VIA ELECTRONIC SUBMISSION

October 21, 2025

Acting Director Russell Vought
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Comments on Personal Financial Data Rights Reconsideration (Docket No. CFPB–2025–0037)

Dear Acting Director Vought,

Apple Payments Services welcomes the opportunity to comment on the Consumer Financial Protection Bureau's ("Bureau" or "CFPB") Advance Notice of Proposed Rulemaking on Personal Financial Data Rights Reconsideration under Section 1033 of the Dodd-Frank Act.

At Apple, our mission is to create technology that empowers people and enriches their lives. Through the seamless integration of hardware, software, and services, we make products that are intuitive and delightful to use. We also believe that privacy is a fundamental human right, and we have designed our products and services to put users firmly in control of their data—including what data is collected, who can access it, and what it is used for.

The principle of **data minimization** is at the heart of Apple's approach to privacy. We collect only the personal data required to deliver what our users need. Whenever possible, Apple processes and analyzes data **on users' devices**, where even we cannot access it. When we do collect personal data, we are clear and transparent about it—and we think everyone else should be, too. We make sure that users know how their personal information is being used, and how to opt out anytime they like. And we make it easy for them to review and take control of the data that they store with Apple through our centralized Data & Privacy Page.[1]

In 2014, Apple brought this combination of attributes—easy-to-use, secure, and privacy-protective—to mobile payments when we launched two transformative technologies: Apple Wallet and Apple Pay.

Apple Wallet is a wallet app on iPhone, iPad, and Apple Watch that is a digital reproduction of a physical wallet—it can securely and conveniently hold digital versions of a user's credit and debit cards as well as a wide variety of other types of cards and credentials, like transit passes, boarding passes, tickets, identity cards, keys, order tracking details, loyalty cards, and more. **Apple Pay** is a feature of Apple Wallet—it is the technical architecture that allows a user to easily present and pay with a digital version of an existing physical credit or debit card that the user has been issued by their financial institution.

[1] *Available at* https://privacy.apple.com/.

Apple Payments Services LLC
6900 W. Parmer Lane
Office No. AC01-2225
Austin, TX 78729

Like everything Apple makes, we designed these features from the ground up to protect users' most sensitive financial data, with best-in-class security features in the hardware and software to help keep users' information safe. For instance, in addition to the data minimization and on-device processing that underlie the design of these technologies, we have also built in biometric security measures to reduce the risk of fraud. At a point-of-sale terminal, Apple Pay uses near-field communication ("NFC"), which only allows devices within a few centimeters of each other to exchange information wirelessly. During the payment process, a user authenticates their identity using Face ID, Touch ID, or a password—and it is only after that authentication that the device transmits an anonymized token that corresponds to a user's card to the merchant's terminal via NFC. The user's card number is not shared with merchants as part of an Apple Pay transaction—just the anonymized token. Over the past decade, millions of users have come to trust Apple Wallet—and today, Apple Pay works with more than 11,000 banks and network partners in 89 markets around the world.

* * *

With more than a decade of experience in designing and offering a secure, privacy-protective, and easy-to-use payments experience, Apple applauds the Bureau's work on Section 1033. Access to financial information empowers consumers to make key financial decisions, such as buying a home, saving for their children's education, or planning for retirement. Apple supports consumers' right to access their personal financial data, as well as modernizing regulations to meet the needs of today's payments ecosystem. However, in designing these rules, it is important that the Bureau do so in a way that does not sacrifice user privacy in the course of enabling user access.

Regulations in the digital payments ecosystem should promote and encourage innovation to ensure consumers can take full advantage of their financial data by lowering barriers to access and putting consumers in the driver's seat. By giving users access to their data, they benefit from more information that they can use to take control of their financial health—enabling them to make informed financial decisions and better understand and manage their spend. To help make sure users get this data in ways that keep them and their data safe, digital payment regulations should create incentives for companies to build privacy-protective tools to allow consumers to most effectively manage their financial health.

To achieve this goal, any Section 1033 rule should seek to provide consumers with the ability to access and port their financial data that is held by the entities that maintain their account data in order to provide consumer financial services to them. Facilitating this consumer access to their financial "system of record" is essential to give users a complete picture of their financial health and promote innovation in the marketplace.

