December 29, 2023

Via www.regulations.gov

Consumer Financial Protection Bureau
1700 G Street, N.W.
Washington, DC 20552

RE: Required Rulemaking on Personal Financial Data Rights; Docket No. CFPB-2023-0052, RIN 3170-AA78

Ladies and Gentlemen:

Mastercard International Incorporated ("Mastercard") submits this comment letter to the Consumer Financial Protection Bureau ("CFPB") in response to the proposed rule on personal financial data rights (the "Proposed Rule"),[1] which would implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Section 1033").[2] Mastercard appreciates the opportunity to provide comments on the Proposed Rule.

Background on Mastercard

Mastercard is a technology company in the global payments and open banking industries. Mastercard operates the world's fastest payments processing network, connecting consumers, financial institutions, merchants, governments, and businesses in more than 210 countries and territories. Moreover, Mastercard powers an interoperable and feature rich open banking and open finance platform globally, and through its subsidiary in the United States, Finicity Corporation ("Finicity"). Mastercard open banking provides secure and trusted information and services, which power economies and empower people—consumers and businesses alike—with innovative tools to leverage their own data for their own financial benefit. Mastercard's experience facilitating global payments and cross-border transactions also allows us to create interoperability between different open banking and open finance markets around the world.

Mastercard believes there is immense value in connecting consumers and small businesses with their financial data and providing them with the tools to do so for their own benefit. Mastercard's own data responsibility principles form the foundation of our approach to open banking and align in many ways with the Proposed Rule. Put simply, we believe that consumers and businesses own their data; have the right to control their data and to benefit from their data's use; and that Mastercard's job is to protect the data of consumers and small businesses. We also believe that data, particularly data that has been de-identified, plays a

[1] 88 *Fed. Reg.* 74,796 (Oct. 31, 2023).

[2] 12 U.S.C. § 5533.

pivotal role in allowing industry to innovate constantly to ensure individuals benefit from the use of their data through better experiences, products and services.

As a data aggregator, Finicity is a leader in the U.S. open banking industry in application programming interface ("API")-based connectivity to access data, and provides a myriad of other services to both authorized third parties and data providers big and small. We have been working with our customers and partners to enable a more secure data sharing method as banks make APIs available and believe that the Proposed Rule will significantly speed this transition. In this, data aggregators provide consumers with far more than just a conduit between data providers and authorized third parties. In today's open banking market, third parties referred to as data aggregators operate in different models. Some operate to provide services solely to authorized third parties. Others, such as Finicity, operate to provide services to authorized third parties but also to provide open banking services directly to consumers. With a holistic approach to serving the consumer financial ecosystem, these data aggregators enable a secure and transparent experience that has a positive impact on the consumer.

Comments

The open banking industry has experienced remarkable development over the past several years. This change has enabled consumers to benefit from new opportunities and to leverage their financial data in new and innovative ways. As consumers adopt and demand more personalized digital tools to save time and money, and look to improve their financial outlook, financial services innovators utilize open-banking solutions to drive stronger consumer engagement and loyalty. The growth of the U.S. open banking market is so robust because consumer demand for better, faster, less expensive and more efficient financial services has been met by participants in the open banking ecosystem partnering to collectively deliver seamless connectivity and innovative financial products that give consumers control over and access to their financial data. Mastercard believes that ensuring consumers have access to their data is of the utmost importance. Doing so empowers consumers to benefit from their financial data through a wide variety of third-party apps and services that utilize the data to offer new experiences. We also believe that consumer data ownership and access rights are foundational to open banking as they are foundational to build trust in the broader financial ecosystem.

Mastercard supports the CFPB's efforts to develop a rule implementing consumer data access rights under Section 1033 that balances consumer data ownership and access rights with the potential disruption a rule could impose on the very ecosystem model and practices that are delivering innovative open banking products and services to consumers today. We offer comments that are intended to enhance aspects of the Proposed Rule and mitigate any unintended consequences that could harm consumers. Mastercard's comments address the following topics: (i) clarification that data aggregators may operate as authorized third parties if they comply with the obligations that apply to authorized third parties; (ii) consistency of the Proposed Rule with existing laws concerning the limitations on collection, use and retention of covered data; (iii) support for reliance on qualified industry standards and a call for the CFPB to begin recognizing standard-setting bodies; (iv) additional granularity on covered data so that consumers can access the information they need to receive their requested open banking products and services and a request to implement Section 1033 in one rulemaking; (v) changes to the authorization practices to make them more practical for the industry; (vi) a proposed timeframe in which data

aggregators and authorized third parties may come into compliance with the final rule that the CFPB issues to implement Section 1033 (the "Final Rule"); (vii) support for the performance specification; and (viii) a remediation process to be set forth in qualified industry standards to address situations in which data providers deny access based on risk management grounds. Below we discuss our comments in more detail.

