October 21, 2025

Comment Intake
c/o Legal Division Docket Manager
Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552
Submitted via Regulations.gov

Re: Personal Financial Data Rights Reconsideration, 12 CFR Part 1033, (Docket No. CFPB-2025-0037, RIN 3170-AB39)

Consumer Reports (CR) appreciates the opportunity to comment on the Consumer Financial Protection Bureau's Advance Notice of Proposed Rulemaking regarding Personal Financial Data Rights under Section 1033 of the Dodd-Frank Act. As an independent, nonprofit membership organization that has worked for almost 90 years to create a fair and just marketplace for all consumers, we write to urge the CFPB to maintain and strengthen consumer protections in financial data sharing.

Executive Summary

Consumer Reports strongly urges the CFPB to maintain robust consumer protections in any revision to the Personal Financial Data Rights rule. As an independent, nonprofit consumer advocacy organization that has tested financial products and educated millions of Americans about their financial choices for nearly a century, we offer our perspective on how to strengthen consumer protections while addressing implementation challenges. Our comment focuses on three critical areas where consumer protection must be maintained:

1. **No Fees for Data Access:** Fees would create insurmountable barriers for consumers who need data-enabled services most. This is a fundamental equity issue that Consumer Reports has long championed.
2. **Consumer-Protective Privacy and Security Controls:** Consumers deserve strong privacy and security protections without having to give up access to beneficial services. These safeguards are critical and shouldn't be used to limit competition or access to services that improve their financial lives.
3. **Implementation That Prioritizes Consumer Benefit:** Section 1033 was enacted in 2010. Since that time, millions of consumers have used data-sharing services without adequate safeguards. The CFPB should move forward with implementing the rule without excessive delay in a way that prioritizes consumer benefits. Consumers have waited long enough for these protections.

I. **Fees Would Deny Consumers Important Rights -** Prohibit All Fees for Consumer Data Access

Consumer Reports strongly recommends maintaining the rule's fee prohibition. This is the critical consumer protection issue in this rulemaking, and getting it wrong would undermine the entire purpose of Section 1033.

Questions 9-10: The fee prohibition serves Section 1033's consumer empowerment purpose.

Section 1033 creates a right for consumers to access and use their own financial information. The statute provides that consumers "shall" have access to this information "in an electronic form usable by consumers." This language is clear and mandatory. Imposing fees would transform this fundamental right into a service available only to those who can afford it—creating exactly the kind of economic barrier that Congress sought to eliminate.

Charging consumers to access their own data contradicts the basic principle that people should control information about themselves since it is generated by the consumer's own financial activities. Consumer Reports has consistently advocated for this principle across sectors for nearly a century. We fought successfully for free annual credit reports because we understood that consumers needed access to information about themselves to make informed financial decisions and protect against errors. The same logic applies even more forcefully to financial transaction data, which consumers need to manage their finances, compare products, and access beneficial services.

Questions 15-17: Fees would create concrete consumer harms that disproportionately impact families and individuals working to improve their financial situations.

The stakes are enormous for consumers. According to the CFPB, Americans still paid more than $5.8 billion in overdraft and NSF fees in 2023, even after some banks voluntarily reduced fees. Personal financial management tools that access transaction data can help consumers avoid many of these fees through real-time balance alerts and spending tracking. But these tools only work if consumers can afford to use them—and data access fees would price out exactly the consumers who need help most.

Research shows that roughly 9% of accounts pay 79% of all overdraft fees, with these consumers overdrafting more than 10 times annually.[1] For consumers facing frequent overdraft charges, budgeting apps with real-time alerts could provide significant relief—but data access fees would make these protective tools unaffordable. Similarly, the 26 million Americans without credit files[2] could benefit from alternative underwriting that uses transaction data, but fees for data access would make it cost-prohibitive to compare multiple lenders when seeking the best terms.

Section 1033 can help address persistent gaps in financial access—but only if data access remains free. CFPB research shows that households earning less than $65,000 annually bear the majority of overdraft fee burdens[3]—precisely the consumers who most need financial management tools but are least able to afford data access charges.

If implementation costs are a concern, it's worth considering the broader economics of financial services. Data providers and other entities in the financial ecosystem generate revenue through various channels including transaction fees, interest rate spreads, and account-related charges. Financial institutions earn interchange fees on card transactions—the Federal Reserve reports that covered issuers collected substantial interchange revenue in 2021.[4] Banks also generate income from interest rate spreads between deposit and lending rates. Additionally, the banking and financial services sector has increasingly focused on data monetization, with the BFSI (Banking, Financial Services, and Insurance) segment representing over 21% of the global data monetization market in 2023.[5] Financial institutions use customer data for internal purposes including cross-selling, with one study showing that data-driven cross-selling strategies can increase revenue by 25% within six months.[6] Many also derive value from customer data through internal analysis. The question is whether it's appropriate for any party—whether data providers, data aggregators, or other intermediaries—to charge consumers for accessing their own financial information, particularly given that this data originates from the consumer's own financial activities.