However, the Bureau should take care that rules under Section 1033 do not impose obligations on technology providers like Apple that do not maintain consumer financial accounts, but do offer privacy-forward services that store data on devices or in other locations that they cannot even access. Sweeping in providers of pass-through digital wallets and other entities that do not own or control (or even have access to) underlying data through "one-size-fits-all" rules will undercut the aims of creating an efficient and trustworthy data ecosystem. Any rule that would seek to require

providers of pass-through digital wallets to obtain access to user financial information they otherwise do not access, use, or store would not only undermine privacy protections like those built into Apple Wallet and Apple Pay by design, but also stifle future innovation in this exciting and fast-developing field of financial technology.

In sum, Apple Payments Services recommends as follows:

- The CFPB should limit "data providers" to account issuers (*i.e.*, banks and card issuers), as account issuers are the systems of record for the financial data in consumer accounts maintained by those financial institutions servicing those accounts. The definition of "data providers" should **exclude digital wallets** that do not own or control consumer accounts or maintain consumer account systems of record. For open banking to work, consumers need access to accurate data from sources-of-truth—account issuers, not those types of pass-through digital wallets.

- Because all persons have a right to know what information a company collects and maintains about them, and to exercise meaningful choice over how that data is processed and for what purposes it is used, everyone should have a right to access and obtain a copy of their personal data. No company should be able to deny a person access to their own records, and **data providers should not be permitted to place limits on what a customer does with their own data** once it is in the customer's control.

- If fees are to be charged for data access, they should be nominal and oriented around cost recovery for the banks—which would give the most flexibility in innovative uses of the data and best promote the consumer's ability to manage their financial health. To the extent fees are permitted, **the CFPB should explicitly prohibit so-called "use case" fees,** where data providers tie fees to specifically how the data is being used (*e.g.*, charging a higher fee for executing a real time payment than for general account access), which are not in the best interests of consumers or innovation.

- The CFPB should align on the principle that **liability should follow the data** and that all market participants should be liable for the risks they create. As long as an entity transfers data in good faith and in compliance with Section 1033 rules, it should not be held liable if a recipient of the consumer's data is subject to a data breach or if there is other misuse of the information by that recipient (or other parties that obtained the information from the recipient), either knowingly or unknowingly.

Apple will continue to build seamless payment infrastructure solutions that build consumer trust and deliver value across the financial industry. We look forward to working with policymakers to develop a regulatory framework that puts consumers—and their privacy—first.

I. The Bureau should ensure consumers have access to their financial data held by those who maintain it on their behalf.

In developing a Section 1033 rule, Apple Payments Services supports the Bureau's aim of putting users in control of their personal financial data. However, to meet Section 1033's goals of

empowering consumers and incentivizing privacy-forward innovation, the rules should focus on ensuring consumers' access to the data they need in a privacy-protective way. This data sits in the systems of record for consumer accounts maintained by financial institutions servicing those accounts. The rule should clarify that pass-through digital wallets that do not own or control that data are not encompassed by Section 1033.

A. Privacy-focused digital wallets that do not own or control accounts, like Apple Wallet, cannot provide consumers reliable sources of truth.

Because of the variety of services a digital wallet can provide and the various data it may or may not be able to access or maintain, treating digital wallets as a homogenous category—as they were under the former rule[2]—will not create a trusted data ecosystem, and it will not incentivize the privacy-forward innovation in the marketplace Apple is committed to.

Digital wallets house a wide range of products and services. For example, some digital wallets provide consumers with easily-accessible coupons, loyalty cards, and similar products, while others offer means of storing access credentials, such as corporate access cards, digital car keys, and digital home keys. Some digital wallet providers also allow for storing or viewing personal financial data. In some instances, those digital wallet providers may also own and control the underlying accounts and their related systems of record. For example, card-issuing banks may both own and control financial accounts and offer a digital representation of those accounts in a digital wallet. In other cases, digital wallets may simply provide a pass-through means for consumers to view personal financial data where the wallet provider neither owns nor controls—nor can even access—the underlying accounts or account records.

