ELECTRONIC TRANSACTIONS ASSOCIATION

1300 Connecticut Avenue, Suite 475
Washington, DC 20036

202.828.2635
electran.org

December 29, 2023

*Via Email Submission*

Comment Intake – Financial Data Rights
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

**Re: Comments Regarding CFPB Proposed Rule to Implement Section 1033 of the CFPA – Docket No. CFPB-2023-0052; RIN 3170-AA78**

Dear Director Chopra:

On behalf of the Electronic Transactions Association (ETA), we appreciate the opportunity to share our thoughts in response to the Consumer Financial Protection Bureau's (CFPB) request for feedback regarding the implementation of section 1033 of the Consumer Financial Protection Act.

ETA members are dedicated to continuously driving innovation in the payment space and values the importance of a financial ecosystem whose participants ensure that consumers and businesses are provided with financial products and services that are convenient, secure, and reliable.

Additionally, ETA members operating globally have already been involved in the creation of open banking frameworks in other jurisdictions, such as the United Kingdom and Canada, and are determined to share their expertise to help secure the best outcomes for consumers in the United States.

ETA appreciates the CFPB's stakeholder engagement and consultation with the industry when detailing the regulatory requirements of the open banking framework. In this regard, ETA commends the CFPB's commitment to investigating the merits of section 1033 through a process that invites input from the public and other stakeholders and welcomes the opportunity to be part of the dialogue.

Access to financial data and information is an important issue that involves consumers, traditional financial institutions, fintechs, and other financial service providers, including data aggregators and third-party application providers. The ecosystem consists of multiple stakeholders, each with differing roles within an open banking framework.

ETA and its members recognize the increased convergence between these groups and the need to preserve consumer access, choice, and control. To preserve market dynamism, ETA strongly encourages the CFPB to be sensitive to the risk of applying a prescriptive regulatory framework and considers the industry to be best positioned to lead in addressing these diverse interests.

**Who We Are**

ETA is the world's leading advocacy and trade association for the payments industry. Our members span the breadth of significant payments and fintech companies, from the largest incumbent players to the emerging disruptors in the U.S and in more than a dozen countries around the world. ETA members make commerce possible by processing more than $44 trillion in purchases worldwide and deploying payments innovation to merchants and consumers.

ELECTRONIC TRANSACTIONS ASSOCIATION
1300 Connecticut Avenue, Suite 475
Washington, DC 20036
202.828.2635
electran.org

**ETA's Input on CFPB's Proposed Rule**

Seeking Clarity Around the Terms Possession and Control

ETA encourages the CFPB to clarify the terms "possession" and "control" of consumer data. Possession and control are two distinct concepts, each with its own implications for the protection and remediation of consumer data. The lack of precise definitions for these terms may lead to ambiguity and potential misinterpretations, impacting both consumers and the entities responsible for managing their financial data.

More often, possession refers to having custody of consumer data but may not necessarily imply ownership or control over the data but rather the responsibility for its safekeeping and storage. On the other hand, the control of consumer data often implies ownership and the ability to determine how the data is used, processed, shared, and has the authority to set policies and make decisions regarding data management.

Control over consumer data is crucial for ensuring proper protection and responsible use. Entities that possess consumer data but lack control over it may find themselves at odds with their own security practices and obligations to access consumer data if they are nonetheless obligated to provide access to such data to third parties. The entities that generate and control data empower organizations to establish and enforce data security policies and access controls. In addition, mere possession of consumer data is not enough to verify information or remediate errors. For example, an entity that provides cloud back-up for data resident on consumer devices may have possession of consumer data but no right or ability to access or use that data. Indeed, the data may be encrypted in a manner that provides technical protections making treatment as a data provider impossible as a practical matter. Entities merely possessing covered data lack the control needed to address inaccuracies as per the proposed rule; conversely, financial institution that maintains the consumer's deposit or credit card account and controls the covered data is in the best position to address inaccuracies in the covered data as required by the proposed rule.[1]

Clarifying these terms, and applying the obligations of a covered data providers only to those persons that control the covered data, is essential for fostering transparency, accountability, and compliance with data protection regulations. A well-defined framework for possession and control would not only empower consumers to make informed decisions about their data but also enable financial institutions and service providers to establish robust data management practices and can help ensure that consumer data errors are remediated effectively.