I. *Dual Role of Data Aggregators as Authorized Third Parties*

The Proposed Rule defines roles for data providers, authorized third parties and data aggregators but appears to contemplate a narrower role for data aggregators than they in fact play in the industry today. The CFPB recognizes in the supplementary information to the Proposed Rule that many third parties rely on data aggregators to assist with accessing and processing consumer financial data,[3] and we believe the interdependence between data aggregators and other third parties will only expand based on the requirements in the Proposed Rule. However, the business model of some data aggregators encompasses more than this, and some data aggregators currently do and in the future could provide important value-added services to consumers in addition to authorized third parties.

It is unclear how the Proposed Rule would apply to a data aggregator that provides disclosures to, and obtains consents from, consumers. One could infer from the Proposed Rule that a data aggregator is limited to acting on behalf of a third party seeking authorization and may not itself seek authorization. Accordingly, Mastercard requests that the CFPB expressly clarify that data aggregators may be authorized third parties so long as they comply with all of the obligations that apply to authorized third parties, such as giving authorization disclosures and obtaining consents. The CFPB could do so by making modifications when it issues the Final Rule, such as:

- Adding to the definition of "authorized third party" in Section 1033.131 a sentence that states: "An authorized third party may include a data aggregator."

- Adding to the definition of "data aggregator" in Section 1033.131 a sentence that states: "A data aggregator may be an authorized third party."

- Clarifying in Section 1033.421(a) that, while third parties operating as data aggregators may perform the authorization procedures on behalf of third parties, they may also do so on their own behalf when operating as an authorized third party.

II. *Data Usage*

Section 1033.421(a) of the Proposed Rule would require that an authorized third party or data aggregator limit its collection, use, and retention of covered data to what is "reasonably necessary to provide the consumer's requested product or service."

[3] 88 *Fed. Reg.* at 74,841.

A. Avoidance of Layered Federal Financial Privacy Protections

The CFPB should not impose new financial privacy regulations on the collection, use and retention of covered data where other laws already address such activities from a financial privacy perspective. This is essential to maintaining a fair and level playing field in the regulatory treatment of these activities irrespective of whether consumers give their financial information directly to a provider of financial services or authorize a provider of financial services to retrieve the consumer's financial information via open banking. Relying on the existing financial privacy protections that apply to the collection, use and retention of covered data would also provide legal certainty and maximize competition, which would result in benefits to consumers and align with the stated aims of the Proposed Rule.

Authorized third parties and data aggregators already are subject to the Gramm-Leach-Bliley Act and its implementing regulation, Regulation P, either as a result of providing financial products and services to consumers or acting as a service provider to a person that does. Regulation P imposes limitations on the disclosure of nonpublic personal information to nonaffiliated third parties by financial institutions and their service providers and limitations on the use and disclosure of nonpublic personal information by service providers that receive nonpublic personal information under certain exceptions to the restrictions on disclosure. Also, Regulation P and the Federal Trade Commission's Safeguards Rule[4] already impose information security requirements on authorized third parties and data aggregators. In addition, a third party that is a consumer reporting agency, such as a Finicity, already is subject to the Fair Credit Reporting Act and its restrictions on use of data.

The Proposed Rule would subject authorized third parties and data aggregators to an additional layer of financial privacy regulations that do not apply to other types of financial services providers despite that the consumer financial information they collect is exactly the same information that they could collect directly from consumers and that consumers have willingly provided to financial services providers for many years in paper form by mail and in electronic form by fax, email and website upload. Accordingly, we ask that the CFPB rely on the existing rules that protect consumer financial data on collection, use and retention when it issues the Final Rule instead of including any such limitations in the Final Rule.

