CONSUMER BANKERS ASSOCIATION
1225 New York Avenue, NW, Suite 1100, Washington, DC 20005
consumerbankers.com

Dodd-Frank Act Section 1033 ("Required Rulemaking on Personal Financial Data Rights") Final Rule Summary

On October 19, 2023, the Consumer Financial Protection Bureau (CFPB) released its notice of proposed rulemaking (NPRM) implementing Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) on personal financial data rights. This proposed rule builds off last year's Small Business Regulatory Enforcement Act (SBREFA) outline on consumers' personal financial data rights.

The relevant text of Section 1033 of the Dodd-Frank Act provides:

> *[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 information shall be made available in an electronic form usable by consumers.*

The CFPB has proposed a rule that would create an open banking-like data sharing ecosystem allowing consumers and the consumer's authorized third parties, including data aggregators that are "retained by" and provide services to those third parties, to access certain information about that consumer from depository institutions and credit card issuers. **Comments on the NPRM are due December 29, 2023. The CFPB expects to finalize the rule by Fall 2024.**

Definitions

Consumer – a natural person

Data Provider – a "covered person" under 12 U.S.C. § 5481(6) that is a financial institution as defined in Regulation E, a card issuer as defined in Regulation Z, or any other person that controls or possess information concerning a covered consumer financial product or service that the consumer obtained from that person.

Third Party – any person or entity that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data

Data Aggregator – an entity that is retained by and provides services to an authorized third party to enable access to covered data

Issues of Note

- ***"Covered data providers" scope remains too narrow.*** As expected, the NPRM explains that the rule covers insured depository institutions and credit card issuers, as well as "other payment facilitation providers," such as "neobanks, digital wallet providers, and similar nondepository entities." CBA had previously urged the CFPB to adopt a broad scope of coverage not only for asset accounts, but also for credit products beyond credit card issuers, like captive auto loan accounts and non-bank credit alternatives, such as Buy Now Pay Later Products. In the NPRM, the Bureau continues to limit its coverage of credit products to just credit card issuers, although the CFPB states it will cover other consumer financial products and services through a supplemental rulemaking.

- ***The scope of the covered data that must be shared with a consumer or authorized third party explicitly includes "Information to initiate payment to or from a Regulation E account."*** This category would include tokenized account and routing numbers that can be used to initiate an Automated Clearing House transaction. The CFPB is also requesting comment on whether data providers should also be required to make available information to initiate payments from a Regulation Z credit card, so there is the risk that this category of "covered data" may expand in the final rule.

- ***Covered data that must be shared with a consumer or an authorized third party also includes APR, payment amount, reward credits, and other "transaction information."*** The NPRM proposes to define the following categories of information as "covered data": (i) transaction information, "such as the payment amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges"; (ii) account balance; (iii) terms and conditions; (iv) upcoming bill information; and (v) basic account verification information. Last year's SBREFA Outline proposed making other categories of information available, including information about prior transactions not typically shown on periodic statements or portals (e.g., consumer reports obtained and used by the bank in deciding whether to provide an account or other financial product or service to the consumer). It appears that the CFPB took CBA's feedback and has eliminated the proposed requirement from the SBREFA Outline to share unnecessary personal information – such as consumer social security numbers and marital status – under the rule.

- ***Data providers would be required to transition to developer interfaces (e.g., application programming interfaces or APIs) to facilitate third parties' access to consumer information.*** The CFPB suggests that this requirement to offer developer interfaces would transition the market away from screen scraping. The CFPB sets a tiered compliance deadline of four tiers for depository institutions, based on asset size. Depository institutions that do not offer online banking or mobile banking applications are exempt from this requirement.

- ***Data providers would be required to apply a data security program that satisfies the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework to their developer interfaces***. Third parties would also be required to certify to consumers that they will apply an information security program that satisfies the GLBA Safeguards Framework or Federal Trade Commission's

(FTC) GLBA Safeguards Rule to their systems for the collection, use, and retention of covered data. However, the CFPB notes in the NPRM that "all or most third parties that would access covered data through a developer interface are regulated by the GLBA Safeguards Framework, most commonly the FTC's Safeguards Rule," so this should be understood as a certification of GLBA compliance, rather than an expansion of the GLBA Safeguards Framework.