Revocation of Consumer Authorization

Consumer confidence is directly related to the perception of privacy, security, and protection of financial information and data. Consumers need to be confident in the safety and security of the overall system, and trust that their financial information and data are being used in accordance with their wishes. To that, ETA agrees that consumers should have a mechanism that they can use to revoke a third party's authorization to access covered data.

The ability of consumers to revoke access to their data aligns with the principles of transparency, autonomy, and data ownership. However, one critical aspect that remains unclear is the revocation timeline for entities within the broader data-sharing ecosystem. Specifically, ETA is seeking clarification

[1] § 1033.351(c)(2)(ii)

on whether the CFPB intends to implement a standardized timeline requiring third-party entities to promptly notify relevant stakeholders of a consumers data access revocation or whether these standards will be industry-led.

Timely notification mechanisms protect consumers from potential misuse of their data. Establishing a transparent and collaborative approach to setting these standards will benefit all stakeholders and help maintain a balance between consumer protection and industry innovation.

Additionally, ETA seeks clarity on a consumer's ability to authorize and revoke specific account data. For example, currently consumers are often allowed to revoke access through the data provider to one account but continue the authorization with another account. Would this practice be continued under section 1033 or would revocation be only permitted under an "all or nothing" approach, as seems to be indicated in the preamble? There also needs to be further clarification for revocation in context of joint accounts – can one account holder revoke authorization that was provided by another joint account holder? ETA recommends the CFPB allow for partial revocation on accounts and all account holders should have the ability to revoke access in the same way all account holders can authorize access.

Standard Setting Bodies

We commend the CFPB for implementing an industry-led and principles-based approach for approving standard setting bodies, which recognizes the importance of collaboration and adaptability in the evolving landscape of consumer access to financial records. ETA acknowledges the significance of industry participation in developing standards that align with the dynamic needs of the financial services sector and believes that an industry-led process ensures that those with direct experience and expertise contribute to the creation of effective, practical, and innovative standards that benefit consumers and industry stakeholders alike.

The principles-based approach provides a flexible framework that can adapt to technological advancements and changing market dynamics. This adaptability is crucial for fostering innovation while maintaining a regulatory environment that prioritizes consumer protection. We appreciate the CFPB's recognition of the need for standards that can evolve with the rapidly changing landscape of financial technology.

The industry has made significant progress in recent years in collaborating on developing standards for interoperability across the entire ecosystem. For example, the Financial Data Exchange (FDX) was established and has developed an API that can facilitate secure data sharing among all parties. It is critical that the CFPB approve standard setting bodies, such as FDX, prior to final rule issuance as any delay may be completely disruptive to the data sharing ecosystem and would significantly delay the industries' ability to implement this rule.

To ensure the industry has the necessary information to support the CFPB's vision for private sector standard setting, we believe the CFPB should provide a safe harbor to entities that comply in good faith with anticipated standards, guidelines, and other oversight and governance functions as standard setting bodies become established. To that, we also have several questions that should be addressed in any future iterations of this rulemaking process:

- How does the CFPB plan to approve standard setting bodies? Is there a timely notification process? If a standard setting body is not approved, will it be able to appeal or be accepted as a standard setting body in the future?

  - ETA believes there should be a timely notification process and standard setting bodies that are denied should be entitled to an appeals process. The appeals process should provide entities with additional consultation with the CFPB to help remedy issues and ensure that the entities are given a fair opportunity to make their case to agency officials. This effort led by the CFPB would ensure that agencies and firms build a strong collaborative relationship that will help ensure further collaboration throughout the process.

- Does the CFPB anticipate a standard setting body or bodies being approved prior to the final rule, or at least prior to implementation? Given the currently proposed 6-month compliance time, a timeline that is significantly shorter than what is required to properly update existing systems for the largest financial institutions and nondepository institutions, compliance standards for data providers and downstream entities will need to be developed.
  - ETA believes standard setting bodies should be approved prior to final rule issuance. Additionally, the CFPB should extend the compliance period, as noted below.

- How does the CFPB plan to handle possible future standards developed down the road that may conflict with CFPB expectations, especially if these standard setting bodies are developed after compliance is required?