B. Permitted Collection, Use and Retention

While we urge the CFPB not to impose new financial privacy requirements on authorized third parties and data aggregators merely because of the manner in which they collect consumer financial data, if the CFPB determines that it will retain restrictions on collection, use and retention when it issues the Final Rule, Mastercard encourages the CFPB to amend the Proposed Rule in four key ways.

[4] 16 C.F.R. Pt. 314.

1. *De-identified Data*

The Proposed Rule does not, but should, carve-out de-identified data from the definition of covered data so that authorized third parties and data aggregators may use de-identified data without limitation. Not doing so would work against consumer interests by limiting product improvements and development, inhibiting the improvement of fraud prevention services and stifling innovation overall. De-identified data is used widely in the financial services industry for business purposes that benefit consumers, including to develop new or enhanced products and services, and to provide products and services that benefit from an understanding of consumer financial behavior without the need to identify any consumers. For example, data can be used to mitigate insufficient funds risk in recurring payments and to address synthetic identity risk (*i.e.*, the risk that an identity is based on fabricated or synthetic credentials not associated with a real person).

Regulation P excludes from its scope "[i]nformation that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses."[5] State privacy laws also exclude de-identified data from their scope. In order to address the risk of re-identification, state privacy laws have adopted an approach of requiring entities to (a) take reasonable measures to ensure that a person cannot associate the de-identified data with an individual, (b) publicly commit to maintain and use the data only in de-identified form and not attempt to re-identify the data, and (c) contractually obligate recipients of the de-identified data to abide by the same requirements. This aligns with long-standing guidance from the Federal Trade Commission and is an approach Mastercard would support in the Final Rule.

The lack of a carve-out for de-identified data in the Proposed Rule creates an inconsistency between the Proposed Rule and other settled laws governing consumer data use. We urge the CFPB to maintain consistency and provide legal certainty by expressly permitting the use of de-identified data when it issues the Final Rule. Doing so would create a level playing field among financial services providers and entities providing products in other industries that are subject to privacy regulations.

2. *Development and Enhancement of Products and Services*

The CFPB should also clarify that a "reasonably necessary" use of covered data includes developing, improving and enhancing products and services. For context on this point, covered data can be used to provide products and services that allow for identity and account verification and security and fraud prevention. Another important use of this data is in support of model validation and self-testing to minimize bias in models and analytics used to provide products and services. These types of models and analytics can be used by authorized third parties to expand credit opportunities to underbanked consumers.

Use of covered data to develop and improve services like these that benefit consumers is critical to continued growth and innovation in the open banking industry and its ability to

[5] 12 C.F.R. § 1016.3(q)(2)(ii)(B).

provide better services over time. To be clear, we do not believe that the services offered today would have been capable of being developed without the use of covered data. Additionally, the development of future models, products and services with which consumers can use their data and from which they benefit will be nearly impossible to provide under the Proposed Rule without clarification that "reasonably necessary" use of covered data does in fact include the improvement, development and enhancement of products and services.

3. *Fraud*

Section 1033.421(c)(2) of the Proposed Rule contains an exemption from the limitations for uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability. We support the inclusion in the Proposed Rule of this exemption and urge the CFPB to ensure that, in the Final Rule, it is broad enough to encompass the use of covered data in future fraud models.

We have previously mentioned uses of covered data for enhancing fraud prevention services. Other examples of fraud prevention services include the use of data from a cross section of consumers' open banking activity from multiple financial institutions to indicate patterns of behavior that can demonstrate systemic issues in financial ecosystem security, *e.g.*, the security of or threat vectors to API channels. Permissioned identification information is used today for identity and account verification and for identifying and reporting suspicious activity. Accordingly, we urge the CFPB to make clear that a permitted use of covered data can be to enhance the safety and security of the open banking and financial ecosystem and that it is "reasonably necessary" to provide the consumer's requested product or service.

4. *Opt In*

Finally, the CFPB should give consumers the right to allow their data to be used for any purpose for which they provide consent so long as the uses have been fully and accurately disclosed to them. Such an explicit opt-in approach would be consistent with the policy underlying Section 1033 because it would give consumers ultimate control over their financial data and could be done through a transparent process.