- ***The NPRM would prohibit secondary use of consumer data by third parties. Also, third parties would not be able to share covered data with other third parties unless "reasonably necessary to provide the consumer's requested product or service."*** The NPRM specifies that targeted advertising, cross-selling of other products or services, or the sale of covered data is *not* reasonably necessary for a third party to provide a consumer's product or service. Thus, third parties may not use consumer data for these purposes. The NPRM allows utilization of consumer data for "uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability" as well as "servicing or processing the product or service the consumer requested."

- ***Third parties would only be able to maintain access to and retain consumer data for one year, unless the consumer reauthorizes the third party's access.*** Third parties, and data aggregators used by such third parties, would need to establish and maintain systems that could receive data access revocation requests, track duration-limited authorizations, and delete data when required due to a revoked or lapsed consumer authorization.

- ***The entity the consumer provides their authorization to depends on whether the consumer themself or a third party is accessing the consumer's covered data.*** If a third party is accessing the consumer's data from the data provider, the authorization is conducted with the third party. In contrast, if the consumer is accessing information from the data provider directly through the consumer interface (e.g., a bank's online checking website or mobile app), then authorization is performed with the data provider.

- ***Data aggregators used by third parties are bound by the scope of the authorization the consumer granted to the third party. When a third party uses a data aggregator, the data aggregator would be required to certify to the consumer that it agrees to the third party's conditions on accessing the consumer's data.*** The third party, however, would be responsible for notifying other third parties, including data aggregators, when the consumer revokes their authorization and for compliance with third party authorization procedures. The authorization disclosures made to the consumer would be required to include the name of any data aggregator assisting the third party. Although the NPRM states that third parties are obligated to perform authorization procedures with the consumer, the final rule needs a clear, fulsome outline of liability for the parties operating in this data ecosystem.

- ***Data providers are prohibited from imposing fees or charges on a consumer or authorized third party in connection with establishing and maintaining a consumer interface and developer interface. Additionally, the CFPB has proposed minimum performance specifications for developer interfaces.*** A developer interface would need to maintain a response rate of at least 99.5% and a response time of at least 3,5000 milliseconds. Failure of a

developer interface to meet these specifications would mean that the developer interface is not "commercially reasonable."

- ***There is no carve out of the NPRM's requirements for small financial institutions, but compliance dates will be staggered to provide flexibility to smaller institutions.*** The compliance dates would be divided into four tiers. Depository institutions holding at least $500 billion in total assets would be subject to the earliest compliance date, which would be six months after publication of the final rule in the *Federal Register*.

Items for Consideration

CBA recommends that members consider and evaluate the following concerns as they provide feedback to inform CBA's response to the NPRM:

Covered Data - Industry should carefully review the types of information that would need to be shared as "covered data" under the NPRM and whether such data facilitates account transferring. Particular attention should be given to whether credentials for initiating a payment to or from a Regulation E account should be shared.

- Although the CFPB has scaled back on some of the covered data elements that were previously included in the SBREFA Outline, the current "covered data" still needs to be examined for nuances and risks. For example, in sharing information about terms and conditions, data providers would be required to include the applicable fee schedule, an annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement. Additionally, although the NPRM proposes to include information for initiating a payment to or from a Regulation E account (i.e., account and routing numbers, which could, but are not required to, be tokenized), the CFPB is expressly requesting comment on whether data providers could also be required to make available information for initiating payments from a Regulation Z credit card.

Fees - Industry should evaluate whether the CFPB's assessment of the costs is accurate, as well as whether a fee may be necessary for data providers to facilitate the creation of developer interfaces, particularly given the expedited timeline outlined for larger institutions.

- The proposal would prohibit data providers from imposing fees or charges on a consumer or an authorized third party in connection with establishing or maintaining a consumer interface and developer interface. Data providers would also be prohibited from imposing fees or charges in connection with receiving requests or making available covered data in response to a request from a consumer or an authorized third party.