Apple Wallet is the latter kind of digital wallet; it lets users view personal financial information and store their credit and debit cards from participating banks in one place on their device. When a user adds a card to their Wallet through Apple Pay, their full card number is never stored on device or on Apple Pay's servers. Instead, the user's card issuer creates a unique Device Account Number, which is stored on the user's device in the Secure Element, an industry-leading, certified chip that Apple designed to safely store payment information. This process—known as tokenization—means that a user's most sensitive financial information is never stored on Apple's servers or backed up to iCloud.

When a consumer uses Apple Pay to complete a transaction, the associated transaction details are provided by the relevant financial institution to the consumer's physical Apple device, where the consumer can access and view them. Although the user can see their transactions made through Apple Pay, Apple itself does not have access to the transaction data such as what users buy, where they bought it, or how much it cost. If a user uses a means other than Apple Pay for a

---

[2] The prior rule assumed "[d]igital wallet providers that facilitate pass-through payments typically also provide a funds-holding asset account or credit card, so would already be subject to the requirements of this rule, including the requirement to maintain interfaces under § 1033.301." 89 Fed. Reg. 90838, 90855. This assumption does the payment ecosystem a disservice by drawing with too broad a brush.

transaction, users cannot see information about that transaction through Apple Wallet (other than a new open-banking-enabled feature in the UK described below).

In this way, Apple Wallet is akin to a spreadsheet program on a computer. Just as a consumer may download data from a financial institution, then use a spreadsheet program to access and view the data on their computer, Apple Wallet allows consumers to centralize data from different financial institutions on their Apple device, then access and view that data through Wallet. But like spreadsheet programs that run locally (and not in the cloud), the company that provides the program cannot access the data the consumer is viewing. And even if it could access the information, as with the spreadsheet program, Apple Wallet is not the source of that underlying data, nor could Apple, as a company, verify or attest to the accuracy of that data.

Because Apple cannot access the vast majority of relevant user information and does not own or control the user accounts—and thus, cannot verify the financial data users view through Apple Wallet—it cannot guarantee that the information on Apple Wallet will provide users with the level of accuracy necessary for users to rely on them as sources of truth—the systems of record belonging to the financial services companies administering those transactions provide that information.

B. The Bureau should exclude pass through digital wallets and instead apply Section 1033 only to entities that own or control users' underlying financial data and accounts.

In this proceeding, the Bureau has an opportunity to correct course on Section 1033 to open and decentralize the banking system by giving consumers more control over their data. The Bureau's former Section 1033 rule applied to "data providers" that issue credit cards and provide certain other financial products or services and broadly included digital wallet providers, 89 Fed. Reg. 90,838, 90,855 (Nov. 18, 2024); *see* 12 C.F.R. § 1033.111(c), example ("A digital wallet provider is a data provider."). The Bureau should use this new rulemaking to apply the rule only to the entities that have access to, and can validate, the user's underlying financial data: those that own and control consumer financial accounts and maintain account systems of record.[3]

The Bureau should not include other entities, like digital wallet providers (such as Apple Wallet) that merely store credentials to allow consumers to access their own personal financial data held by other entities, as data providers. Instead, determining whether a digital wallet is a data provider should be based on that digital wallet's actual role: namely, **whether it owns and controls the financial accounts and maintains what may be considered a system of record for the consumer account**.[4] Doing so helps ensure that users can obtain accurate data from sources of truth, and that entities like Apple can continue to provide users with a choice in the marketplace that prioritizes user privacy. This approach—based on whether or not the entity owns and controls,

---

[3] This should not include entities acting as service providers in maintaining an account system of record on behalf of data providers, regardless of their role in the upkeep and maintenance of the underlying system.

[4] *See, e.g., PayPal, Inc. v. CFPB*, 728 F. Supp. 3d 31, 39, 41–42 (D.D.C. 2024) (the Bureau should not attempt to "shoehor[n]" pass-through digital wallet providers into a Section 1033 Rule).

and thus can validate the accuracy of, the underlying data—reflects the aims of Section 1033 to promote a trustworthy and efficient system of data access.

