December 23, 2023

Director Rohit Chopra
Consumer Financial Protection Bureau
1700 G Street NW
Washington, D.C. 20552

Re: Docket No. CFPB-2023-0052
RIN 3170-AA78

Submitted via Federal Rulemaking Portal

Consumer Reports wishes to submit these revised comments in response to the Consumer Financial Protection Bureau's (CFPB's) Proposed Rulemaking on Personal Financial Data Rights, issued October 19, 2023. This revised comment letter is an amended version of a comment letter (comment tracking #: lqf-i0ms-sc66) submitted on December 21, 2023. This amended version of our comment letter specifically amends the section entitled: "**Limitations on use of consumer data - secondary use."**

The proposed rule would require certain financial institutions - card issuers and other payment facilitation providers to make consumer data – including transaction data – more readily available to consumers and authorized third parties. It also would place consumer protection obligations on these entities, as well as on third parties authorized to collect and use that data. The proposed rule also creates important standards for data access. The below comments address Consumer Reports overall views on the proposed rule and respond to questions posed by the CFPB referenced throughout the proposed rule.

Summary

Technology is fully integrated into the traditional financial marketplace with the continual introduction of new apps and services which are transforming consumers' access to financial services, relationships with financial institutions, and increasing consumers' digital footprint. In an August 2022 Consumer Reports Survey, we found that 83 percent of Americans—and 90 percent of Americans under age 60—were using at least one fintech app on their mobile devices, and that Americans were using an average of two of the types of fintech apps we asked about.[1] With this context in mind, the convergence of the newest technologies and their integration in consumer finance products and services - Generative AI, Open Finance, Tokenization - may present an opportunity to help consumers receive safer and more fairly

[1] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,123 U.S. adults, August 2022.

priced financial products and services. Yet, with the number of actors involved in the provision of a consumer financial product or service, there are also greater risks to the consumer, particularly when the consumer has no visibility into and no means or rights to know who has access to their personal financial data and there are no clear standards around the collection and use of that data. Business models develop largely around the ability to leverage consumer data and consumers lack any agency to know who has their information and control how it is used. In this environment, consumer data is more frequently in transit, making consumers more vulnerable to increased fraud and scams.

Consumer Reports is pleased to see that the CFPB's proposed rule provides firm and clear guardrails, and uses a rights based data access framework. This will, among other things, provide consumers with rights and control over their financial data through new categories of covered financial data providers, limitations on financial data sharing, an explicit consent mechanism, and the requirement of technical developer interfaces and consumer dashboards to facilitate increased consumer access and control over their own data. In so doing, companies who were largely behind the scenes and whose business models largely tethered to the ability to share and monetize consumer data[2] would have more appropriate constraints around the use of consumer data; and would have to obtain consumer express consent to collect and use their data. Furthermore, consumers may have increased visibility into the true costs of their financial choices, and may more easily move between providers and choose financial services whose business models and data practices align with their interests.

To achieve these outcomes, Consumer Reports advocates for strengthening the final rule notably by:

1. providing more expansive, durable coverage across data categories, sources and uses,
2. removing loopholes which may exclude marginalized groups,
3. making certain exemptions less ambiguous,
4. instituting more constraints regarding the selling of consumer data; tightening authentication protocols to protect consumers from harm,
5. increasing regulatory surveillance over new data ecosystems, and
6. including deterrence mechanisms like financial penalties and private rights of action to uphold safeguards in practice.

[2] As noted in the Rule's introduction, "Divergent interests in the market with respect to the scope, terms, and mechanics of data access, and problems with the responsible collection, use, and retention of data have impeded the negotiation of access agreements and the development of market-wide standards. This leads to inconsistent data access for consumers and costs for the market." By closing gaps allowing previously minimal constraints on data commercialization behind the scenes, coupled with increased user awareness and control channels on usage integrity, the framework appears to balance innovation interests with managing risks from opaque monetization externalities disproportionately impacting consumer welfare alone thus far.

A more robust 1033 rule should go to the furthest to include:

1. Universal coverage - All institutions and core account types should provide consumers with open access to their data by default, irrespective of size, only with strictly bounded exemptions.
2. Transaction history - At least 3 years of detailed transactions should be included rather than limited snapshots that inhibit insights.
3. Third-party permissions - allow consumers to give third-party financial apps permission to securely access their financial data, with strong consent procedures and security standards in place to protect consumers.
4. Competitive parity - Financial institutions should provide the same data access to third parties that they provide in their own applications. This prevents discrimination that limits consumers' choices.
5. Screen scraping backup - The rule should require financial institutions to provide access to consumer financial data through modern APIs (application programming interfaces). Screen scraping should only be allowed temporarily as a backup if companies haven't yet updated their systems to enable API data access. This ensures consumers don't lose access to their financial data.
6. Cover expanded data categories - Regardless of data source or entity type, the rule should expand the scope of data categories to include tax records, student loan accounts and other federal data holdings to help drive financial transparency.
7. Strict licensing constraints - Third parties accessing consumer financial data must agree to fair, non-discriminatory licensing terms. Their licenses should bar them from making consumers waive existing legal rights or privacy protections.

Consumer Reports' more detailed comments below address the following:

- Coverage of "data provider" - what is the scope of products and services that should be covered?
    - feedback on what similar non depository entities should qualify as data providers.
    - Coverage of Electronic Benefits Transfer (EBT) cards[3] and whether issues related to EBT data accessed directly by the consumer and whether these issues should be addressed under payments data, and third-party practices related to

[3] From the proposed rule: "The CFPB is considering whether to add EBT-related data to the final rule, or whether to reach EBT cards in a subsequent rulemaking. While EBT cards differ from the current scope of data types included in the proposed regulation in some ways, they have some significant similarities, including that they are used by consumers to make regular purchases. The CFPB requests comment on whether the most appropriate way to solve issues related to EBT data accessed directly by the consumer is through section 1033 of the CFPA, and whether it should do so as part of this first rulemaking related to payments data or a subsequent rule under section 1033. The CFPB also seeks comment on third party practices related to consumer-authorized EBT data, including the interaction between those practices and the limitations on uses that are not reasonably necessary in proposed § 1033.421(a) and (c). Finally, the CFPB seeks comment on the benefits and drawbacks of enabling third party access to EBT-related data, including with respect to data security."

consumer-authorized EBT data, including the interaction between those practices and the limitations on uses that are not reasonably necessary
    - Exemptions - whether these should extend to non depository data providers that do not provide an interface for their customers and whether exemptions should also extend to non depository data providers that do not provide an interface when the rule is issued but subsequently provide an interface
    - Exemptions - whether small depository financial institutions[4] should be exempted on the basis that the exemption would promote the CFPA's purpose of ensuring that markets for consumer financial products and services are competitive. However some consumers - traditionally excluded and underserved consumers - would not have the benefits of the proposed rule.