- While the proposed rule prohibits secondary uses of consumer data as part of the third party's authorization, will the standard setting body establish a process to determine if the use of covered data falls outside the scope of the initial authorization? Or will it be determined by the CFPB or data provider to make those conclusions?

<u>Prohibition on Using Data for Secondary Use Cases</u>

ETA believes entities should be able to use deidentified data for secondary use cases. While we acknowledge and support the importance of protecting consumer privacy, we believe it is essential to consider the potential benefits of allowing entities to use deidentified data for secondary purposes. However, we caution the CFPB from attempting to define new privacy regimes around open banking data. Existing laws and regulations already provide a robust framework for protecting consumer privacy in the financial services industry. Adding an additional layer of regulations would only stifle innovation and hinder competition.

Allowing entities to leverage deidentified data for secondary purposes would allow for the improvement of innovative products and services that benefit consumers. When handled responsibly, the use of deidentified data for secondary purposes can align with ethical data practices and in conjugation with privacy safeguards and anonymization techniques, entities can strike the balance of improving their products and offerings with the protection of consumer privacy. Furthermore, the final rule should explicitly prohibit the ability to reidentify all entities, including the data provider itself, involved in open banking transactions. This essential safeguard would effectively eliminate the risk of individuals being linked to specific data points and further strengthen consumer privacy protections.

Deidentified data has immense potential for improving innovative products and services that cater to the diverse needs of consumers. By enabling entities to access and utilize this data, the CFPB can foster an environment conducive to innovation and competition within the financial services industry. For example, the use of secondary data allows entities to improve financial literacy tools that educate consumers about financial concepts.

Digital Wallets and Regulation E

The Supplemental Information to the proposed rule provides that digital wallet providers are Regulation E financial institutions, without detailed discussion, all while purporting to not make any amendments to Regulation E. Specifically, it states that, "Regulation E financial institutions—including digital wallet providers, entities that refer to themselves as neobanks, and traditional depository institutions --- have and will continue to have error resolution obligations…" and that "[d]igital wallet providers and entities that refer to themselves as neobanks generally qualify as Regulation E financial institutions and sometimes also may be Regulation Z card issuers have and will continue to have error resolution obligations." ETA respectfully submits that if the CFPB seeks to take such positions, it must do so via notice and comment rulemaking.

"Financial Institution" under Regulation E includes, "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," with certain limited exceptions. As the CFPB otherwise acknowledges, the term "digital wallet" does not have a clearly defined meaning and could be read to encompass a wide range of products with a wide variety of often divergent features and functionality. For example, while some digital wallets involve the issuance of an "account" under Regulation E, others do not. Similarly, whether any particular digital wallet itself constitutes an "access device" under Regulation E would depend upon the specific functionality of the digital wallet. Given the breadth and ambiguity of the term "digital wallet," the statement that digital wallet providers are Regulation E financial institutions is simply overbroad. Furthermore, digital wallet providers are not specifically addressed in the Electronic Fund Transfer Act or Regulation E, and given the broad scope of technologies and services provided under the term "digital wallet," if the CFPB intends to take a position regarding the application of Regulation E to the broad class of services for which the term "digital wallet" is used, it is an appropriate topic for notice and comment rulemaking pursuant to the Administrative Procedures Act. Accordingly, ETA requests the CFPB clarify in the Supplemental Information to the final rule that whether any particular digital wallet provider is a Regulation E financial institution will depend on the specific characteristics of the digital wallet service.

Facilitation of Payments

ETA encourages the CFPB to clarify the meaning of "facilitation" within prong (3) of the definition of "covered consumer financial product or service." The term "facilitation" may be interpreted to be inordinately broad and it is unclear as currently proposed to the scope of activity the CFPB intends to include within the defined term. For example, the mere provision of telecommunications services can, in part, facilitate digital payments in the sense that they enable those payments to occur remotely. ETA welcomes the opportunity to comment upon this critical component of the proposed rule once there is additional clarity as to the CFPB's intent as to the encompassed products and services within "covered consumer financial product or service."