---

[1] Consumer Financial Protection Bureau data, cited in Congress.gov, "Congress Repeals CFPB's Overdraft Rule" (2025), Congressional Research Service.

[2] Consumer Financial Protection Bureau, "Data Point: Credit Invisibles" (May 2015)

[3] Consumer Financial Protection Bureau, "Data Point: Overdraft/NSF Fee Reliance Since 2015" (December 2021).

[4] Federal Reserve, "2021 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions" report - documents interchange revenue collected by covered issuers

[5] Grand View Research (2024) - BFSI sector represents 21.1% of global data monetization market in 2023

[6] BAI Banking Strategies (May 2024) - Case study showing 25% increase in cross-sell revenue from data-driven strategies within 6 months

Rather than imposing fees on consumers, implementation costs could be addressed through industry standardization, which reduces expenses for all participants. Bodies like the Financial Data Exchange demonstrate how shared technical approaches lower costs while improving security and reliability. Phased implementation timelines allow entities to spread investments over time. Technical assistance programs can help institutions comply without shifting costs to consumers. The CFPB can also implement reasonable protections against abusive request patterns. These approaches distribute costs more equitably across the ecosystem without creating barriers for consumers who need these services most.

Consumer Reports' evaluation of financial products demonstrates how competition serves consumers when data access is available. When personal financial management tools can access data freely, they compete to provide better features, more accurate insights, and more useful services. This competition drives innovation that benefits consumers. Free data access enables efficient loan comparison services that help consumers find better rates—our research consistently shows that consumers who compare multiple financial product offers achieve significantly better outcomes. When consumers can easily access and move their data, market participants must compete on service quality and fair pricing. Fee barriers would undermine these competitive benefits, ultimately harming consumers through higher costs and reduced service quality.

Consumer Reports recommends prohibiting all fees for consumer data access without exception. Any fee structure—whether labeled "administrative costs," "processing fees," "data access charges," or "service charges"—would undermine Section 1033's consumer empowerment purpose. The principle must be clear: consumers should never pay to access their own financial data.

II. Security Must Protect Consumers, Not Restrict Access - Security Standards Should Enable Consumer Protection

Based on our Fair Digital Finance Framework testing and Digital Standard evaluations, Consumer Reports supports robust security requirements that genuinely protect consumers while ensuring access to beneficial services. Security is essential, but it cannot become a pretext for limiting competition or denying consumers access to services that improve their financial lives.

Question 18: Our product testing reveals what effective consumer security requires—and what it doesn't.

Through our Fair Digital Finance Framework, we have evaluated security practices across peer-to-peer payment apps, Buy Now Pay Later services, banking apps, and digital wallets. This

extensive testing provides clear insights into what genuine consumer security requires. Our testing has revealed concerning gaps in current practices that Section 1033 can help address. When we evaluated peer-to-peer payment apps, we found that 9% of users reported being victims of scams or fraud on these platforms[7]—a rate that demonstrates significant security vulnerabilities in current data-sharing practices that rely on screen scraping and credential sharing. Security features vary dramatically across banking apps, with some institutions providing robust protections while others lag significantly behind. Fraud protection documentation is often incomplete or unclear, leaving consumers confused about their rights and protections. Consumer recourse mechanisms are inconsistent, with some institutions providing clear processes for addressing unauthorized transactions while others create obstacles.

Effective consumer security requires more than just technical measures—it requires transparency that enables consumers to understand and manage their own security. Based on our testing, consumers need clear information about how their data is being protected, what security measures are in place, what to do if security issues arise, and who is responsible when problems occur. This transparency is often lacking in current financial services, leaving consumers in the dark about their protections until something goes wrong.

Strong liability standards drive better security practices—a finding consistent across our years of product evaluation. When entities face clear consequences for security failures, they invest in better protection. For financial data, this means establishing clear responsibility when security failures occur, protecting consumers from unauthorized transactions, prohibiting contractual terms that waive consumer rights, and implementing meaningful penalties that actually deter entities from taking shortcuts with consumer security. Without these liability standards, security remains optional rather than essential.