- Definition of "consumer" - Should it encompass all individuals or individuals holding specific financial products? Should it include small businesses?
- Establishing and Maintaining data access (§ 1033 (I)(C) C) - Should it be limited to simply accessing data, or include rights to transfer data to third parties?
- Data delivery methods - What technical standards, interfaces and transfer mechanisms appropriately facilitate consumer data access?
- Categories of data covered - What constitutes "account and transaction data"? Should aggregated data or metadata be included?
- Data scope & usability - What specific data elements, history windows, and use case requirements meet consumer needs?
- Data accuracy, security & privacy - What data handling practices, quality controls and consent requirements should apply to all providers?
- Other rights & freedoms - Does existing regulation adequately govern fees, usage restrictions and other potential data harms?

These comments are detailed below.

Coverage of data providers (§ 1033.111(a) through (c))

We advocate for expansion of the types of data providers to be covered under the proposed rule to include nondepository entities which are often part of the broader banking ecosystem. Additionally we would like to see inclusion of Electronic Benefits Transfer cards also included as a data provider.

[4] From the proposed rule: "The CFPB has also preliminarily determined that the proposed exemption would promote the CFPA's purpose of ensuring that markets for consumer financial products and services are competitive. As noted above, the depository institutions that would be exempt from the proposed rule's requirements tend to be very small institutions that may not be as technologically sophisticated as larger institutions and likely do not have the resources to support or maintain the interfaces that would be required by the proposed rule. Subjecting these institutions to the proposal could significantly disrupt their businesses, potentially threatening access to consumer financial products and services and reducing competition for consumer financial products and services—both contrary to carrying out the objectives of CFPA section 1033."

Non depository entities that should qualify as data providers under the proposed rule

While not holding customer deposits, there are a vast array of non depository entities that we would urge the CFPB to consider including as a qualified data provider under **§ 1033.111(a).** These organizations play a significant role in the financial services ecosystem as they provide valuable data that contributes to the enriched services offered under open banking frameworks and are connected to or communicate with the consumer's underlying transaction account which support some of the functions relied upon by covered data providers under the current proposed rule. These entities and services also play a significant role in consumer financial lives. Examples of such non depository entities include:

- Payment Service Providers (PSPs) that facilitate payments for goods and services or process money transfers. This includes online payment gateways, mobile payment services, and e-wallet providers.
- Investment Firms and Brokerages that offer investment products and services. They might provide data related to investment accounts, stock trading, retirement accounts, and wealth management services.[5]
- Credit Bureaus and Credit Reporting Agencies that collect and provide information about individuals' credit histories, including credit scores, credit accounts, and repayment histories.
- Fintech Companies offering various products like peer-to-peer lending, crowdfunding platforms, robo-advisors for investment, and personal finance management tools.
- Bill Payment Services that facilitate the payment of utility bills, rent, or other regular expenses often interact with a consumer's basic banking transaction account. They can provide data on payment history and outstanding bills.
- Loyalty and Reward Program Providers managing loyalty programs and rewards are a large feature of the credit card market; the companies are connected to consumer credit card transactions and have insights into consumer spending patterns and preferences.
- Financial Management and Budgeting apps aggregate financial data from various sources to provide users with a comprehensive view of their finances, including spending habits and savings.
- Non-Bank Lenders include various types of credit institutions that are not traditional banks, like payday lenders, student loan providers, or businesses offering buy-now-pay-later services.

[5] In the spring of this year, Consumer Reports collected consumer stories on their experiences with data brokers or ending up in scenarios which are beyond the originally agreed use of their data. The following consumer describes some of the challenges consumers can face with regard to the downstream use of consumer data in the investment context. "I subscribe to a stock advisory service. I receive offer after offer of unwanted advice on investments of all kinds. I'm sure my advisor's support company is selling my information and generating all the unwanted emails. I have asked them specifically not to share my email or address with others. Probably a waste of effort because the flood continues!!!"

In a true open banking ecosystem, these entities should be subject to the same standards and conditions to share their data (with customer consent) to create a more holistic financial picture for each user, enabling more personalized and efficient financial services.

Electronic Benefits Transfer (EBT) cards

Consumer Reports advocates for the expansion of data providers to include Electronic Benefits Transfer card providers. Over 40 million Americans rely on needs-based EBT card programs for essential food and cash assistance; enabling consumer data access would vastly impact financial lives[6]. Bringing EBT cards into the consumer data access framework outlined in the proposed rule also aligns with the goals of Section 1033 by driving financial inclusion, welfare, and innovation through data empowerment. Inclusion of EBT cards acknowledges the interconnectedness of payment data sources that collectively influence consumer financial lives. It enables budgeting insights from a major spend category for many low-income families. A harmonized data access framework that cuts across public and private data holders would best serve consumers.

Financially vulnerable consumers rely on EBT cards the same way others rely on bank accounts and payment cards. Because EBT cards serve similar functions for managing money and making transactions, EBT data access should have equal protections. Thus it is important that EBT cards and related data services be included under this proposed rule. These parallel functions include a standardized, electronic payment card, use of debit cards, PIN access, checking balances, etc. Program designs allowing small cash withdrawals can help cardholders demonstrate responsible debit card management and start establishing positive payment histories.

[6] EBT cards provide benefit recipients both convenience as a payment method and oversight of their benefit funds each month when facing food, financial and other insecurities. By enabling financial access for vulnerable segments of the population and providing a gateway for them to build digital fluency, credit history, and engage more meaningfully with banks, payment networks, retailers and the broader financial ecosystem. EBT cards can support the most vulnerable consumers' entry into the banking ecosystem, leading to more open checking / savings accounts.