- In effect, data providers (like banks and other depository institutions) are required to subsidize the creation of an entire data access ecosystem, which will result in "upfront and ongoing costs" according to the CFPB, yet the NPRM lacks any meaningful method by which these data providers could recover those costs or otherwise split costs with other data access ecosystem participants. The CFPB notes that it considered "whether its proposed rule should permit a reasonable, cost-based fee to recover the upfront or fixed costs associated with establishing and maintaining the interfaces" but determined that such a fee was unnecessary. This claim should be carefully evaluated given that, according to the CFPB itself, "[i]n 2022, the number of individual instances in which third parties accessed or attempted to access consumer financial accounts *exceeded 50 billion and may have been as high as 100 billion*…" The NPRM does not place significant limits on third parties' access to developer interfaces, so data providers will need to fund the creation of developer portals that will likely need to handle over 100 billion access attempts in a year.

Developer Interface Standards - Industry should review whether the developer interface standards proposed by the CFPB are feasible, as well as identify any practical difficulties in meeting these standards through a developer interface. Additionally, industry should consider whether such standards should be promulgated by industry standard-setting organizations (SSOs) rather than the CFPB.

- According to the NPRM, the CFPB would set performance specifications for developer interfaces, requiring that their performance be "commercially reasonable." The CFPB in the NPRM sets quantitative minimum performance specifications that must be met in order for the performance to be qualify as "commercially reasonable." These standards include requiring a response rate of at least 99.5% and requiring that responses be provided within 3,500 milliseconds. These thresholds were determined based on information the CFPB received from data providers on existing consumer interfaces, as well as the thresholds set in other jurisdictions, such as Australia and the United Kingdom.

Liability - Industry should evaluate the liability implications under Regulation E and the NPRM for data providers and consumers.

- In its discussion of the applicability of other laws to Section 1033, the CFPB notes that "[c]onsumers are protected from liability from these unauthorized transfers under [the Electronic Fund Transfer Act] and Regulation E, although the relevant financial institution may be able to seek reimbursement from other parties through private network rules, contracts, and commercial law." Although the CFPB proposes several measures to mitigate the risk of unauthorized transfers – such as transitioning away from screen scraping, allowing data providers to share tokenized account numbers, and requiring that third parties comply with the GLBA Safeguards Framework – there is still significant risk that consumer information accessed by third parties can subsequently be misused by those third parties or other actors that illicitly gain access.

- It appears that, based on the facts and circumstances, either the data provider or the consumer would be liable for any consumer losses under Regulation E, even though the information that was used to facilitate those losses was accessed through a third party.

Inclusive SSOs Recognized by the CFPB - Industry should evaluate how existing industry SSOs would operate under this new regime, and whether these SSOs are likely to be approved as "fair, open, and inclusive" under the criteria outlined by the CFPB.

- The CFPB notes throughout the NPRM that, for many requirements, indicia of compliance "would include conformance with standards promulgated by fair, open, and inclusive standard-setting bodies recognized by the CFPB." With respect to the requirement that a developer interface must make available covered data in a standardized format, conformance with a format set forth in a qualified industry standard would be deemed to constitute compliance.

- However, for a standard set out by an SSO to be valid for serving as an indicia of compliance, the SSO promulgating such standard would need to apply for recognition by the CFPB, the process for which would include an evaluation by the CFPB into whether the SSO is "fair, open, and inclusive" based on seven factors. These factors include whether "decision-making power is balanced across all interested parties, including consumer and other public interest groups, at all

levels," an openness in membership to including "consumer and other public interest groups with expertise in consumer protection, financial services, community development, fair lending, and civil rights," and adequate due process in the SSO.

Screen Scraping – Industry should evaluate the implications of the transition away from screen scraping applying only to accounts covered by the final Section 1033 rule and likely remaining permissible for non-covered accounts.