This approach is also important to enable authorized third parties or data aggregators to innovate and provide additional consumer-benefitting services and tools that are broader in scope than those reasonably necessary to providing a requested product or service. For example, a data aggregator may have a tool available to consumers that would give consumers a consolidated view of linked accounts and account access by authorized third parties, so that those consumers could control and manage access to their data in one centralized location. Consumers could use a tool like this to manage consents, account-linking, data share authorizations and revocations.

III. *Qualified Industry Standards*

Mastercard supports the CFPB's approach of incorporating qualified industry standards issued by CFPB-recognized standard-setting bodies into the Proposed Rule. We offer two specific comments in this section on the use of qualified industry standards and, elsewhere in this

letter, we suggest other elements of the Proposed Rule in which the CFPB could incorporate qualified industry standards.

A. Recognition of Standard-Setting Bodies

We believe that industry standard-setting bodies are best positioned to develop and maintain standards that meet the needs of the market and facilitate innovation. Mastercard is specifically supportive of API standards developed by the Financial Data Exchange ("FDX"). FDX provides the tools for secure and reliable financial records access and we encourage the CFPB to officially recognize FDX as an issuer of qualified industry standards.

Regarding recognition, we are concerned about the timing of publication of qualified industry standards in relation to the CFPB's rule making process. Participants in the open banking ecosystem will need to rely on qualified industry standards as they build their infrastructure and plan for compliance with the Final Rule. This work will need to be done before the Final Rule becomes effective. Thus, it is important that ecosystem participants know the relevant qualified industry standards and standard-setting bodies before the Final Rule goes into effect. For this reason, the CFPB should begin recognizing standard-setting bodies as issuers of qualified industry standards as soon as practicable, taking into consideration the deadlines for compliance with the Final Rule.

B. Compliance via Qualified Industry Standards

In order for qualified industry standards bodies to be utilized fully in relation to the Final Rule, Mastercard encourages the CFPB to make compliance with qualified industry standards a safe harbor for compliance with the requirements in the Final Rule, instead of using compliance with qualified industry standards as indicia of compliance We note that the Proposed Rule already (i) "deems" a data provider to comply in Section 1033.311(b)(1) with the requirement to make available a developer interface if the interface makes available covered data in a format that is set forth in a qualified industry standard and (ii) "permits" a data provider to comply with the requirement to incorporate data fields in the data provider's control or possession into its policies and procedures pursuant to Section 1033.351(b)(1) by incorporating the data fields defined by a qualified industry standard, provided doing so is appropriate to the size, nature, and complexity of the data provider's activities. The CFPB should adopt this approach for all other references to compliance with qualified industry standards when it issues the Final Rule.

A full safe harbor for compliance will provide certainty and clarity to market participants and provide incentives for them to invest in this space. Otherwise, some participants may not expend the resources to adhere to qualified industry standards if doing so could still result in noncompliance with regulatory requirements. We believe creating a safe harbor will maximize uniformity and the quality of the consumer experience.

IV. *Scope of the Proposed Rule*

A. Data Providers and Covered Consumer Financial Products or Services

The CFPB chose to prioritize Regulation E accounts, Regulation Z credit cards and payment facilitation products and services as being within scope of the Proposed Rule through the definitions of "data provider" and "covered consumer financial product or service." The supplementary information to the Proposed Rule recognizes that there are covered persons under Section 1033 that typically share information concerning financial products and services that are not currently within the scope of the Proposed Rule, such as those covered persons that offer mortgages, automobile loans and student loans.[6] The CFPB noted that it plans to bring these covered persons within scope of the rule through a supplemental rulemaking.[7]

Mastercard agrees with the CFPB that its current proposal covers a majority of the data currently in use in the market today in open banking. However, the expansion of the open banking ecosystem in recent years shows how quickly different types of consumer financial data are being used in new and innovative ways. Consequently, Mastercard believes that the CFPB should not wait for a supplemental rulemaking to implement Section 1033 with respect to the other covered persons that will ultimately be subject to its requirements at a later date. We recognize that the CFPB excluded some types of consumer financial services because the information involved in those services does not typically support transaction-based underwriting across a range of markets or payment facilitation. Other types of financial data are outside of CFPB's jurisdiction and similar consumer rights will need to be conferred upon uses of these services by other regulators. However, if the CFPB issues the Final Rule in the phased approach described in the Proposed Rule, the CFPB will create a two-tiered marketplace for access to data even within its own jurisdiction. This could cause consumer confusion. It could also have other unintended consequences, such as imposing unnecessary burdens on authorized third parties and data aggregators and perpetuating the use of consumer credentials.