EBT cards operate on the same payment rails as mainstream debit cards, thus consumer users of EBT cards have similar challenges accessing their own data. These include:

1. Trouble accessing their full transaction and account history through an online portal. This makes monitoring and record-keeping difficult.
2. EBT cards can be vulnerable to skimming, online fraud, and theft like other debit cards. Customers may lose benefits or have trouble getting fraudulent charges reversed. More control over their own EBT card data would allow consumers to better understand spending patterns, contest errors, avoid fraud, etc.
3. Complexity of EBT system. The rules around receiving and using food and cash benefits can be complex. Consumers may have trouble understanding restrictions, expiration of unused benefits, etc.
4. Difficulty managing card and PIN. Keeping track of an EBT card and PIN, requesting replacements when lost, or changing a forgotten PIN can be challenging processes for some consumers. Consistent access to a consumer interface would vastly improve the consumer experience.

Better data access, fraud protection, ease-of-use measures and consumer education could help improve the experience for EBT consumers. Streamlining processes could also reduce stigma and barriers to getting assistance. Additionally, as EBT systems are already electronic, providing consumer data access through APIs requires minimal incremental costs and would provide consumer data access on par with mainstream banks. Additionally, consumer-permissioned data access creates opportunities to develop tools and services that improve the EBT consumer experience.

The complex rules governing usage conditions and qualifications around programs like SNAP and TANF administered through EBT systems can disadvantage consumers lacking proper visibility. Hence the rule should be expanded to uplift safeguards in the following ways:

1. Mandate standardized monthly account statements itemizing cumulative balances, transaction categorizations, imposed fees and expiries for unused allocations.
2. Require plain English disclosures around terms like time-bound usage, items eligibility like approved retailers or product types and re-certification policies as searchable tracking.
3. Institute proactive notifications for approaching expiration of allocated unused benefits as cautionary alerts to cardholders through multiple channels.
4. Enforce interoperability standards for data access including detailed transaction histories to seamlessly port records into personal finance apps helping track, budget and optimize household use aligned to qualification criteria.

The proposed rule should thus be expanded to encompass EBT card systems as a key data holder subject to consumer data access rights and safeguarding requirements. Inclusion would have significant consumer impact, providing parity in data access and allowing consumers to have better budgeting ability, dispute resolution and management of this critical lifeline. Bringing

EBT systems within 1033 establishes consistent expectations for transaction data utility and portability irrespective of source (government or private sector). It upholds the principle of equal data rights applicability.

The rule should classify EBT systems as a payment processor bound by provisions around data delivery methods, accuracy, security and consumer control applicability to private processors. Interaction with existing EBT program regulation can prohibit uses of accessed data that violate restrictions on benefits utilization monitoring.

Excluded data providers (§ 1033.111(d))

The proposed rule would exempt data providers (as defined in proposed §1033.111(c)) from the requirements of the proposed rule if they have not established a consumer interface as of the applicable compliance date. The rule also exempts certain smaller relationship based depositories such as credit unions and community banks that do not offer any such service. As the rule points out, “among credit unions with fewer than 1,000 deposit accounts, only 21 percent offer online banking services.” The CFPB additionally requests comment on whether there are non depositories that do not provide an interface for their customers, and if so, whether an exemption should include them; and, whether it should require any exempt depositories to make covered data available in a non-electronic form.

Consumer Reports would advocate for the broadest and deepest parity of data access for consumers possible to conform with the spirit of the rule 1033 rulemaking. Digital access is an important defining issue in financial inclusion and a rule which excludes a whole swath of consumers, based on the fact that they lack equal access to digital financial services that are accessible to mainstream consumers, will not incentivize relationship banking institutions and the broader financial services ecosystem to develop critical technical, technological infrastructure to support ever increasingly complex consumer data needs.

The proposed rule's exemption for data providers without a consumer interface raises important concerns around equitable data access that the CFPB could better address in order to avoid reinforcing systemic digital access inequity.

1. Significant consumer data resides with processors lacking customer portals and these data are vital for consumer insights. Payment networks, data utilities, account/transaction aggregators often have expansive financial histories but currently don’t provide direct access. Consumers who lack access to higher quality financial products can and should benefit from access to their own information. Even without interfaces, these datasets enable critical categorization, cash flow planning and decisioning functionality for budgeting apps, lenders etc.

2. There is a risk that the rule - without inclusion of these depositories and non depositories would further entrench data monopolies. Incumbents could consolidate further and inhibit competition from disruptive entrants needing broad data access.

3. Non-electronic access, while a good step forward, has limitations and would reinforce a tiered approach in financial quality and offerings for the most vulnerable consumers. Providing only statements/reports via mail has narrow utility vs machine readable exports that better serve digital tools.

As such, the CFPB should mandate API/download based machine access at minimum for all providers based on technical feasibility irrespective of customer portal presence. This upholds the essence of portable and usable data access in the marketplace rather than just principles. Phased stipulations allowing market solutions to mature - such as longer timeline exemptions for the smallest institutions - are a better transition strategy than broad technology-linked exemptions to address adoption challenges that exist today. Additionally, there are a few approaches which should be considered by the CFPB that could make implementation of required digital data interfaces under the proposed rule more feasible for smaller depository and non-depository financial institutions without causing excessive burden:

1. Shared industry utilities. Smaller entities could collaboratively invest in shared data access infrastructure hosted by a common third-party rather than each building custom interfaces. API costs are amortized.
2. Turnkey packages from core processors - Major provider systems like FIS, Finastra, Fiserv that host small bank/CU core systems could enable white-labeled data access as part of existing contracts.
3. Reference approaches and tools - Industry groups and vendors could publish open-source templated data access code, demo integrations and testing suites to simplify adoption.
4. Cloud services leverage - Solutions like Stripe, Plaid, Yodlee could offer data interface modules usable by clients to minimize software development needs.

Overall, a combination of market utilities, turnkey packages and phased stipulations could provide a transition path for small firms lacking scale/skills to stand up API-based data access independently in the near term.