Practical Security Measures: Consumer Reports' Fair Digital Finance framework has identified security practices that actually protect consumers:

- Encryption in transit and at rest
- Multi-factor authentication options
- Regular security updates
- Transparent incident response procedures
- Clear communication when issues arise

Questions 19-20: Security Costs Should Not Become Consumer Barriers

[7] Consumer Reports, "Peer-to-Peer Payment Services: Findings from CR's Nationally Representative American Experiences Survey" (2022).

Our research across industries shows common approaches reduce costs while improving security. Industry standardization through bodies like the Financial Data Exchange provides secure approaches that:

- Eliminate the need for each entity to create proprietary solutions
- Allow third parties to implement security once
- Create network effects improving security as adoption grows
- Reduce ongoing maintenance costs

Support for Smaller Entities: Consumer Reports recognizes community banks and credit unions face different constraints. Security frameworks should include:

- Phased timelines for smaller institutions
- Technical assistance and shared resources
- Recognition that smaller institutions often serve underserved communities who particularly benefit from data access

Questions 21-22: Security Incentives Should Serve Consumer Protection

Our digital finance product evaluations shows effective security comes from multiple sources.

Regulatory Oversight: Strong, enforced security standards create powerful incentives. Our research shows entities subject to clear requirements and regular auditing maintain better security.

Market Incentives: While consumer trust is essential in financial services and security failures can damage reputation and business viability, market incentives alone are insufficient to protect consumer assets. Without robust regulatory requirements, companies consistently under-invest in security measures that protect consumers from fraud and unauthorized access. Our research across financial products demonstrates that voluntary industry practices leave significant gaps in consumer protection, which is why Section 1033's security mandates are necessary to ensure all consumers receive adequate protection regardless of which institution or service they use. Consumer trust is essential in financial services.

Consumer Empowerment: Consumer transparency and control are important components of a comprehensive security framework, but they cannot substitute for mandatory security standards. While providing consumers with visibility into which entities access their data and the ability to easily revoke access creates valuable accountability, individual consumer action alone cannot address systemic security vulnerabilities or prevent sophisticated attacks. Consumers need both the tools to manage their own data relationships and strong regulatory protections that ensure baseline security practices across all entities. Consumer empowerment tools must

complement—not replace—robust security mandates that protect all consumers, regardless of their technical sophistication or time to actively manage permissions.

Security Framework Based on Consumer Protection
Consumer Reports recommends a security framework grounded in what actually protects consumers rather than what creates barriers to access.

Standardized Requirements Create Consistency: Our evaluations of financial products demonstrates that standardized approaches work better than proprietary solutions. Industry-standard protocols like those developed by the Financial Data Exchange provide secure, consistent approaches that all participants can implement. Regular security assessments using recognized frameworks ensure ongoing protection rather than one-time compliance. Mandatory reporting of security metrics to regulators enables oversight and accountability. Prompt disclosure of serious incidents—particularly those affecting consumers—allows people to protect themselves and holds institutions accountable.

Consumer Transparency Enables Self-Protection: When given the proper tools, consumers can ably manage their security. Clear dashboards showing current data access authorizations help consumers monitor who has their data. Prompt incident notification—consistent with requirements in various state data breach laws that mandate notification without unreasonable delay—enables consumers to respond quickly to potential compromises. Plain language explanations of security practices, rather than technical jargon, help consumers understand their protections. Information about consumer recourse options ensures people know what to do when security fails.

Strong Liability Drives Better Practices: Our product testing consistently shows that entities with clear liability invest more in security. Clear liability standards for security failures mean institutions cannot hide behind vague terms when problems occur. Prohibition on contractual waivers of consumer rights prevents institutions from forcing consumers to give up protections as a condition of service. Meaningful penalties that actually deter shortcuts—not nominal fines that become a cost of doing business—create genuine incentives for strong security. Private rights of action for harmed consumers provide an additional enforcement mechanism beyond regulatory oversight, giving consumers direct recourse when security failures cause them harm.

III. Privacy Through Consumer Control and Transparency - Empower Consumers With Meaningful Control

Based on our extensive privacy advocacy work and Fair Digital Finance testing, Consumer Reports knows that effective privacy protection requires simple, meaningful consumer

control—not complex restrictions that ultimately serve corporate interests over consumer needs. Privacy and data access are not in conflict when systems are designed with consumers in mind.

Question 30: Our product testing and decades of privacy research inform what consumers actually need to protect their privacy while accessing beneficial services.

Through our Fair Digital Finance evaluations, we've documented a disturbing pattern leaving consumers exposed. When we tested banking apps, nearly all overshared data with marketing partners, with only one not sharing personal data by default. Our December 2023 survey found 69% of Americans want to limit how banks share their data[8]—yet current practices make this nearly impossible. The disconnect between what consumers want and what they receive reveals fundamental privacy protection failure.