This approach also aligns with the statutory purpose of Section 1033: it does not require service providers that do not have access to user data to obtain that data; such a system would undercut privacy-protective technologies.[5] The statute prohibits the Bureau from requiring entities to provide "information that a covered person cannot retrieve in the ordinary course of business," 12 U.S.C. § 5533(b)(4), and in fact disclaims the imposition of "any duty on a covered person to maintain or keep any information about a consumer," *id.* §§ 5533(b)(4), (c). Extending the revised rule to cover entities regardless of whether they maintain covered personal financial data and can verify the accuracy of such data would violate these limits—and, critically, require providers to collect *more* data than before. This goes against data minimization principles and best practices, and puts consumers at more risk of having their data exploited. *See* 12 U.S.C. § 5512(b)(2)(A)(i) (requiring the Bureau to consider "potential benefits and costs to consumers and covered persons" in rulemaking).

Focusing on entities that **own or control customer account systems of record** would provide consumers with the most reliable information. Even if an entity can technically access some amount of personal financial information owned or controlled by another entity, if they are not responsible for administering the underlying account and neither own nor control the account details, any data available to them may not be as complete or accurate as that contained in a true system of record. For example, if a financial management app receives erroneous account balance data from a third-party data aggregator, and a consumer relies on that data to make a purchasing decision, Section 1033 could have the unintended—and perverse—result of severely damaging consumer financial health and well-being.[6] If, on the other hand, the personal financial management app received account balance data from the account's system of record held by the regulated financial institution administering the account, consumers could trust that the data on which they were making a decision is accurate, and the end result would be improved consumer decisioning and, ultimately, improved consumer financial health.[7]

In the digital payments ecosystem, trust in the systems and entities providing the data is critical. The Bureau should carefully consider the scope of Section 1033 by focusing on true account

---

[5] *See* 12 U.S.C. § 5533(a) ("[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." (emphasis added)).
[6] Many other stakeholders have similar concerns about data inaccuracies, as the Bureau's prior final rule reflected many comments expressing that concern. *See*, *e.g.*, 89 Fed. Reg. 90838 and proposed 12 C.F.R. 1033.421(d) (intended to address data providers' obligations for providing accurate data).
[7] Relying on market forces to push consumers and businesses to "good" data sources also will not work. Even if the majority of entities obtain Section 1033 data from "good" sources, not all will—some may choose to obtain it from sources offering delayed data, or data whose transmutation introduces errors. That will result in some financial health tools showing one balance and other tools showing another balance, leaving the consumer in the position of needing to track down a source of truth or, at worst, deciding that there is no utility in these types of products after all, rendering Section 1033 ineffective.

systems of record administered by entities that are tasked with maintaining accurate financial information for their customers.

II. A customer account system-of-records approach has helped power Apple's ability to design innovative, open banking payment solutions.

Other jurisdictions' approaches demonstrate how open banking can help consumers manage their financial health and incentivize privacy-focused innovation: by requiring owners of customer account systems of record—but not other entities—to provide access to financial data, those countries have engendered consumer trust and enabled Apple's engineers to design innovative tools for users.

For example, in the United Kingdom, only financial institutions that directly issue the cards and accounts, (which the UK refers to as "account information service providers," or AISPs) or payment-facilitation providers (which the UK refers to as "payment information service providers," or PISPs) must share information.[8] This thoughtful approach has not only allowed Apple to continue offering great tools to our users for managing their financial data in a privacy-protective manner—it has enabled us to design even more innovative features for consumers.

Last year, for example, the UK's Open Banking initiative meant we could release an open banking feature in the UK which empowers users to seamlessly view the details of their financial accounts—including Apple Pay and non-Apple Pay transactions—in Apple Wallet. This new feature allows users who have added a debit or credit card to Apple Wallet to connect the accounts associated with those cards—as well as other accounts held at the underlying financial institutions—to their Apple Wallet. Once linked, users can view both Apple Pay and non-Apple Pay transactions, as well as other financial details, such as account balances, in their Apple Wallet. For the first time, a user's account details are now easily accessible on their device, allowing consumers to see the key financial information, such as account balances, transaction history, and credit limits, with a few simple taps. This connected cards feature also benefits banks and card issuers, enabling them to develop deeper relationships with existing customers through new opportunities to connect with their customers.