To be clear, the information concerning financial products and services that would not be covered in the Final Rule but that is within the scope of Section 1033, such as mortgages, automobile loans and student loans, will still be needed to provide open banking products and services requested by consumers. Authorized third parties and data aggregators may have to use different infrastructure to obtain such information if a data provider does not make it available through a developer interface. We believe that the best solution to benefit all participants in the open banking ecosystem would be for the CFPB to implement Section 1033 in the Final Rule with respect to all covered persons, rather than a subset, and forego any supplemental rulemaking. If the CFPB does not do so, however, the CFPB should clarify that existing market practices should be permitted to continue to ensure access to the full array of data that is currently available for any categories of information that would be out of scope of the Final Rule.

---

[6] 88 *Fed. Reg.* at 74,804.

[7] *Id.*

Also, products and services will continue to evolve and will likely result in new forms of data being available to consumers that are not currently in use. We encourage the CFPB to set a date in the future when it will review the scope of data providers and covered consumer financial products or services issued in the Final Rule to determine what other forms of financial data may be in use by consumers at that point in time and be appropriate for incorporation into the Final Rule.

Finally, there is uncertainty in the open banking industry about whether certain participants will be considered data providers as a result of controlling or possessing information concerning the facilitation of payments from a Regulation E account or Regulation Z credit card. To address this uncertainty, the CFPB should provide additional examples of entities or businesses that would be subject to the Final Rule under these prongs of the definitions of "data provider" and "covered consumer financial product or service."

B. Scope of Covered Data

Section 1033.211 of the Proposed Rule defines "covered data," which must be made available by data providers, using six broad categories with examples. We believe these categories cover most data used in the market today and do not think these categories need expansion, but we urge the CFPB to be more granular in its approach to defining the covered data in these categories to ensure that consumers can access the data needed today to receive the products and services they request. As with our comment above related to the scope of data providers, we also encourage CFPB to set a date in the future when it will review the scope of covered data to determine if any additional clarity is needed. Below are examples of specific data elements and concepts that the CFPB could include in a more granular approach to its existing "covered data" categories when it issues the Final Rule:

- The "covered data" element in Section 1033.211(d) of the Proposed Rule is the terms and conditions for an account. The CFPB recognizes that certain elements from terms and conditions are important and are included in a list of examples of data that must be provided—the 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. Another data element often found in terms and conditions is a consumer's credit limit. Together with the other data elements from the terms and conditions referred to above, the credit limit is an important factor for consumers when choosing their products and services. In the use case of enabling competitive products for the consumer, knowing a consumer's existing credit limit can be a key factor.

- The "covered data" element in Section 1033.211(e) of the Proposed Rule is upcoming billing information. Mastercard is interested to know if this category includes remittance details (*e.g.*, the account details of a payee for any scheduled payments). Remittance details are important to enabling bill payments, *e.g.*, a consumer paying a credit card bill. Without the remittance details, a payment to the biller cannot be set up or reconciled.

- The presence of additional authorized users, co-signers or joint account owners on an account is another example of data we believe is included in the existing categories of

covered data. This information helps to improve verification of account ownership when opening an account, applying for a loan or enabling account-based payments.

- Mastercard seeks clarity on whether an electronic copy of a consumer periodic statement is currently considered covered data. Some lenders or investors who buy loans require the actual statement to be included in the loan file as proof of documentation of assets or income. These lenders and investors may not accept verification reports provided by open banking providers in lieu of the statement itself. On this point, Section 1033.301(b) of the Proposed Rule would require a data provider, upon request, 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. If this is intended to mean that an electronic copy of a consumer periodic statement is covered data, then the CFPB should clarify this provision.

- Another area where granularity could be helpful is around the "covered data" element in Section 1033.211(c) of the Proposed Rule describing information to initiate a payment to or from a Regulation E account. The CFPB explains that a data provider may comply with its obligation to provide this element by making available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number. The CFPB may wish to clarify whether any tokenized information that is provided should allow authorized third parties and data aggregators all of the same functionality as receiving non-tokenized information. In other words, does the CFPB intend that there should be parity between tokenized and non-tokenized information included in covered data?

