface is updated;
  - Include how third parties can get technical support and report issues with the interface; and
  - Be easy to understand and use, similar to data providers' documentation for other commercially available products.

Information about developer interface performance:

- At least 13 rolling months of monthly performance results that measure how often the developer interface provides a proper response to queries to the interface for covered data

Regulation of data providers

Required policies and procedures

A data provider would have to establish and maintain written policies and procedures that are reasonably designed to achieve the following objectives:

Tailoring

- Policies and procedures should be "appropriate to the size, nature, and complexity of the data provider's activities."

Recordkeeping

- Records should describe whether data included in each new record is "covered data."
- Records should describe whether data is not made available on the interfaces because it is subject to an exception.
- Whenever a denial is made because the data is subject to an exception or because the data provider cannot authenticate the consumer or third party, the data provider should:
  - Create a record explaining the basis for denial; and
  - Communicate as quickly as practical to the consumer or third party the type of information denied and reason for denial.

Review

- Policies and procedures should be periodically reviewed and updated "as appropriate to ensure their continued effectiveness."

Accurate data

- Records should address any inaccuracies noted by the consumer or authorized third party.
- An indicia of compliance with the accuracy requirements is whether a data provider's policies and procedures conform to a qualified industry standard regarding accuracy.

Record retentions

- Records related to data provider's response to a consumer or third-party request for information (or request from the developer interface) must be retained for at least three years.
- All other records must be retained for a reasonable period of time.

Regulation of authorized third parties

Authorization disclosures and limits

A data provider would have to provide a consumer with an authorization disclosure that is "clear, conspicuous, and segregated from other material."

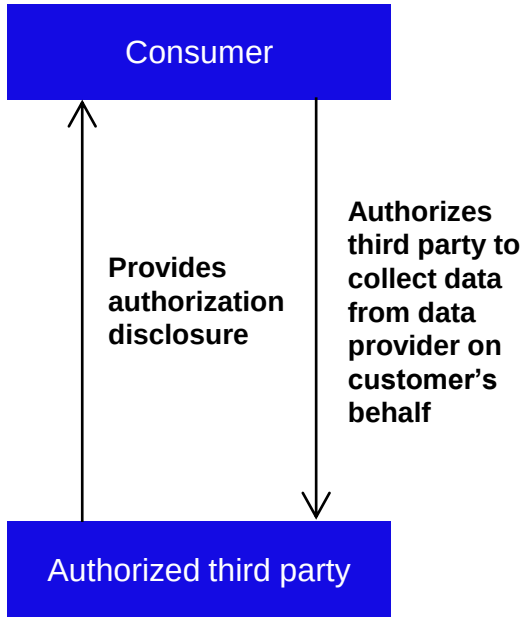
An authorization disclosure is required to:

- Be clear, conspicuous, and segregated from other material.
- Include:
  1. The name of the authorized third party;
  2. The name of the data provider that controls the covered data;
  3. A brief description of the product or service that the consumer has requested the third party provide;
  4. A statement that the third party will collect, use, and retain the consumer's data only for the purpose of providing that product or service to the consumer;
  5. The categories of covered data that will be accessed;
  6. A statement certifying the third party's obligations to limit its use of data; and
  7. A description of the revocation method provided for in the proposal.

Maximum duration: The authorization disclosure would only remain effective for up to one year, after which the third party would have to obtain a new authorization. If a new authorization is not obtained, then the third party would:

- Not be able to collect any more data from the data provider on behalf of the consumer, and
- Only be able to use previously collected data if the data remains reasonably necessary to provide the consumer's requested product or service.

Providing data: Once authorized, the authorized third party would be able to collect data and either deliver the data to the consumer or make it available in a location readily accessible to the consumer (e.g., in the third party's interface).



Regulation of authorized third parties

Limitations on use of data

Authorized third parties:

- Would only be able to collect, use and retain consumers' data to the extent "reasonably necessary to provide the consumers' requested product or service."
  - Other than providing the prohibited list below, the proposal does not provide any measurable way to determine whether a use is "reasonably necessary." The CFPB has requested comment on whether there are technology-based solutions that could allow a user to limit a third party's use of the consumer's data.
- Would not be allowed to collect, use, or retain consumers' data to conduct:
  - Targeted advertising;
  - Cross-selling of other products or services; and
  - Sales of covered data.