- The NPRM would require data providers to prevent third parties from accessing the developer interface using any credentials that a consumer uses to access the consumer interface. This is asserted to effectively transition industry away from screen scraping. However, the NPRM defines "covered consumer financial product or services" to mean Regulation E accounts, Regulation Z credit cards, and facilitation of payments from a Regulation E account or Regulation Z credit card. As a result, to the extent that screen scraping is limited, it is only limited in connection with accounts covered by a Section 1033 final rule, and presumably would continue to exist in the marketplace for other non-covered accounts.

Section by Section

General

- **§ 1033.111 – Coverage of Data Providers**
  - A "data provider" includes the following entities:
    - A financial institution, as defined in Regulation E;
    - A card issuer, as defined in Regulation Z; and
    - "Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person," which would include digital wallet providers.
  - Depository institutions that do not have an interface through which they receive requests for covered data and make available covered data in an electronic form usable by consumers are excluded from coverage.
  - Other accounts, such as captive auto loan accounts and non-bank credit alternatives like Buy Now Pay Later products are not covered by the NPRM.

- **§ 1033.121 – Compliance Dates**

Data Providers		Compliance Date
Depository Institutions	**Nondepository Institutions**	
$500 billion in total assets or greater	Generated $10 billion in revenue in preceding calendar year or are projected to generate at least $10 billion in revenue in current calendar year	Six months after publication of final rule in *Federal Register*
$500 billion - $50 billion in total assets	Generated less than $10 billion in revenue in preceding calendar year or are projected to generate less than $10 billion in revenue in current calendar year	One year after publication of final rule in *Federal Register*
$50 billion - $850 million in total assets	N/A	Two and a half years after publication of final rule in *Federal Register*
$850 million in total assets or less	N/A	Four years after publication of final rule in *Federal Register*

- **§ 1033.141 – Standard Setting**
  - SSOs may request that the CFPB recognize it as an "issuer of qualified industry standards." If an SSO is recognized as such and the CFPB deems the SSO is "fair, open, and inclusive," then indicia of compliance with various provisions of Section 1033 would include conformance with standards promulgated by that SSO.
  - The CFPB outlines seven factors it will consider in determining whether a "standard-setting body is fair, open, and inclusive and is an issue of qualified industry standards": (i) openness; (ii) balance; (iii) due process; (iv) appeals; (v) consensus; (vi) transparency; and (vii) CFPB recognition.

Obligation to Make Covered Data Available

- **§ 1033.201 – Obligation to Make Covered Data Available**
  - Data providers would be required to make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a consumer financial product or service the consumer obtained from that data provider.
  - Data providers are obligated to make available the most recently updated covered data, including authorized but not yet settled debit card transactions.

- **§ 1033.211 – Covered Data**

Category of "Covered Data"	What Category Consists Of
Transaction information, including historical transaction information in the control or possession of the data provider	Amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges. Data providers are deemed to have made available sufficient historical transaction information if it makes available at least 24 months of such information.
Account balance	Includes available funds in an asset account and any credit card balance. The CFPB requests comment on whether this term is sufficiently defined or whether additional examples of account balance, such as the remaining credit available on a credit card, are necessary.
Information to initiate payment to or from a Regulation E account	This includes a tokenized account and routing number that can be used to initiate an ACH transaction. In complying with this obligation, a data provider is permitted to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number. *Note*, the CFPB is requesting comment on whether data providers should also be required to make available information to initiate payments from a Regulation Z credit card.
Terms and conditions	Includes applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.
Upcoming bill information	Includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.
Basic account verification information	Limited to name, address, email address, and phone number.

- **§ 1033.221 – Exceptions**
  - There are four categories of covered data that data providers do not need to make available to a consumer or an authorized third party: (i) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors; (ii) any information collected for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct; (iii) information required to be kept confidential by any other provision of law; and (iv) any information that cannot be retrieved by the data provider in the ordinary course of its business with respect to that information.

Data Provider Interfaces; Responding to Requests

- **§ 1033.301 – General Requirements**
  - Data providers are obligated to maintain both a consumer interface and a developer interface. Both interfaces must be able to make available to a consumer or an authorized third party covered data in a machine-readable file that can be retained and transferred for processing into a separate information system.
    - A "consumer interface" is defined as "an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by consumers in response to the requests."
    - A "developer interface" is defined as "an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by authorized third parties in response to the requests."
  - Data providers are specifically prohibited from imposing any fees or charges on either the consumer or the authorized third party in connection with establishing or maintaining the interfaces, and in connection with receiving requests or making covered data available.