- The Proposed Rule also permits a data provider not to make available "[a]ny information that the data provider cannot retrieve in the ordinary course of its business with respect to that information." We recognize that this is a statutory exception from Section 1033, but it is unclear what it means for a data provider to not be able to retrieve information in the ordinary course of its business. We believe this is an area where additional clarity would be helpful.

V. *Authorization*

A. One-Year Maximum Reauthorizations and Payments Use Cases

Sections 1033.421(b)(2) and (3) of the Proposed Rule would set the maximum duration of an authorization at one year after the consumer's most recent authorization and require that a third party obtain a new authorization annually to continue to collect covered data beyond each one-year period. In the supplementary information to the Proposed Rule, the CFPB discussed the range of comments that it received on imposing a maximum duration during its Small Business Regulatory Enforcement Fairness Act process. The CFPB sought to strike a balance between longer term use and frequent reauthorizations. Specifically, the supplementary information to the Proposed Rule states that some commenters stated that a maximum duration

would result in undesired loss of services for consumers or frustration of consumer intent.[8] The CFPB also recognizes that some products or services, like bill pay, overdraft prevention, or personal financial management, require long-term access and that a maximum duration may not be sufficient to ensure that third parties act on behalf of consumers over the longer term.[9]

We recognize the importance of consumers periodically being made aware of where their data is being used and for what purposes. While we believe that a one-year maximum authorization is an appropriate requirement for some use cases, we are also concerned that this provision could have unintended consequences for other use cases. These consequences could be especially burdensome on payments use cases. In a payments use case, a consumer, on an ongoing basis, authorizes a payment to be made from the consumer's account, exemplified by recurring bill payments for mortgages or utility bills, or schedules receipt of a payment into the consumer's account, exemplified by account-to-account payment of wages, such as for a rideshare driver. In either case, a consumer could fail to make or receive a payment when otherwise expected.

In lieu of reauthorization for payments use cases, we encourage the CFPB to consider alternative approaches to remind consumers of the way their data is being used. For example, the CFPB could allow authorized third parties to end additional collection of consumer data after one year without reauthorization but allow the retention and continued use of a tokenized account number for payments. Additionally, the CFPB could require an annual notice to be given by each authorized third party using consumer data for payments data that describes the purpose for which such authorized party is accessing the covered data and enables the consumer to revoke the related authorization. Such an annual notice could be defined by qualified industry standards bodies to ensure consistency. This would provide the same transparency as the consumer would receive through a reauthorization but would be a more practical way to reduce the risk of consumer harm. We thus request that the CFPB not impose a maximum duration to retain and use data for payment use cases and instead consider these alternative approaches.

B. Authorization by Third Parties

While Mastercard believes that data providers play a critical and necessary role in the initial authentication of a consumer, we encourage the CFPB to clarify that authorization for consumer requested products and services must be carried out only by third parties or data aggregators acting on their behalf. Section 1033.331(b)(1)(iii) of the Proposed Rule would include as a condition to a data provider making available covered data that the data provider must receive information sufficient to confirm that a third party has followed the Proposed Rule's authorization procedures. In the supplementary information to the Proposed Rule, the CFPB states that it preliminarily determined that data providers should confirm the third party's authorization with the consumer and that this condition would be satisfied where the data provider receives a copy of the authorization disclosure the third party provided to the consumer

[8] 88 *Fed. Reg.* at 74,835.

[9] *Id.*

and that the consumer has signed.[10] We understand this to mean that before providing access to a consumer's covered data, data providers must confirm the third party's authorization with the consumer.

Mastercard recognizes the importance of data providers being able to limit the scope of data available to third parties and that data providers have an interest in data security and a need to manage risk. However, an express requirement for a data provider to confirm the authorization during a real-time open banking transaction is likely to create friction and a negative consumer experience by slowing the authorization process.

C. Data Aggregator Requirements

When an authorized third party uses a data aggregator, Section 1033.431(b) of the Proposed Rule would require that the authorized third party's authorization disclosure must include the name of any such data aggregator and a brief description of the services the data aggregator will provide. The CFPB should defer to qualified industry standards to set the requirements for descriptions of data aggregator services.