Definition of "consumer" (§ 1033.131) - Should the definition of consumer encompass all individuals or individuals holding specific financial products? Should it include small businesses?

The CFPB is proposing to define the term consumer to be a natural person to distinguish the term from the third parties that are authorized to access covered data on behalf of consumers. In our view the proposal takes an expansive view by defining a "consumer" as any individual or small business seeking access to their financial data under Section 1033 are aligned with the spirit of Section 1033 of DFA to empower all consumers. Limiting data access rights by product, sector or entity would potentially exclude underrepresented consumers and would establish parity of data access rights across the broader banking, financing and payments landscapes. Additionally, the inclusion of small business would recognize and include scenarios where personal and small business financial lives are interconnected and that there is an important value to enable permissions-based data portability to serve both worlds.

Data Scope and Usability. Subpart B.

Making covered data available.

The CFPB requests comments on the benefits and data needs for consumers who are in the process of switching accounts. Enabling easy access to key financial data during account switching is pivotal to ensure true portability and competition across providers. While the proposed covered data definition allows some baseline transition support, Consumer Reports is of the view that additional data attributes would significantly smooth switching journeys. These attributes should include:

1. Account Credentials - login usernames/passwords, challenge question responses, device identifiers registered for multifactor authentication given security dependencies.
2. Transaction Mapping - categorization of payees, tagging of recurring vs sporadic payments and ability to download high frequency transaction lists to easily set up at new provider.
3. Customer Service History - records of support interactions, complaints, fulfillment status so that consumers may continue to have oversight on any dispute resolution progress when moving accounts.
4. Associated Documents: statements, contracts, tax documents related to closure of existing products so ongoing liabilities, claims and audit needs aren't disrupted.

In considering these additional attributes, there are indeed some data sensitivity challenges which ought to be addressed to ensure their inclusion does not increase consumer vulnerability to fraud and scams. Their inclusion in any amended coverage thus should be coupled with stringent access controls to provide true continuity of financial context when consumers switch out of restrictive vendor lock-ins into better products or rates.

Historical data. (*§ 1033.211(a)*)

The CFPB proposed rule § 1033.211(a) explains that a data provider would be deemed to make available sufficient historical transaction information if it makes available at least 24 months of such information. In the SBREFA Outline, the CFPB considered a data parity approach to historical transaction data, where a data provider would only need to share as much historical transaction data as it makes available through a consumer interface. However, in the proposed rule, the CFPB notes concerns that, "in practice, a data parity approach would be difficult to enforce and would leave some consumers without sufficient historical transaction data to support transaction-based underwriting, account switching, and other use cases.[7]"

Consumer Reports believes a 36 month safe harbor for transaction history data strikes the right balance between parity, utility and feasibility. However, additional provisions around historical data access would further prevent consumer disadvantages. Specifically:

1. Timeline parity for all categories. The CFPB should apply a 36 month access parity across transaction, account terms, ownership changes, interest rate modifications and fee updates. This would prevent provider cherry picking of beneficial histories only.
2. Machine access mandates irrespective of portal visibility. Financial companies should give the same technology access to historical data to consumers and third parties that they can already view in account portals. Even lengthy records available now only by manual requests should allow automated access through APIs or data downloads. This ensures fair data access no matter how someone connects to their information.
3. Change log accessibility. Metadata should also be included in account and transaction data in order to facilitate and detail changes to account attributes and transactional mappings over 36 months so adjustments can be programmatically reconciled on connected applications.
4. Close loopholes allowing resetting clocks. Financial institutions should not be allowed to reset the 36 month transaction data history clock by arbitrarily opening "new" successive accounts and deprecating old identifiers. The CFPB's proposed 1033 rule should constrain financial institutions from exploiting such loopholes.

Equal historical access provisions across all relevant categories prevents selective data use disadvantages to consumers. Change logs and parity constraints uphold transparency and fairness. With these improved protections, the 36 month provision delivers useful longevity.

Terms and conditions

The CFPB requests comment on whether the final rule should include more examples of information that must be made available under terms and conditions. As outlined, the proposed rule spans the suite of parameters needed for consumers to fully understand "what's under the hood" across key account types - not just superficial descriptors. Consumer Reports recent

[7] TK cite to proposed rule

reviews and comparative evaluations of popular fintech apps, for example, demonstrate that indeed oftentimes important information is buried in the fine print and companies can be more plain and transparent disclosing important information. The CFPB's proposed rule, by reaching into historically obscured fine print, could help to guide usage and switching decisions beneficially.

The proposed rule, however, could benefit from expanded, granular examples of mandatory disclosures or additional data points to include under "terms and conditions" provisions. Some clearer specifications could encompass:

1. Historical changes over 36 months in core pricing terms like minimum balance tiers linked to specific interest rates and associated monthly fees.
2. Latest program eligibility requirements and restrictions around services like overdraft coverage, disputed transaction rights and small-balance waivers.
3. Complete fee schedules spanning deposits, payments, transactions, wire transfers and other common product levies mathematically denoted.
4. Comprehensive qualifications and eligibility formulas underpinning promotional rates, rewards earnings, and cross-sell offers referencing precise thresholds, exclusions and limitations.

Adding more discrete illustrations tied to known categories of common fees, pricing, qualifications and product policies can more effectively govern data accessibility for consumers. It disrupts opacity advantages institutions have profited from by preventing vague disclosure compliance and in turn providing consumers access to vital data parameters needed for sound financial decisions.

Account Verification

The CFPB requests comment on whether the proposed basic account verification information category would accommodate or unduly interfere with beneficial consumer use cases today and whether it is appropriate to limit this category to only a few specific pieces of information. Consumer Reports believes that the CFPB's proposed scope of basic account verification strikes the right balance between utility and risk. Because mandating Social Security Number (SSN) data availability creates disproportionate vulnerability without proportional value in most consumer data use cases, we would advise against requiring inclusion. Specifically SSNs:

1. Are not imperative for common account verification purposes like checking name/address consistency or confirming email/phone ownership. Regulated entities can request this explicitly if truly required.
2. Enable criminal impersonation attempts and exacerbates identity fraud potential across financial systems if protections fail given heightened data sensitivity.