Financial Data Processing Products or Services

The CFPB has proposed adding "providing financial data processing products or services…" to the definition of a financial product or service under the Consumer Financial Protection Act (CFPA). While ETA does not object to expanding the definition to include financial data processing services, the CFPB proposes to use a different definition than that already established by Congress[2] without explanation for

[2] 12 U.S.C. 5481(15)(A)(vii)

deviating from the existing statutory language. For example, the CFPB has included within its proposed definition the "transmitting" of financial data, which is a utility function rather than a data processing function. We believe the CFPB should adopt the statutory definition already used for purposes of clarifying that financial data processing products or services are otherwise included within the definition at Section 1001.2(b).

Exception for Data Not Accessible Through a Consumer Interface

Proposed 1033.111(d) would exempt from the proposed rule depositories that have not established a consumer interface, and we welcome the CFPB's request for comment regarding eligibility for this exemption. While we support the general rationale for the exemption, we believe that exemption should not apply on an entity-basis, but rather should exempt from the definition of "covered data" any data that is not made accessible by the covered data provider to its customers through a consumer interface and should be expanded to apply to nondepository covered data providers as well.

Both depository and nondepository covered data providers may be in control of data that is held in a variety of manners and in a variety of databases and may make only a subset of that data available to their customers through a consumer interface. The decision to do so may have been made for a variety of reasons, including privacy and security considerations, technological burdens, and operational challenges. The cost imposed on covered data providers to maintain a developer interface and provide access to data they have otherwise made available through a consumer interface is justified by the important goals of open banking, including to allow consumers to choose from where they will access their financial information, and to encourage the transition away from screen scraping consumer interfaces given the myriad concerns described in the proposed rule. However, covered data providers should not be obligated to build access tools to data the provider is not already making accessible to its customers through a consumer interface. Such a requirement places an undue burden on covered data providers that is inconsistent with the goals and rationale for open banking initiatives. As a result, we would encourage the CFPB to consider limiting the definition of covered data to only data that the covered data provider makes available through a consumer interface and to apply this exclusion to both depository and nondepository covered data providers.

Need for Additional Compliance Time

Under the Proposal, financial institutions with at least $500 billion in assets and nondepository institutions that generate at least $10 billion in revenue would be required to comply with the final rule within six months after it is published in the *Federal Register*. We believe this timeframe is insufficient and unreasonable. The CFPB should provide even the largest entities with at least 18 months after the later of the issuance of the final rule or the recognition of a standard setting body to comply, whichever is later.

Additionally, the CFPB should provide a two-and-a-half-year compliance timeframe for smaller (those generating less than $1 billion in revenue) nondepository institutions in order to ensure full compliance. Under the Proposal, nondepository institution data providers that generated at least $10 billion in revenue in the preceding calendar year, or are projected to generate at least $10 billion in revenue in the current calendar year, will have six months to comply. And those nondepository institutions that generated less than $10 billion in revenue would be required to comply with the final rule within only one year. We believe that similar to the multiple categories provided for depository institutions, the CFPB should include smaller nondepository institutions in the two- and half-year compliance requirement section for those smaller nondepository institutions that generated less than $1 billion in revenue in the preceding

calendar year, or are projected to generate less than $1 billion in the current calendar year. This would align the compliance timeframe for smaller nondepository institutions with the compliance timeframe for similarly situated smaller depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets. As the CFPB appropriately recognized, these smaller institutions do not have the necessary resources to meet the shorter compliance deadlines. The current one-year timeframe for smaller nondepository institutions (those with less than $1 billion in revenue) is insufficient and the additional time of two and half years should be provided to ensure full compliance.

We agree with the CFPB that access to financial data by data aggregators and others that is authorized by the consumer can provide consumers with significant benefits. However, it is at least in part because of these beneficial changes that additional compliance time is needed. For example, there needs to be changes in how data providers communicate with recipients. Currently, data providers do not communicate directly with aggregators and third parties. This would need to be changed to develop the required revocation process and much thought and planning would need to be done before these changes are implemented to ensure that the revocation process operates effectively, sufficiently protects consumer data, and is to the benefit of consumers.