The data aggregator used by an authorized third party would also have to make certifications to the consumer as set forth in the Proposed Rule. Section 1033.431(c) of the Proposed Rule would also require that if an authorized third party retains a data aggregator after the consumer has completed the authorization procedures, the new data aggregator must also satisfy the requirement to provide certification. The CFPB should clarify what steps must be taken by such a new data aggregator as to existing consumer customers of an authorized third party, whether the authorized third party begins to rely on a data aggregator for the first time or changes from one data aggregator to another. We especially encourage the CFPB to ensure the required steps when an authorized third party switches a data aggregator are not so burdensome that they limit competition or make it too difficult for a third party to switch aggregators. Mastercard believes that an authorized third party should be permitted to comply with this obligation by posting the data aggregator's certifications on the authorized third party's website in a manner consistent with qualified industry standards. The proposed disclosures to existing customers are likely to be challenging for the authorized third party or new data aggregator and unlikely to be helpful to consumers.

D. Account-by Account Authorization

Consumers may have more than one account at the same data provider. When this is the case, we encourage the CFPB to ensure that a consumer must check a box or take a similar step to expressly select the accounts for which the consumer is granting access. Such a requirement could be defined by qualified industry standards. This is important to permit the consumer maximum control over access to covered data. Similarly, we also ask that the CFPB ensure that revocation of consent be made in a comparable manner with the consumer having to expressly select the accounts for which a consent is revoked.

[10] 88 *Fed. Reg.* at 74,823.

VI. *Compliance Timeline for Authorized Third Parties and Data Aggregators*

Section 1033.121 of the Proposed Rule contains a staggered compliance timeline for data providers based on their size, but the Proposed Rule does not grant any leeway to authorized third parties or data aggregators that may be necessary for them to continue accessing data in an uninterrupted manner. When a data provider comes into compliance with the Final Rule, its developer interface will prohibit access to covered data through the use of consumer credentials, and a data provider need not permit access to covered data through a method other than the developer interface.

The shift in the industry to using application programming interfaces to access data is significant to improve consumer protection, and Mastercard has been a leader in driving the industry in that direction. However, third parties and data aggregators will need time to build infrastructure to connect to the developer interface of each data provider. If a data provider does not make its developer interface available until close to the applicable compliance date, the CFPB risks putting authorized third parties and data aggregators in a position in which they will not be able to access covered data, because they will not have sufficient time to connect to the developer interface and will no longer be able to access data through the use of consumer credentials. Accordingly, Mastercard urges the CFPB to permit authorized third parties and data aggregators to continue to use credentials to access covered data for a period of up to six months after a data provider first makes its developer interface available.

VII. *Performance Specification*

Mastercard supports the inclusion of the quantitative minimum performance specification to ensure the functioning of a developer interface. Specifically, we believe that the 99.5 percent threshold and the description of a "proper response" are appropriate to ensure consumers are able to access data from data providers without significant interruption. We are also appreciative that Sections 1033.311(c)(1)(i)(B) and (C) of the Proposed Rule look to qualified industry standards to determine reasonable notice of downtime and the total amount of scheduled downtime in a relevant period. We urge the CFPB to finalize the performance specification in the same form as it has been included in the Proposed Rule.

VIII. *Denials of Access*

Section 1033.321(a) of the Proposed Rule would permit a data provider to reasonably deny access to its developer interface based on a risk management concern, such as a safety and soundness issue or an information security issue. Moreover, Section 1033.321(c) of the Proposed Rule states that indicia of such a denial being reasonable is adherence to a qualified industry standard related to data security or risk management. We recognize the importance of this denial right for data providers. However, the Final Rule should require qualified industry standards on this issue to include a process for a third party to remedy the data provider's concern to be able to continue accessing covered data. In the absence of such a process, the Proposed Rule could penalize a third party or consumer by disrupting access to covered data for unnecessarily long periods of time after the third party has remedied a data provider's concern.

* * *

Mastercard appreciates the opportunity to provide comments on the Proposed Rule. If there are any questions regarding our comments, we would welcome a conversation with the CFPB. Please do not hesitate to contact us.

Sincerely,

Tom Carpenter
Senior Vice President, Global Open Banking & Open Finance

cc: Tina Woo, Senior Managing Counsel, Regulatory Affairs, Mastercard International Incorporated