3. Are unnecessary and provide little upside for typical budgeting, payments and other everyday apps centered around transaction visibility rather than intensive credit adjudication.

As such, limiting account verification information to contact information balanced against risk of loss is prudent here. However, to uphold principles of parity, any provider that voluntarily provides SSN visibility within their own interfaces should equally enable access to externally connected applications upon appropriate consumer consent. This upholds an equal playing field without disproportionate risk transfer in the name of data portability.

Data scope exceptions

Where the proposed rule includes certain categories of data for which data holders are not obligated to provide full consumer data access in specific restricted cases, the CFPB has asked for comment on whether the rule should include additional examples of data that would or would not fall within the exceptions, and whether this provision sufficiently mitigates concerns that data providers may cite these exceptions on a pretextual basis.

Consumer Reports advocates for limited exceptions and only ones that must also serve consumers' interests, not institutions alone. Otherwise, data holders may try exploiting allowable exceptions to restrict consumer data access primarily to defend competitive advantages, retain exclusivity, and avoid transparency - rather than legitimate infrastructure constraints. Potential pretexts which could cause consumer harm which may be cited by data holders may, for example, include: spurious cost constraints that hamper only specific data utilities rather than total availability, false infrastructure limitations when viable interoperable formats are discarded, and risk standards invoked unevenly across portfolio offerings without cause.

Oversight and transparency requirements limiting subjective application of data access exceptions, coupled with customer empowerment would ensure exceptions don't undermine 1033's promise. Thus, the CFPB should additionally consider:

1. Inclusion of quantitative coverage thresholds to prevent cherry picking. For example, the exceptions would apply only if less than 5% of the consumer base will experience data denial for their specific products.
2. Inclusion of a third party audit requirement. The CFPB should consider requiring independent annual evaluations of cited rationales for invoking exceptions that validate evidence consistency and ethical application.

3. Including additional mechanisms to uphold market discipline by facilitating consumer visibility and choice such as notification and disclosure. If exceptions will be applied to their data access, proactive notifications should allow consumers to close accounts from restrictive institutions.

Establishing and Maintaining data access. Subpart C. Should data access be limited to simply accessing data, or include rights to transfer data to third parties?

We are pleased to see that the CFPB has outlined in its proposed rule robust data access rights which preserve both the right for consumers to directly access their financial data as well as grant permission to third parties to access data in order to enable full value realization. By establishing what specific consumer financial data companies must make available and allow access to, it ensures consumers can actually use the data access rights set out under section 1033 in practical ways - not just empty promises.The inclusion of specific technical standards, additionally guarantees that concrete data access rights are durably upheld across providers, transitions, and market changes rather than just an aspirational standard that erodes over time. Additionally, to balance innovation of data portability with safeguards, the rule establishes clear requirements around consumer control, transparency from third-parties and accountability for data holders on downstream usage.

Specifically, we are pleased to see that this section of the rule:

1. Provides accountability around compliance by outlining standards to compel actual delivery of data access by requiring covered providers to maintain a consumer interface and to establish and maintain a developer interface, not just rely on good faith efforts.
2. Outlines technical specifications for data availability in practice, preventing companies from using obstacles like format restrictions or selective data sharing to avoid giving full consumer access and benefits.
3. Outlines security and privacy safeguards such as the requirement of proper containment controls, consent flows for sensitive financial information, and limiting provider and third party use of consumer data to only what is necessary to provide the service.

Overall, these provisions put consumers in the driver's seat enabling them to leverage financial tool innovation and specialized data analytics features to their advantage when data can flow into budgeting, savings, investing apps etc. Additionally, these data access rights will allow for consumers to more easily port their data when changing financial service providers, promoting competition when consumers aren’t locked into vendor ecosystems and interfaces.

We would urge the CFPB to ensure that the final rule continues to include important safeguards which protect consumers against risks of third party access to their data, even if permissioned. These include:

1. Data minimization requirements which limit secondary use of consumer data. This will limit / reduce avenues for data misuse or exposure and provide accountability around downstream usage. These requirements will also reduce misleading marketing or upselling.
2. The requirement of consumer and developer interfaces to allow for centralized view of data; explicit consent and revocation mechanisms; and help consumers with the complexity of tracking and managing permissions granted across expanding third-party ecosystems.
3. Prohibition on data providers imposing fees or charges for establishing or maintaining the interfaces required under the proposal.

Qualified industry standard (§§ 1033.131 and 1033.141) what attributes are helpful for ascertaining whether open banking standard setting bodies are fair, open and inclusive.

The CFPB has asked for comment on the adequacy of the proposed rule's qualified industry standard definition and whether these proposed attributes are helpful for ascertaining whether an open banking standard-setting body is fair, open, and inclusive. Consumer Reports believes that the proposed rule sets reasonable baseline attributes to assess if an industry standard-setting body for open banking data sharing models is sufficiently inclusive and collaborative. The rule includes important key attributes notably:

- requirement of solicitation from diverse stakeholders,
- transparent decision processes,
- publicly available standards documentation, and
- fair license cost structures.

These together would help to prevent exclusionary practices. The attributes in the proposed rule indeed provide a sound foundation for driving collaborative standards and some augmentations - outlined below - would further bolster CFPB's objectives. However, Consumer Reports recommends the following augmentations to further validate open governance. The rule should include:

1. Balanced representation rules in standards development committees to prevent any single category of entities (e.g. large banks) from unilaterally dominating decision making.
2. Expectations around response processes for addressing stakeholder input during standards development so feedback doesn't get ignored. Current standards bodies, for example, in addition to not having balanced representation do not also provide the same voting rights across categories of membership.

3. Quantitative or percentage targets for standards adoption across implementation categories like small banks, credit unions etc. High concentration among a few large providers indicates lack of multi-stakeholder relevance.
4. Clear appeals/dispute resolution mechanisms for standard setting process or decisions called into question later for fairness or transparency issues.

Adding parameters that expressly monitor balance of influence, would better ensure effective oversight guardrails against standards getting gamed to benefit specific groups rather than consumers' priorities around safe and useful data.

Third party access and data risk management.