Regulation of authorized third parties

Required policies and procedures

Authorized third parties would be required to maintain accurate data, meaning they:

- Must "establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party, if applicable."
- The proposal specifies that a third party's policies and procedures regarding accurate data:
  - Can be determined in light of the third party's size, nature, and complexity of its activities;
  - Must be periodically reviewed and updated as appropriate to ensure their continued effectiveness; and
  - Must consider
    - Accepting covered data in the standardized format required of data providers; and
    - Addressing information provided by a consumer, data provider or another third party regarding inaccuracies in the covered data.
  - **An indicia of whether a third party's policies and procedures are compliant** is whether its policies and procedures conform to a qualified industry standard regarding accuracy.

davispolk.com

Davis Polk

Regulation of authorized third parties

Required policies and procedures

Data security: An authorized third party would have to apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the rules issued pursuant to section 501 of the GLBA or, if the third party is not subject to section 501 of the GLBA, the information security program required by the Federal Trade Commission's (**FTC's**) Standards for Safeguarding Customer Information.

Record retention: Authorized third parties would have to retain any records evidencing their compliance with these rules for at least three years. Records that must be retained include:

- A copy of the authorization disclosure that is signed or otherwise agreed to by the consumer and reflects the date of the consumer's signature or other written or electronic consent;
- Actions taken by the consumer, including actions taken through a data provider, to revoke the third party's authorization; and
- Data aggregator certification statements provided to customers.

davispolk.com

Davis Polk

Regulation of authorized third parties

Required customer disclosures

An authorized third party would be required to have in place policies and procedures that allow it to be able to provide to a consumer, upon request, the following information:

- Categories of covered data collected;
- Reasons for collecting the covered data;
- Names of parties with which the covered data was shared;
- Reasons for sharing the covered data;
- Status of the third party's authorization; and
- How the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation.

davispolk.com

Davis Polk

Regulation of authorized third parties

Revocation of authorization

Revocation method: Third parties would have to provide consumers "with a mechanism to revoke the third party's authorization to access the consumer's covered data."

- The mechanism must be "as easy to access and operate as the initial authorization."
- The third party must "ensure the consumer is not subject to costs or penalties for revoking the third party's authorization."

Partial revocation: Third parties would have to provide a consumer with the ability to revoke the consumer's consent to the third party's data access for each product or service provided by the third party.

- Consumers would have the freedom to choose whether to fully revoke a third party's access or whether to revoke a third party's access for only certain products or services offered by the third party. The proposal warns third parties to not condition the provision of one product or service on maintaining access to consumers' data for a separate product or service.
- In contrast, data providers would not be allowed to offer consumers the ability to partially revoke the data access of a third party or data aggregator. Instead, data providers would only be able to offer consumers the ability to fully revoke a third party's access.

Disclosing a revocation: A third party would have to inform "the data provider, any data aggregator, and other third parties to whom it has provided a consumer's covered data when the third party receives a revocation request from the consumer."

Regulation of data aggregators

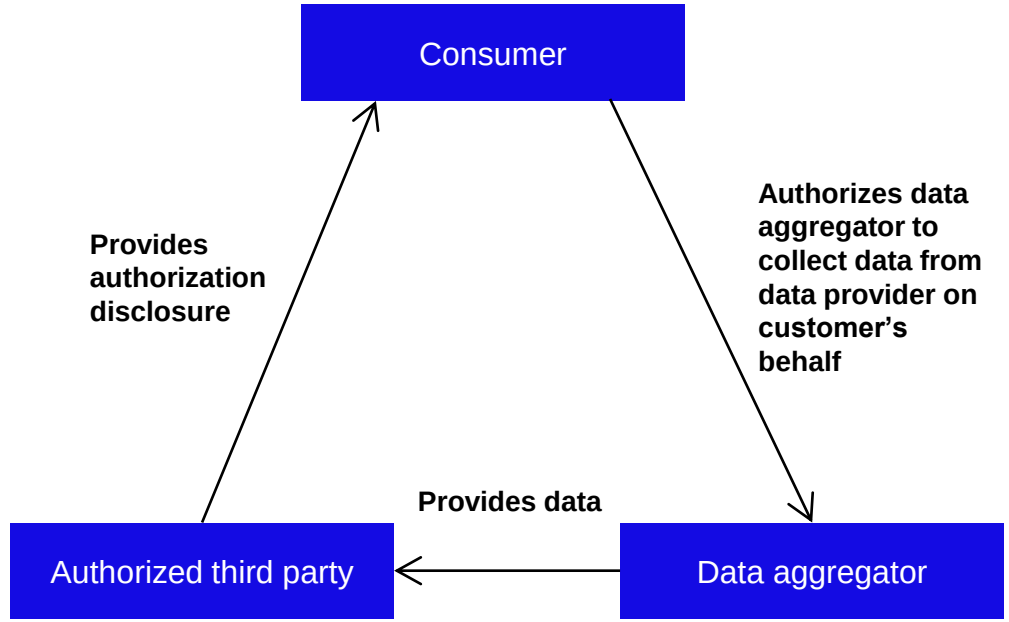
Interaction between consumers, authorized third parties and aggregators

Authorization disclosure: An authorized third party that relies on a data aggregator would need to disclose the use of a data aggregator to the consumer in the authorization disclosure form.