Additional time would also be needed to incorporate new data elements that would be required to the extent they are not currently made available. This includes certain covered data such as scheduled payments, bill pay information, and terms and conditions. The CFPB should also note that as a general matter, bill pay service is a separate product or service from the offering of a Regulation E account and many of those systems operate differently from each other. As part of these compliance effort, it would also be helpful for the CFPB to provide additional clarifications for this covered data, specifically the parameters and the extent this information would need to be provided as much of this information is already available to the consumer on a financial institution's website and consumer-facing mobile applications. Additional clarity is also needed as to whether certain products, such as corporate card products held by individuals, are excluded from the definition of a covered consumer financial product or service. Overlaying all of these compliance requirements is the need to develop necessary policies and procedures and provide sufficient employee training.

Lastly, ETA suggests that any final section 1033 rule should clarify that for covered data providers, the relevant revenue threshold that determines the provider's compliance data should include only revenue from the covered payments service and not aggregate revenue across affiliated entities and businesses of the covered data provider which have no relationship to consumer financial services.

Delay the CFPB's FCRA Rulemaking Process

The CFPB is currently engaged in a separate rulemaking process to amend Regulation V, which implements the Fair Credit Reporting Act (FCRA). ETA suggests the CFPB pause the FCRA rulemaking until section 1033 is implemented. These two regulations overlap significantly, and their combined impact on financial institutions won't be fully understood until section 1033 is finalized.

The CFPB's current FCRA proposal risks significant unintended consequences for entities complying with section 1033. The proposed expansion of the "consumer reporting agency" (CRA) definition could inadvertently classify compliant financial institutions as "furnishers" under the FCRA, especially where the data providers are required to provide information to a designated third party that is considered a CRA. This would subject them to compliance requirements and potential liabilities under two separate regulatory frameworks.

To address this critical issue, we urge the CFPB to implement the following:

- Clearly exempt data providers under section 1033 from FCRA obligations where information is provided subject to section 1033 authorization. This would ensure regulatory clarity.

- Coordinate closely between the FCRA rulemaking and section 1033 implementation. This collaboration will help identify and address potential conflicts or overlaps, ensuring a consistent and efficient regulatory environment for financial institutions.

These steps will allow for a comprehensive understanding of the combined regulatory landscape and prevent entities from facing conflicting or duplicative requirements and also permit a better-informed notice and comment rulemaking period.

Liability Requirements

As we indicated in our comment letters in response to the ANPR and the SBREFA Proposals, it is our view that the CFPB should align on the principle that liability should follow the data and that all market participants should be collectively liable for the risks they create. As long as the entity transfers the data in good faith and in compliance with the section 1033 rules, it should not be held liable if a downstream recipient is subject to a data breach or if there is other misuse of the information by that downstream recipient or other parties that obtained the information from the downstream recipient, either knowingly or unknowingly. As the CFPB works to issue a final rule, ETA urges the CFPB to address and develop a comprehensive liability framework.

Continued Payments and Data Access Authorization

ETA agrees with the CFPB that consumers would benefit from the ability to provide annual authorizations for third party data access. While the proposed one-year maximum authorization duration is a step in the right direction, it introduces unnecessary friction and administrative burdens for both consumers and businesses. Certain ETA members propose a simpler and more efficient approach: using continued payments as an implicit annual authorization for third party data access.

Instead of requiring explicit reauthorization every year, continued payments automatically renew access, eliminating the need for consumers to take separate actions. This reduces friction and complexity, improving user experience and reducing abandonment rates. Streamlining the authorization process would encourage more consumers to utilize financial services that rely on third party data access. This would promote financial inclusion and expand access to products and services.

Continued payments represent an implicit form of consent, indicating an ongoing desire for the service and its associated data sharing. In addition, consumers maintain ultimate control. They can readily terminate data access and service at any time by simply stopping payments. This provides a clear and readily accessible opt-out mechanism.

By leveraging continued payments for annual authorization, the CFPB can strike a balance between consumer protection and business efficiency. This approach streamlines the process, reduces burdens, and encourages continued access to valuable financial services. We urge the CFPB to seriously consider this proposal when finalizing the section 1033 rule.

Data Access Caps

Under the proposed rule, data providers are required to offer a developer interface with commercially reasonable performance, including a proper response rate of at least 99.5 percent. However, the CFPB also proposes in § 1033.311(c)(2) to prohibit a data provider from unreasonably restricting the frequency with which it receives and responds to requests for covered data from an authorized third party through the data provider's developer interface.