- **§ 1033.311 – Requirements Applicable to Developer Interface**
  - *Standardization:* The developer interface must make available covered data in a standardized format, meaning the data must be made available in a format set forth in a qualified industry standard or, if there is no such standard, in a format widely used by developer interfaces of other similarly situated data providers.
  - *Performance Specifications*: The performance of a developer interface must be commercially reasonable. Performance is commercially reasonable if its response rate is equal to or greater than 99.5% and the response time may not be more than 3,500 milliseconds. Moreover, a data provider may not unreasonably restrict the frequency with which it receives and responds to requests.
  - *Security Specifications*: Data providers must not allow third parties to access the developer interface using any credentials that a consumer uses to access the consumer interface. This would effectively end screen scraping.

- **§ 1033.321 – Interface Access**
  - Data providers may reasonably deny a consumer or third-party access to an interface based on risk management concerns. The denial must be, at a minimum, directly related to a specific risk, and must be applied in a consistent and non-discriminatory manner.

- Data providers have a reasonable basis to deny access to a third party if:
  - The third party does not present evidence that its data security practices are adequate to safeguard the covered data; or
  - The third party does not make the following information available to the public, meaning it must at least be as available as it would be on a public website: (i) the third party's legal name and any assumed name it is using while doing business with the consumer; (ii) a link to its website; (iii) its Legal Entity Identifier; and (iv) contact information a data provider can use to inquire about the third party's data security practices.

- **§ 1033.331 – Responding to Requests for Information**
  - Data providers need to make covered data available to a consumer upon receiving information sufficient to authenticate the consumer's identity and identify the scope of data requested.
  - Data providers need to make covered data available to an authorized third party upon receiving information sufficient to authenticate the consumer's and third party's identities, confirm the third party has followed the appropriate authorization procedures, and identify the scope of data requested.
    - Data providers may confirm the scope of a third party's authorization by asking the consumer to confirm which account(s) the third party is seeking to access and the categories of covered data the third party is requesting to access.
  - Data providers are not required to make covered data available in response to a request when either a withholding exception applies, the data provider believes there is a risk management concern, the data provider's interface is not available, or in circumstances when a third party's authorization has been revoked or expired.
  - The foregoing obligations to make covered data available to consumers and authorized third parties apply to accounts that are jointly held.
  - Data providers can make available to consumers a method of revoking a third party's authorization, and must notify the authorized third party if it receives a request from a consumer to revoke that third party's access.

- **§ 1033.341 – Information about the Data Provider**
  - Data providers must make the following information about itself readily identifiable to members of the public, meaning at least as available as it would be on a public website, in human-readable and machine-readable formats: (i) legal name and, if applicable, any assumed name used while doing business with the consumer; (ii) a link to its website; (iii) its Legal entity Identifier; and (iv) its contact information that enables a consumer or third party to receive answers to questions about accessing covered data.
  - Data providers must also disclose 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 developer interface.
  - Data providers must disclose the quantitative minimum performance specification that the data provider's developer interface achieved in the previous calendar month. The disclosure must include at least a rolling 13 months of the required monthly figure.

- **§ 1033.351 – Policies and Procedures**
  - Data providers must have written policies and procedures, and these must be reasonably designed to ensure that the data provider creates a record of the data fields that are covered data, what covered data are not made available, and the reasons that such covered data was not made available. Data providers must also create records when denying a third party access to a developer interface and denying a request for information.
  - The policies and procedures must be reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface.
  - Records related to a data provider's response to a consumer's or third party's request for information, or a third party's request to access a developer interface, must be retained for at least three years after a data provider has responded to the request. These records include records of a request for a third party's access to the interface, records of requests for information, copies of a third party's authorization, and records of actions taken by a consumer and a data provider to revoke a third party's access.