- The disclosure would need to include a name of the data aggregator as well as "a brief description of the services the data aggregator will provide."

Certification to consumer: Data aggregators would have to certify to consumer that it agrees to the same restrictions placed on authorized third parties for the collection, use and retention of consumer data.

- The data aggregator certification would have to be included in the authorization disclosure or provided separately to the consumer.



Development of industry data standards

The proposal incorporates "qualified industry standards."

- **A qualified industry standard** is "a standard issued by a [CFPB-recognized] standard-setting body."
- **To become a CFPB-recognized standard-setting body**, a body would have to:
  - Make open to interested parties all sources, procedures, and processes used and allow interested parties to meaningfully participate in standards development on a non-discriminatory basis;
  - Balance decision-making power across all interested parties including consumer and other public interest groups, at all levels of the standard-setting body, meaning that there "is meaningful representation for large and small commercial entities within these categories," no "single interest or set of interests dominates decision-making," and "a recognition that some participants may play multiple roles, such as being both a data provider and an authorized third party";
  - Use documented and widely available policies and procedures, provide adequate notice and time to prepare for meetings and standards development and create a fair and impartial process to resolve conflicting views;
  - Implement an appeals process to impartially handle appeals;
  - Develop standards by consensus, meaning there is general agreement and requiring that "comments and objections are considered using fair, impartial, open, and transparent processes";
  - Make transparent to interested parties the policies and procedures for participating in, and developing, standards; and
  - Be recognized within the last three years as a standard-setting body by the CFPB
- A body would be able to request that the CFPB recognize it as a standard-setting body. The CFPB would then consider the above conditions when considering the request.

The CFPB does not currently recognize any standard-setting bodies that can create "qualified industry standards" under this proposal.

Development of industry data standards

Many of the proposal's thresholds for determining whether a party's participation has complied with the rule refer to whether the party has complied with "qualified industry standards."

Involved party	Determination	Location in proposal	Effect of compliance with "qualified industry standard"
Data provider	Whether a developer interface makes available covered data in a standardized format	§ 1033.311(b)(1)	Sufficient for compliance
Data provider	Whether a data provider's notice of downtime for its developer interface was reasonable enough to qualify as scheduled downtime	§ 1033.311(c)(1)(i)(B)	Indicia of reasonableness
Data provider	Whether the total amount of scheduled downtime a developer interface incurs is reasonable	§ 1033.311(c)(1)(i)(C)	Indicia of reasonableness
Data provider	Whether a developer interface's performance is commercially reasonable	§ 1033.311(c)(1)(ii)(A)	Indicia of reasonableness
Data provider	Whether frequency restrictions placed on authorized third parties' access to a developer interface are reasonable	§ 1033.311(c)(2)	Indicia of reasonableness
Data provider	Whether the denial of access due to an identified risk management or data security issue was reasonable	§ 1033.321(c)	Indicia of reasonableness
Data provider	Whether the revocation method provided to consumers by data providers is a reasonable method to revoke third party authorization	§ 1033.331(e)	Indicia of reasonableness
Data provider	Whether a data provider has made a record of the data fields that are covered data in the provider's control or possession	§ 1033.351(b)(1)	Sufficient for compliance if (1) doing so is appropriate to the size, nature, and complexity of the data provider's activities and (2) the data fields included identify all the covered data in the data provider's control or possession
Data provider	Whether a data provider has reasonably designed its policies and procedures to ensure its data is accurately made available	§ 1033.351(c)(3)	Indicia of reasonableness
Authorized third party	Whether reauthorization is collected by an authorized third party in a reasonable manner	§ 1033.421(b)(3)	Indicia of reasonableness
Authorized third party	Whether the authorized third party has reasonably designed its policies and procedures to ensure the data it collects is accurately received	§ 1033.421(d)(4)	Indicia of reasonableness

Davis Polk contacts

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Contacts	Phone	Email
Matthew J. Bacal	+1 212 450 4790	matthew.bacal@davispolk.com
Justin Levine	+1 212 450 4703	justin.levine@davispolk.com
Eric McLaughlin	+1 212 450 4897	eric.mclaughlin@davispolk.com
David L. Portilla	+1 212 450 3116	david.portilla@davispolk.com
Gabriel D. Rosenberg	+1 212 450 4537	gabriel.rosenberg@davispolk.com

davispolk.com © 2023 Davis Polk & Wardwell LLP

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.