If data providers are prohibited from limiting volume (access) to developer interfaces, it may prove difficult to maintain the performance requirement of 99.5% without significant investments in the infrastructure. To determine the level of investment, an entity would need to assess volume, which cannot be forecasted absent historic trend information.

Although the proposed rule prohibits a data provider from unreasonably restricting the frequency it receives and responds to requests, it does allow certain restrictions that pose an unreasonable burden on the data provider's developer interface. For example, an organization may need to impose a temporary access cap, such as limiting the number of allowable data requests or frequency of those requests, during certain periods of the year in which an entity may experience increases in calls to their APIs. This could occur in situations of security or other incidents in which an entity may need to temporarily limit access to protect consumer data. In this type of example, spikes in consumer data requests could result in unintended consequences and hinder an entity's ability to comply with the proposed performance requirements.

As the CFPB continues to develop this rule, our members agree that such frequency restrictions must be applied in a manner that is fair, open, and transparent. Our members recommend the CFPB to consider the merits of either enabling caps based on reasonable volume forecasting, permitting access caps that are specific to the product or service authorized by the consumer, or allow some variance in performance for unexpected spikes in call volume as an alternative to the current proposed requirements.

Assessment of Cost for Providing Covered Data

The CFPB notes that third parties have made payments to data providers to incentivize them to create a developer interface of sufficient quality and in a timely manner. While rare in the current market, the proposed rule would eliminate the ability to charge this type of fee. To best understand the potential implications, the CFPB should review the United Kingdom's developments in their open banking efforts. For instance, the recent Garner Review on the Future of Payments[3], proposes to revisit the commercial model of open banking, looking at a range of options including allowing providers to (a) recoup the costs of providing the infrastructure; (b) recoup the costs of providing the infrastructure plus funding a level of consumer protection; and (c) recoup the costs, fund consumer protection, and make a small profit margin. The development of a commercial model is key priority of UK regulators and is aimed at ensuring open banking is economically sustainable and creates incentives to providers to invest in and support it going forward. Based on learnings from this recent report, the CFPB should consider the link between entities' ability to charge reasonable fees and the resulting impact to regulatory compliance performance minimums. The test for this commercial model could be on a specific use case, such as Variable Recurring Payments, as has been the case in the UK.

[3] Garner, Joe. *Future of Payments Review.* 2023. assets.publishing.service.gov.uk/media/6557a1eb046ed400148b9b50/Future_of_Payments_Review_report.pdf

The UK is also considering impacts on liability in the data flow. One recommendation that they are exploring is a measure to set up a regulator-led entity that will set standards and support the development of proportionate liability framework. As illustrated by the developments occurring in the UK, it is reasonable to allow covered data providers to assess at a minimum, a de minimis fee to an authorized third party to help recoup the cost needed to establish, maintain, and support the data provider interfaces and other processes needed to comply with the rule's requirements.

For the reasons outlined, our members recommend the CFPB to clarify whether providers may assess such a fee to any authorized third parties seeking access to the data providers' interfaces. By permitting the charging of fees, authorized third parties will also be motivated not to make additional data calls beyond what is needed to deliver the product or service, or will face increased costs to do so unnecessarily.

Electronic Benefit Transfer Data

Electronic Benefit Transfer (EBT) cards and data are separate and distinct from the commercial market and therefore do not easily lend themselves to the intent of the proposed regulation. In the EBT ecosystem, the "consumer" is a government program beneficiary. Before expanding the scope of the proposed regulation to cover EBT, the Bureau should consult with the U.S. Department of Agriculture, Food and Nutrition Services (FNS), and relevant state agencies that administer EBT programs.

As the Bureau notes, EBT cards and data differ from the current scope of data types included in the proposed regulation.[4] The administration of EBT does not lend itself to the intent of the regulation because of key differences from the commercial market. In the commercial market, consumers sign-up for services with various providers and have numerous choices from which to choose from - whether that's to bank, seek a loan, invest and more. EBT is governed and managed by the U.S. Department of Agriculture's FNS, relevant U.S. state agencies, and contracted processors. Program beneficiary data belongs to the state, not the cardholder. There is no opportunity to move or transfer government managed Personal Identifiable Information (PII) data between providers. If a beneficiary moves states for example, they have to reapply for benefits.