The CFPB requests comment on the extent to which CFPB rule or guidance, or other sources, should address whether a data provider's denial of third party access to a developer interface under § 1033.321(a) would be reasonable with respect to any particular risk management practices. Consumer Reports understands that denying third-party access may create inherent consumer disadvantages regardless of cited risk management rationales. Reasonableness standards without oversight mechanisms carry high abuse potential but may also frustrate a consumer's right to access data under CFPA section 1033. This balance can be struck in the 1033 rule by:

1. Requiring companies to use a common risk assessment approach to balance data access versus security priorities. This standardized methodology applies fairly across different financial sectors. It aims to prevent one-sided data access denials based on individual companies' subjective judgments.
2. Requiring denial justifications include portal parity provisions - any access permitted internally must have external corollaries secured to equivalent levels. Prevent arbitrary restrictions.
3. Instituting consumer choice preservation principles for tapering third-party data access through easily porting data directly to replacement services. Don't terminate usage.
4. Enforcing interoperability principles so data holders utilize common, non-proprietary architectures. Ensure denial excuses aren't protecting closed ecosystems.
5. Enabling collective redress mechanisms. The rule should allow consumer advocacy groups to formally dispute unreasonable barriers that block financial technology innovators from accessing the data they need to build competitive market alternatives to incumbent options. Allowing consumer interests to collectively challenge restrictions through an organized redressal process strikes the right balance between open data access rights and managing risks.

In essence, "reasonable access" without governance guardrails has enabled platforms historically to frame protectionism as prudence. In this context warnings, for example, warnings against securitization risks were ignored until systemic contagion after proprietary risk modeling

flourished absent oversight, leading to a financial crisis. Access priorities must be collectively informed, not individually invoked to preserve status quo against innovation threatening incumbents most.

Data accuracy, security & privacy - What data handling practices, quality controls and consent requirements should apply to all providers?

Consumer Reports is supportive of an expansive 1033 proposal that facilitates consumer ability to permission their data and supports pro-consumer interests such as data portability. That said, the proposed rule may not prevent unintended privacy erosion as an inevitable byproduct of well-intentioned ambitions without appropriate corresponding protections crafted for this shifting landscape. The proposed rule makes some accommodations on a few of the specific privacy rulemaking requests made by consumer groups, but gaps remain in formalization of certain safeguards in the current draft:

1. Privacy impact assessment requirements are not explicitly mandated; the rule only encourages assessments or voluntary frameworks. Privacy impact assessments would help to assess risks from expanded data collection or sharing enabled under new access pathways.
2. Prohibitions exist on using accessed data to discriminate in credit eligibility, but protections excluded for other areas like employment, housing and insurance, which despite permissions granted, could exacerbate exclusion in employment, housing and insurance eligibility.
3. Downstream data flows have to be disclosed by primary collectors in the proposed rule but no visibility requirements for second order onward transfers. We had hoped to see more formal requirements for transparency into downstream data flows detailing each onward transfer as well as purposes from initial access points, rather than just first tier visibility.
4. The rule neither prohibits indefinite storage retention nor provides firm storage expiry mandates for post usage period, collected consumer financial information. Indefinite retention is only discouraged. The rule should prohibit indefinite storage retention and explicitly outline any exception.

5. While purpose limitation principles govern initial collection bounds in the rule, such as identifying that purposes such as sale of consumer data or collection for use in targeted advertising[8] is not considered necessary to use the service, the rule provides no

[8] In the spring of this year, Consumer Reports collected consumer stories on their experiences with data brokers or ending up in scenarios which are beyond the originally agreed use of their data. This consumer describes experience in the payment context:
"Baited with free offers, bombarded with unwanted mail. It seems every time a purchase is made they give you some sweet 20% off offer or better "by just submitting your email". Unfortunately it's a tactic used to capture your data and attempt to sell you more and more ads and share your email with others. It's gotten to a point where my email has thousands of spam advertisements and hundreds of junk emails per

constraint requirements to be instituted on downstream sales or monetization by primary apps accessing data.
6. The rule provides no new private right of action for enforcement compared to current mechanisms under existing acts like GLBA.

Gramm-Leach-Bliley Act and private right of action

While the proposed 1033 rule does not inherently weaken existing Gramm-Leach-Bliley Act (GLBA) protections governing consumer financial data privacy and sharing permissions, Consumer Reports advocates for and would support a rule which goes further to create more explicit privacy protections for consumers. Specifically, while GLBA today requires banks and insurers to provide privacy notices and opt-out choices for data sharing with third parties, many prominent fintech apps, data aggregators and payment processors remain outside its supervision perimeter.

Consumer Reports is glad to see that the proposal covers these previously unregulated entities to ensure consumers retain visibility and control uniformly over financial data access now increasingly flowing through tech mediators.

Consumer Reports would advocate for an explicit private right of action that empowers consumers to legally pursue penalties against companies violating data access or usage provisions under the proposed 1033 rulemaking. Private consumer action rights play an important role in upholding accountability in data access, privacy commitments and policy ambitions codified in rulings. They provide commensurate checks against predictable marketplace incentive problems and should be included in the CFPB's proposed rule because:

1. Court adjudicated remedies often supplement scaled, risk-based supervision as consumer protection agencies often have resource constraints limiting oversight capacities. This is heightened amid the rapidly evolving data ecosystems across consumer finance. Thus, a private right of action provides more accessible, timely and cost-effective resolution avenues compared to sole reliance on lengthy regulatory complaint mechanisms after incidents manifest at scale.
2. The threat of private lawsuits can work as an economic deterrent, incentivizing compliance investments proportional to actual consumer risk exposure levels.

---

day. Sometimes a really important job offer or other correspondence is literally lost in a sea of junk e-mail clogging my mail and preventing me from seeing what I actually need to see.

You can go ahead and try to unsubscribe but sadly your efforts are futile. Suddenly you will be bombarded with thousands of useless unwanted emails from similar companies that want your business. Some companies send multiple emails daily meaning I may have twenty emails from one business that I never signed up for. Don't fall for the bait! Be smart and reject these offers or any website that won't let you proceed to shop without providing your data."