Our Buy Now Pay Later analysis revealed privacy policies averaging college-level reading difficulty,[9] making it impossible for typical consumers to understand data collection and use. Even consumers wanting informed decisions cannot understand the information presented. Our peer-to-peer payment evaluation documented inadequate disclosure of data monetization and difficult-to-find privacy controls.[10] These findings demonstrate current privacy practices systematically fail consumers.

Consumer data should be protected by default, but at the very least they need clear information about which entities accessed their data, transparency about data use after sharing, notification of secondary uses beyond original authorization, and simple explanations in plain language people can understand. The current system fails on every dimension.

Ongoing Control: Our testing shows consumers want easy ways to manage data relationships over time:

- Simple processes to modify permissions
- Easy revocation without service penalties
- Granular control over different data types and uses
- No complex procedures requiring extensive time

Accountability: Our decades of advocacy show rights are meaningless without enforcement:

- Clear disclosure of commercial data uses

[8] Consumer Reports, "Banking Apps: 2023 Nationally Representative Survey" (2023).
[9] Consumer Reports, "Buy Now, Pay Later: A Case Study for a Digital Finance Standard" (2023).
[10] Consumer Reports, "Peer-to-Peer Payment Apps: A Case Study for a Digital Finance Standard" (2023).

- Restrictions on exploitative practices
- Enforcement with real penalties
- Transparency about company compliance

Questions 31-33: Our Testing Reveals Concerning Industry Practices

Our Fair Digital Finance evaluations documented:

- Vague privacy policies that don't clearly explain data monetization
- Buried terms in lengthy documents few consumers can understand
- Difficult-to-find opt-out mechanisms
- Automatic consent through unclear terms of service

Consumer Reports Recommends:

Balanced Consumer Control Over Secondary Uses: Consumer Reports recommends a balanced approach that protects consumers from exploitative data practices while allowing beneficial uses that improve services. The key is distinguishing between uses that serve consumers versus those that primarily extract value from consumer data.

Prohibited Data Practices: The sale of Section 1033 consumer financial data to data brokers, marketing firms, or other third-party entities for commercial purposes unrelated to the service the consumer requested should be prohibited entirely. This practice commodifies consumer data without providing any direct benefit to consumers.

Permitted Internal Uses Without Opt-In: Financial institutions and authorized data recipients (the services consumers choose to use) should be able to use consumer data for legitimate operational purposes without requiring separate opt-in consent:

- Product improvement and service enhancement that directly benefits users
- Internal analytics to improve service quality and user experience
- Fraud prevention and security monitoring
- Compliance with legal obligations
- Research and development using de-identified or aggregate data

These internal operational uses should be subject to strict data minimization principles. Entities should document why identifiable consumer data is necessary for these purposes rather than

de-identified or aggregate data, and should use the least identifiable form of data that accomplishes the legitimate purpose.

Requiring Opt-In Consent: Separate, specific consumer consent should be required for:

- Any data sharing with entities other than the financial institution or the authorized data recipient
- Uses that generate direct revenue from consumer data (such as selling insights or marketing access)
- Sharing with affiliates or partners for their own commercial purposes
- Marketing or targeted advertising to the consumer, even by the primary service provider
- Training AI models or algorithms that will be used in products or services beyond what the consumer requested
- Any use that significantly changes the nature or scope of originally authorized data access

Clarification on "Third Parties": The CFPB's rule uses 'authorized third party' to describe entities like budgeting apps that consumers choose to access their data. From the consumer's perspective, these are 'first parties' providing a requested service. When we refer to 'third parties' in this letter, we mean entities beyond this consumer-authorized service—such as data brokers, marketing firms, or affiliates that the consumer did not directly choose.

Question 34: Consumer Research on Privacy Policy Failure. Research consistently shows few consumers read privacy policies, and even fewer understand them. According to Pew Research, only 9% of Americans always read privacy policies.[11]

The problem isn't consumer apathy—reading every privacy policy would take hundreds of hours annually. And even when consumers try, most policies are written at college level with vague language that doesn't provide meaningful information.

Solutions Based on Consumer Reports' Work

1. Standardized, Simplified Consent:

Following CFPB's model forms for mortgages and credit cards, we need standardized data sharing consent:

- Maximum 8th grade reading level
- Required plain language tested with consumers

[11] Pew Research Center, privacy policy research (2023)

- Standardized format for key information
- Visual design highlighting important terms
- Prohibition on burying important terms

2. Just-in-Time Consent:

Rather than requesting everything up front, use contextual consent:

- Initial authorization for core service
- Separate requests for different data types or uses
- Context-specific explanations at decision point
- Clear notices when practices change

For example: A budgeting app first requests transaction data for budgeting purposes. Later, if it wants to use data for product recommendations, it asks specifically with clear explanation.