*Program Beneficiary Access to Their Benefits*
In the proposed rule, the CFPB notes that "EBT-related data are mainly accessed directly by the consumer through private entities that have contracted with State or local governments that administer programs for Federal government agencies."[5] However, this is not the case today. Beneficiaries of EBT programs have access to state-run cardholder portals and portals managed by private entities on behalf of state agencies. Additionally, there are text messaging, mobile application, Interactive Voice Response (IVR), and customer service hotline options for beneficiaries to gain real time access to their benefits information. Therefore, expanding the rule to cover EBT does not fill an existing gap, but instead opens the door for the dilution of the state's ability to monitor the beneficiary's PII data and for the commercialization of that information. These risks may increase the beneficiary's exposure to fraud through providers with no direct contract with state agencies.

*Third Party Provider Risk*
There are several third party providers in the EBT system that operate by scraping benefits information, without official affiliation with state agencies, FNS, or the contracted EBT processor. Many of these

[4] 88 Fed. Reg. 74804
[5] *Id.*

entities provide direct services to program beneficiaries without clearly disclaiming that they are not affiliated with the official federal and state-run programs. This creates a situation in which program beneficiaries do not have full information and believe they are working with a state-sanctioned program provider when they are not. Expanding the scope of the proposed regulation would result in FNS and U.S. state agencies losing control over various program parameters currently in place to protect program beneficiaries. For example, FNS oversees the participation of all participating retailers that process EBT program benefits. Should the rule expand, a third-party provider may seek to launch a new product directly with a retailer, but without explicit permission of FNS to ensure that the product does not supersede or conflict with federally mandated guidelines. Today, current product innovations such as internet shopping for EBT, are closely monitored by FNS to protect program beneficiaries and ensure the proper restrictions are put in place as required by the program. If the regulation were to expand scope, the rule would have to require the establishment of formal contractual relationships between third party providers and FNS, U.S. state agencies, or government contracted providers. Without that distinct connection, government agencies will lose the ability to know how program beneficiaries are utilizing their benefits or if they are utilizing them at approved locations.

*Data Security*
U.S. state agencies are responsible for and manage all EBT-related data. Providers in the ecosystem, such as a processor, do not own EBT beneficiaries' data nor can they put in place any new products or solutions without the explicit permission of the state agency. If the proposed rule were to expand, providers without direct contracts with state agencies would be able to utilize program beneficiaries' data without any controls or restrictions in place (such as restrictions on purchases of alcohol, cigarettes or other items prohibited by the program). This puts program beneficiaries' data at risk and reduces the state's ability to protect data.

Should the regulation be expanded, the Bureau would need to clarify who is liable should there be a release of PII data. EBT processors, which run call centers on behalf of state agencies, would be inundated with potentially fraudulent activities. If EBT data is opened for commercial use, states will not be able to identify where a breach is occurring nor be able to quickly mitigate the situation. Providers without state contracts would also have no requirement to report a breach as they have no direct responsibility, at this time, for reporting the data they collect and utilize. Current EBT processors negotiate specific provisions through state contracts regarding liability and data breach. This ensures that when an incident occurs, the issue can be identified, and states can support potential reimbursement quickly.

Scope of "Covered Data Providers"

There is a fundamental distinction between digital payment applications that hold funds on behalf of consumers ("stored funds wallets") and digital payment applications that hold payment credentials ("pass-through wallets"). Stored fund wallets store value accounts or funds stored while in transit to designated recipients such as in P2P transfers or provide the sole means for a consumer to access their funds such as via a bank partnership, while pass-through wallets never hold funds on behalf of consumers but process payments using existing credentials.

Requiring pass-through wallets to provide covered data would not provide any additional benefits for open banking or consumers. Specifically, the section 1033 proposed rule would require covered data providers to provide six categories of covered data, and pass-through wallets do not have unique information in any of these categories:

1) Transaction information (proposed section 1033.211(a)): Because a pass-through wallet provider only stores information for underlying payment methods issued by companies that are already covered data providers (e.g., debit and credit card issuers), each transaction processed by a pass-through wallet will also be reflected in the transaction history of these underlying payment method issuers. For example, a consumer or authorized third party can already obtain debit card, credit card, and prepaid account transaction data from the issuers of these payment methods (each of which would be covered data providers in their own right), and the pass-through wallet provider would typically provide the issuer with certain basic information about the transaction (e.g., merchant name). Thus, requiring the pass-through wallet provider to provide the same information as well would be purely duplicative.