Authorized Third Parties

- **§ 1033.401 – Third Party Authorization; General**
  - Third parties seeking access to covered data from a data provider must: (i) provide the consumer an authorization disclosure; (ii) provide a statement to the consumer certifying that the third party agrees to its obligations; and (iii) obtain the consumer's express informed consent to access covered data that is signed by the consumer electronically or in writing.

- **§ 1033.411 – Authorization Disclosure**
  - The authorization disclosure must be provided by the third party to the consumer electronically or in writing, and must be clear, conspicuous, and segregated from other material.
  - The authorization disclosure must include the following information:
    - The name of the third party;
    - The name of the data provider;
    - A brief description of the product or service that the consumer has requested and a statement that the third party will collect, use, and retain the consumer's data only for that purpose;
    - The categories of covered data that will be accessed;
    - The certification statement acknowledging the third party agrees to its obligations; and
    - A description of the revocation mechanism.
  - The authorization disclosure must be in the same language in which the third party and consumer were communicating. If it is in a language other than English, it must include a link to an English-language translation.

- **§ 1033.421 – Third Party Obligations**
  - The third party must limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer with the requested product or service.
    - Other permissible uses of covered data include:

- Uses that are specifically required under other provisions of law;
- Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and
- Servicing or processing the product or service.

  - It is prohibited using covered data for the following purposes:
    - Targeted advertising;
    - Cross-selling of other products and services; or
    - The sale of covered data.

- Covered data collected by a third party can be maintained for a maximum period of one year after the consumer's most recent authorization. Collecting covered data beyond the one-year period requires the third party to obtain a new authorization from the consumer.
  - If the consumer does not reauthorize the third party, the third party must no longer collect covered data pursuant to the most recent authorization, and no longer use or retain covered data previously collected, unless such use or retention is necessary for providing the product or service.
- Limitations on the use of covered data apply to third parties the consumer engages with as well as use of data by other third parties.
- Third parties need to establish and maintain written policies and procedures to ensure covered data are accurately received and accurately provided to another third party.
- Third parties must apply to its systems for collection, use, and retention of covered data an information security program that satisfies GLBA or, if not subject to GLBA, the FTC's Standards for Safeguarding Customer Information.
- When sharing covered data with another third party, the third party must require the other third party by contract to comply with the original third party's obligations.
- The third party must provide the consumer a copy of the signed authorized disclosure and provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. The third party must be able to, upon request provide the consumer the following information about the third party's access to the consumer's covered data:
  - 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 and verification the third party has adhered to a request for revocation.
- The third party must provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's covered data, and ensure the consumer is not subject to costs or penalties for revoking authorization.
  - Third parties are responsible for notifying the data provider, any data aggregator, and other third parties they have provided the consumer's covered data when the consumer has revoked authorization.
  - Upon receipt of a consumer's request to revoke authorization, the third party may no longer collect covered data or use or retain covered data previously

collected unless the use or retention is reasonably necessary to provide the product or service.

- **§ 1033.431 – Use of Data Aggregator**
  - Data aggregators can perform authorization procedures with consumers on behalf of the third party, but the third party remains responsible for compliance with the authorization procedures.
  - The authorization disclosure must include the name of any data aggregator that the third party will be using to access covered data, as well as a brief description of the services that data aggregator will provide.
    - The data aggregator must certify to the consumer that it agrees with the conditions on access the consumer's data.
    - In these instances, the third party must include the data aggregator certification in the authorization disclosure or the data aggregator must provide the certification to the consumer in a separate communication.

- **§ 1033.441 – Policies and Procedures for Third Party Record Retention**
  - A third party must establish and maintain written policies and procedures to ensure retention of records evidencing compliance. Records must be maintained for no less than three years after a third party obtains the consumer's most recent authorization.
  - The third party must retain a copy of the signed authorization disclosure, and a record of actions taken by the consumer, including actions taken by the consumer through a data provider, to revoke the authorization.
    - If the third party uses a data aggregator, the third party must retain a copy of any data aggregator certification statement provided to the consumer separate from the authorization disclosure.