3. Consumers also need the ability to be made whole; thus individual redress makes data rights tangible rather than theoretical standards without restitution pathways for access denial or misuse issues.

Limitations on use of consumer data - secondary use

Under the proposed rule the use of covered data that is not reasonably necessary to provide the consumer's requested product or service—i.e., secondary uses—would not be permitted as part of the third party's authorization to access the consumer's covered data. We acknowledge that effectively de-identified data, which cannot be reasonably re-identified, does not pose the same privacy risks as personal information, and that such data is crucial for research, product improvement, and ecosystem safety.

The rule's current specifications:

1. Require providers to disclose at initial consent any commercial use intentions, while encouraging data security and usage accountability.
2. Limit sharing access credentials or authentication details which pose immediate account fraud threats, but no constraints are required around sharing anonymized behavioral insights.
3. Prohibit access under false pretenses for outright fraudulent collection, but there are no usage ceilings for authorized collectors to address overhoarding.
4. Provide a right to opt-out and revoke access with specific data holders, but no facility to govern subsequent transfers by collectors to onward third parties.

The CFPB also requests comments on whether any secondary uses should be allowed through an opt-in mechanism. In requesting comment, the CFPB rightly notes in its proposed rule that there are some secondary uses of consumer data by third parties which could benefit consumers such as improved products and adjusted pricing which benefits the consumer.

On balance and with consumer consent, there are other additional uses such as innovation to improve consumer products and experience, or to prevent fraud, which may confer more benefit than risk to consumers.

Any restrictions on use should differentiate between truly de-identified data and re-identifiable data. Therefore, we suggest that use restrictions should not apply to data that has been effectively de-identified and cannot be reasonably re-identified. This approach enables the responsible utilization of valuable data while maintaining robust privacy protections. For re-identifiable data, which has not been effectively de-identified, we support stringent use restrictions to ensure consumer privacy is not compromised. It is essential to have clear guidelines and criteria to differentiate between truly de-identified data and re-identifiable data, with the latter subject to strict use limitations.

Consumer Reports would support an opt-in mechanism alongside specific prohibition of high risk secondary usage scenarios which warrant additional safeguards. These include:

1. Granular transaction histories fueling hyper-targeted marketing of predatory products to vulnerable demographics flagged through cashflow instability insights gleaned after initial data access.
2. Wealth indicators or home ownership data elements powering discriminatory exclusion from credit eligibility through non-regulated scoring algorithms deployed without consumer visibility.
3. Opaque bundling deals with commercial partners like retailers and tech platforms enabling broad data sharing well beyond authorized scopes marked through permissions under false declarations of necessity.
4. Behavioral insights derived from location, spending habit data mixes enabling legally unconstrained profiling which could limit socio-economic mobility via invisible scoring barriers shaping vital opportunities selectively.

Taking personal details from people's financial transaction records without oversight can lead to harmful impacts over time. Individuals may lose control over their information. Marginalized groups may face more barriers to opportunity. Basic rights to privacy as both individuals and communities may be slowly taken away. For example, little control exists over downstream usage, resale or derivative analysis by apps after initial data is pulled based on original consent. This leaves major privacy blindspots and risks for consumers.

Consumer Reports would recommend the following considerations and adjustments to the use limitations and secondary use provisions of the rule.

1. Ensure trailing oversight mechanisms, specifically ongoing governance capabilities, to allow consumers visibility and control on how financial information, once accessed by permitted third party apps, would get subsequently utilized for commercial purposes over time. The rule should ensure consumers can continuously monitor or govern usage integrity after changing motives.
2. The existing rule's requirement for a 12-month reauthorization and data deletion upon access revocation provides important safeguards. Rather than blanket mandatory expiration periods, any additional expiration period requirements for raw data holdings should align with these existing protections to avoid redundancy.
3. While the proposed rule lacks subsequent consent or transparency demands for downstream changes, we emphasize support for a system where data, if passed downstream, would still require transparency and consent, particularly in an opt-in regime.
4. Expand parity in civil liability for harms like discrimination, fraud etc. whether caused directly by primary apps or through second-order data propagation across wider commercial ecosystems.

5. Increase penalties and fines for violations to heighten deterrence incentives around responsible data stewardship motivating higher investments in governance by the fintech sector.

Consumer Reports would advocate for an opt-in mechanism allowing consumers choice in secondary data use beyond the primary purpose, rather than outright restrictions. Clear and informed permissioning upholds privacy while enabling beneficial use cases around innovation and fraud prevention. Overall we aim to strike a balanced approach considering both privacy protection needs and potential innovation/product development benefits from responsible data leveraging under appropriate oversight. Fostering an ecosystem where consumer data can be used with accountability also serves public interest. Fundamentally, stronger constraints on downstream freedoms combined with deterrence systems for non-compliance can uplift incentives furthering consumer welfare over solely commercial interests as data permeates sectoral ecosystems.

Consumer awareness and education

For consumers to fully reap the intended benefits of open banking requires that they must first understand how it works and become comfortable using it. However, this can often prove to be a challenge. In the modern digital world, consumers have become increasingly cautious regarding their data privacy and security (for good reason). Open banking may come across as complex and risky for some consumers. Other consumers, excited about the apparent convenience and increased capabilities, may be at increased risk of fraud and scams. A lack of understanding and mistrust toward open banking has hampered uptake in other countries. For example, research from the United Kingdom, where open banking has been in place for over five years, found that 60% of consumers still do not fully understand open banking, 63% do not use it, and 84% do not fully trust it.[9]

Consumer Reports suggests that it would be beneficial to integrate considerations regarding consumer awareness and understanding into open banking implementation from the start. For example, concrete steps that could be taken include requiring that consumer interfaces be designed to be intuitive and user-friendly and embed clear guidance and instructions for consumers on how to utilize open banking-related features and functions. Features and functions such as setting limits on use of data and rescinding authorization should be easy and intuitive to use and accompanied with clear explanations.