2) Account balance (proposed section 1033.211(b)): Pass-through wallets do not store or provide access to any consumer funds; they would have no account balance information to provide.

3) Information to initiate payment to or from a Regulation E account (proposed section 1033.211(c)): Pass-through wallets do not issue Regulation E accounts to consumers, so there would be no Regulation E accounts for which the pass-through wallet can uniquely provide payment initiation information.

4) Terms and conditions (proposed section 1033.211(d)): A pass-through wallet generally does not charge a fee to consumers, does not charge any annual percentage rate or yield (because the provider has issued no credit nor any asset account to the consumers), does not offer overdraft coverage, and generally does not have any other terms and conditions in its consumer-facing agreements (if any) that would be relevant to any open banking service (e.g., a payment service or credit underwriting service).

5) Upcoming bill information (proposed section 1033.211(e)): Pass-through wallets generally are not used for bill payments. However, even in circumstances where a pass-through wallet is used to pay a bill, the pass-through wallet provider often does not have visibility into the upcoming payment. It is, the biller and consumer that control whether and when a payment is made, and the payment method wallet is simply used to supply, and sometimes charge, the relevant payment credentials.

6) Basic account verification information (proposed section 1033.211(f)): While pass-through wallet providers may have certain basic consumer information, because they are not holding funds on behalf of consumers, they typically are not required to perform know your customer checks to verify this information. As a result, this information likely would not be relied on by a third party and therefore would not be helpful for an open banking service provider to access.

Additionally, ETA assumes the CFPB did not intend the scope of covered data provider to capture a physical point-of-sale terminal or a merchant's facilitation of credit card, debit card, prepaid account, or other covered payments in connection with transactions on the merchant's own stores, including the merchant's own marketplace websites.

As a result, while some ETA members don't agree, we believe the CFPB should exempt pass-through wallets, point-of-sale terminals, and merchant facilitation from the scope of covered data providers. Additionally, any remaining covered data providers, including potential pass-through wallet exemptions,

should not duplicate data already reported by the Regulation E account issuer or Regulation Z credit card issuer.

Service Providers

The CFPB should clarify that service providers, as defined in the CFPA[6], are excluded from the definition of "data provider" because a consumer does not "obtain" the underlying covered financial product or service from a service provider that is merely fulfilling contractual obligations to provide services on behalf of a covered financial institution that provides the covered financial product or service for which the consumer seeks to obtain covered data pursuant to the proposed rule.

Although service providers may have access to covered data for purposes of carrying out services on behalf of a covered financial institution, the covered data to which the consumer may seek access pursuant to the proposed rule is actually controlled by the financial institution, not the service provider. Indeed, consumers are more likely to look to their financial institution that maintains the consumer's deposit or credit card account (rather than a service provider) when seeking access to covered data related to the products or services the consumer obtained from their financial institution.

In addition, because service providers are typically not involved in the movement and settlement of funds, they typically do not possess many of the categories of covered data detailed in the Proposal, such as rewards credits, fees, finance charges, account balance, fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, upcoming bill information and other data related to the Regulation E accounts and Regulation Z accounts.[7] Because service providers have access to a limited scope of covered data, including them within the scope of covered data providers would frustrate the underlying purpose of the Proposal. Indeed, consumers and their authorized third parties who seek data from service providers would receive insufficient data to enable common beneficial use cases like personal financial management. Consumers and their authorized parties would have to go to the applicable financial institution to obtain the full scope of covered data as contemplated by the CFPB.

*  *  *

ETA appreciates the opportunity to provide input on this important issue. If you have any questions, please contact me or Scott Talbott, ETA's Executive Vice President, at stalbott@electran.org.

Sincerely,

Jeff Patchen
Director of Government Affairs
Electronic Transactions Association

[6] 12 U.S.C. § 5481(26)(A)
[7] § 1033.211