Apple built this connected cards feature with Apple's industry-leading privacy-by-design principles. To power it, Apple Wallet facilitates the transfer of data from a financial institution to the user's device—Apple itself does not store any of this sensitive data. Instead, those account details are stored on the user's device or in the user's encrypted cloud storage, and are viewable through Apple Wallet on iPhone, iPad, and Apple Watch. Apple does not maintain, own, or control the data.

The UK's regulatory framework has also enabled Apple to offer FinanceKit, an application programming interface ("API") that enables third-party financial-management apps to access the on-device financial information that consumers receive through our new card-connecting feature. FinanceKit relies on explicit user consent, meaning that users have control over what information is

---

[8] *See* The Payment Services Regulations 2017, SI2017/752 arts. 69, ¶ 2 (obligating account issuers to share information with PISPs), 70, ¶ 2 (obligating account issuers to share information with AISPs).

shared, from which accounts, and the time period for which information is shared. Once a user approves the data sharing, a financial-management app can directly retrieve the information that is stored on-device. By giving users direct control over how their data is shared, FinanceKit reduces the security risks that arise when a consumer must provide a third party with login credentials for another account.

In other words, FinanceKit offers users a safe and secure way to share their financial data with trusted third parties.

This great experience and the resulting value to consumers and the payment ecosystem have been possible because of the regulated access to *accurate* information derived from *sources of truth*. The same level of reliable experience could not be possible if the consumers could not be sure that the data provided was accurate—which works in the UK because the system relies on data from customer account systems of record.

III. The Bureau should ensure safe and secure data-sharing that prioritizes consumer control and removes barriers to access.

At Apple, we design our products and services to put users firmly in control of their data, including who can access it, and what it is used for. We believe that an effective Section 1033 rule should also put users in control of their data and remove barriers to access. Users should have a right to access and obtain a copy of their personal data, determine who they share their data with, and for what purposes. To that end, we support a rule that gives consumers the ability to knowingly and safely authorize the disclosure of their information to trusted third parties, and that prohibits data providers from placing limits on how consumers can use their data once they have it—limitations known as secondary use restrictions.

Users should not be restricted in how they use their own financial data. Just as a consumer can use a physical copy of their bank statement to get a mortgage, make a budget, or file their taxes, financial institutions should not be able to restrict how a consumer uses their digital information. Instead, consumers should be empowered to use digital information obtained pursuant to Section 1033 as they see fit.

Similarly, to prevent practical limitations imposed by varying costs, financial institutions should be prohibited from charging "use case" fees that change based on how a consumer seeks to use their data. For instance, a financial institution should not charge more for access to consumer data when it is used to execute a payment than it does for general data access—this will create barriers for consumer access to open banking based on the preferences and incentives of certain institutions. Rather, if financial institutions are permitted to levy fees, those fees should be nominal and should only reflect the infrastructure costs associated with allowing data access. Limiting fees and restrictions on how consumers use their data will protect consumers and promote further innovation in the financial industry.

Data providers have raised data breach and privacy concerns to justify secondary use restrictions, and Apple is very sensitive to those interests given its dedication to protecting users. However, those concerns could be minimized by properly allocating liability to third parties. As such, Apple

Payments Services recommends that the Bureau adopt a rule limiting data providers' liability for third-party data breaches, so long as the data provider transfers data in good faith and is otherwise in compliance with Section 1033. To make sure the rule also protects consumers, it could also clarify that recipients of the data from the data providers would remain liable to consumers for breaches or privacy violations caused by the recipients' own misconduct. This rule would give data providers comfort regarding their potential liability, while continuing to incentivize high security standards across the industry—and allowing consumers the most control over their own data.

* * *

At Apple Payments Services, we support the goal of empowering consumers by expanding their access to trusted financial data. To do so in a way that also respects consumer privacy and innovation, the Bureau should thoughtfully consider who any Section 1033 rule covers. We are proud of the industry-leading privacy and security measures we have built for Apple Pay and Apple Wallet—for more than a decade, we have earned users' trust and built tools that allow them to make informed decisions. The Bureau should create a regulatory framework that allows Apple to continue to provide these privacy-protective services that users value.

Sincerely,

Apple Payments Services LLC