More broadly, guidance and education and awareness campaigns from both industry as well as government would be beneficial. These campaigns should include clear and simple explanations of what open banking is, how it can be used, how it benefits consumers, and what safeguards are in place. Guidance and education would benefit from concrete examples and illustrations of use cases for open banking. For example, the Australian Competition and

[9] https://uk.nttdata.com/news/five-years-on-and-60-percent-of-consumers-still-dont-understand-what-open-banking-is

Consumer Commission provided educational materials and resources to help consumers understand open banking and their rights when first launching their open banking regime.

Thank you for the opportunity to submit these comments. For further information please contact Delicia Reynolds Hand, Director of Financial Fairness, Consumer Reports at Delicia.Hand@consumer.org.

Appendix - Consumer Stories

The below excerpts of consumer stories represent anecdotal examples of the varying challenges consumers can have with downstream use of their data.

Issue	Consumer Story
A Flood of Unwanted Advice and Advisors	I subscribe to a stock advisory service. I receive offer after offer of unwanted advice on investments of all kinds. I'm sure my advisor's support company is selling my information and generating all the unwanted emails. I have asked them specifically not to share my email or address with others. Probably a waste of effort because the flood continues!!!
Database blues	More times than I could ever count in recent years, my personal data, and many times incorrect, has appeared in numerous databases. These data brokers don't bother to check or verify whether or not that information is factual. Trying to get personal data removed is nearly impossible. I have had to pay a firm that specializes in removing information from databases, and although they do a good job, it still does not stop the proliferation of my personal data including social security number, addresses, phone numbers, etc from appearing in these databases. My personal data should be Just that, personal! There should be a federal law against data brokers, and data harvesting!!! Why should I have to spend money, not to mention all the time and hassle and headache, because of greedy #@$&@/!
Unwanted Investing Advice	I think one investor newsletter I subscribed to sold my email address. I was receiving 5-6 unwanted, unsolicited emails a day and I made the mistake of unsubscribing to one. Now they know I am real and am now receiving 60 a day. I don't dare try and unsubscribe. They say they come from India, the UK, Delaware is a big one, Indiana, all over the place. I am at a loss to know how to stop it.
Baited with free offers, bombarded with unwanted mail	It seems every time a purchase is made they give you some sweet 20% off offer or better “by just submitting your email”. Unfortunately it’s a tactic used to capture your data and attempt to sell you more and more ads and share your email with others. It’s gotten to a point where my email has thousands of spam advertisements and hundreds of junk emails per day. Sometimes a really important job offer or other correspondence is literally lost in a sea of junk e-mail clogging my mail and preventing me from seeing what I actually need to see. You can go ahead and try to unsubscribe but sadly your efforts are futile. Suddenly you will be bombarded with thousands of useless unwanted emails from similar companies that want your business. Some companies send multiple emails daily meaning I may have twenty emails from one business that I never signed up for.

	Don’t fall for the bait! Be smart and reject these offers or any website that won’t let you proceed to shop without providing your data.
Data Broker Hacked in January 2023	The data brokers involved are Truthfinder and Instant Checkmate both entities are owned by PeopleConnect Holdings, Inc. that affected 20.22 million users, with the sole purpose of finding information about people. On 4/20/2023, I was notified by Experian IdentityWorks that my personal info was compromised and found on the dark web directly related to Truthfinder and Instant Checkmate's data breach. None of the 20.22 million breached users were notified of the alleged breach, as of this date. I have not found any class action taken against PeopleConnect Holdings, Inc.or its two entities that were breached. I am considering filing a class action, as soon as I locate appropriate legal counsel that are willing to take this matter further.
ms	Two years ago, I started to shop online to change auto insurance. My data was shared and I received all kinds of calls to both my home and cell phone numbers as well as online requests for more information.
Stolen CC # won’t stop it	My credit card was compromised and used for purchases at a Safeway store states away from me. I contacted the credit card company and canceled the card. I contacted Safeway, explained the situation several times insisting my contact info be removed. I still get their ads. NOTE: I have never ordered groceries online and I do not shop at Safeway.

Disparate impact	As a Special Agent (Retired-DHS) turned Private Investigator for the past 15 years I cannot count how many times I have assisted clients and potential clients on the current activities that Data Brokers are deploying. Data Brokers analyze demographic information, purchasing patterns, and online behavior to identify trends and patterns specifically related to elderly consumers. By examining data points such as age, health-related searches, or interest in retirement planning, they can create profiles that target or (and or) categorize older individuals. In my view, as a layman, I present the following to our elected officials and legal professionals. Consumer segmentation: Data brokers often employ consumer segmentation techniques to group individuals based on similarities in their behavior, preferences, and demographics. They may create segments specifically tailored to elderly consumers, considering factors such as spending habits, healthcare needs, or technology adoption. This very “segmentation” is being used in further big-data marketing strategies, “targeting” products and services for the elderly. Analysis: Data brokers are currently conducting analyses to determine if their data practices and (or) algorithms disproportionately affect elderly consumers. This involves comparing the outcomes or consequences experienced by different age groups to identify potential disparities. For example, if certain marketing campaigns or product recommendations result in significantly different outcomes for elderly individuals compared to younger age groups, it can be argued that a disparate impact exists. Privacy concerns and consent: Data brokers are making their own rules, thus attempting to address the issue of potential disparate impact by highlighting the importance of privacy protections and obtaining informed consent. They often argue that their data collection practices are intended to provide personalized experiences and improve consumer satisfaction for all age groups, including the elderly. By emphasizing the voluntary nature of data sharing and the ability for individuals to opt-out or control their data, they aim to demonstrate that any potential disparate impact is not intentional. In my view, this conduct is unethical and clearly reveals the deceitful conduct being played upon Americans every day. Industry regulations and self-regulatory measures: Data brokers are attempting to emphasize their compliance with relevant regulations and industry self-regulatory measures. For example, they may adhere to guidelines set by data protection authorities or industry associations that aim to prevent discrimination and promote fair practices. By demonstrating their commitment to ethical and responsible data usage, they argue that any disparate impact on elderly consumers is unintentional and mitigated through compliance measures. Self-regulation through their control of the AI is clearly not working, the human side of the equation is being totally neglected. The impacts of data-driven profiling on different consumer groups, including the elderly, should be carefully examined, thus ensuring fair treatment and protection of individual rights. These practices clearly raise concerns about privacy, data ethics, and potential discrimination.