3. Consumer Education:

Based on our 90 years of consumer education:

- Plain-language guides explaining data rights
- Public education about privacy and control
- Resources to exercise rights effectively
- Tools making rights actionable

4. Plain English Requirements:

All consumer-facing disclosures should:

- Use plain, simple language
- Avoid legal jargon and technical terms
- Be tested with consumers for comprehension
- Include illustrative examples
- Be available in languages serving significant populations

Consumer-Beneficial Secondary Uses: A Balanced Approach

Consumer Reports recognizes that some data uses beyond immediate service delivery can benefit consumers when properly safeguarded. The final rule's prohibition on secondary uses for targeted advertising, cross-selling, and data sales appropriately protects consumers from exploitation. However, there are limited circumstances where secondary uses can serve consumer interests without compromising their privacy or control.

1. **Permitted Secondary Uses.**

Who can use data: Financial institutions and authorized data recipients—the services consumers choose to use—should be able to use consumer data to improve their services when properly safeguarded. These are improvements to the services the consumer selected, not uses by unrelated third parties or marketing partners.

Requirements for permissible service improvement uses:

- **Direct Consumer Benefit:** Improvements must directly benefit consumers using the service, not merely increase company profits or efficiency
- **Data Minimization:** Entities must document why identifiable personal data is necessary for the improvement, rather than de-identified or aggregate consumer data. Where possible, improvements should be developed using de-identified data.
- **Ongoing Consumer Control:** Consumers maintain the ability to opt out of having their data used for service improvements without penalty or reduction in service quality
- **Strict Limitations:** Use must be limited to the entity providing the service, with no sharing with affiliates, partners, or other companies
- **Transparency:** Regular reporting to regulators demonstrates how data contributed to meaningful consumer benefits, with summary information available to consumers

Examples of permissible uses:

- A budgeting app using transaction patterns to improve categorization accuracy for its users
- A lending platform analyzing repayment data to refine credit models that benefit applicants
- A financial planning tool using anonymized user behavior to enhance interface design

Prohibited uses:

- Sharing improvement insights with affiliated companies for their own services

- Using consumer data to develop products the consumer didn't request
- Combining Section 1033 data with other data sources for marketing purposes
- Training AI models for use in unrelated products or services

2. **Research Promoting Financial Inclusion and Consumer Protection:**

Consumer Reports has long supported research using consumer data to inform policy and improve consumer outcomes. As a research-driven consumer advocacy organization, we understand the value of data analysis for:

- Understanding financial challenges facing consumers
- Evaluating product effectiveness and identifying consumer harms
- Informing policy recommendations that serve consumer interests
- Advancing financial access for Americans who have been underserved by traditional banking

Required safeguards for research uses:

- Proper de-identification using established standards that prevent re-identification
- Research serving clear public interest or consumer benefit purposes
- Published results made available to inform policy and consumer protection efforts
- Strong protections for all consumers, including those most at risk of exploitation
- Robust oversight ensuring compliance with de-identification standards

Required Consumer Controls for Secondary Uses

Beyond permitted internal operational uses (fraud prevention, security monitoring, and legally required activities), consumers need meaningful control over how their data is used.

For non-operational secondary uses, entities must provide:

- **Clear, separate disclosure** explaining the specific secondary use in plain language
- **Ongoing ability to revoke consent** without affecting primary service access or quality
- **Regular reporting to consumers** about secondary use activities, including what data was used and for what purposes
- **Strict prohibition** on conditioning primary service access on consent to secondary uses

Important Exception: Security and Fraud Prevention
Certain critical security functions should not require opt-in or allow opt-out:

- Fraud detection and prevention
- Security monitoring and threat detection
- Compliance with legal obligations
- Protecting the integrity of the financial system

These uses protect all consumers and the broader financial ecosystem, making opt-out inappropriate. However, they should still be subject to data minimization principles and transparency requirements.

Universal Data Minimization Requirement

For all secondary uses, entities must prioritize using de-identified or aggregate data wherever possible. Use of identifiable personal information requires documented justification showing why de-identified data is insufficient for the stated purpose.

Need for Additional CFPB Guidance
Consumer Reports recommends that the CFPB provide clearer guidance on secondary use boundaries, particularly regarding:

- Standards for proper de-identification in research contexts
- Scope of "reasonably necessary" product improvements
- Safeguards for AI/algorithm training using covered data
- Consumer notification requirements for secondary uses

IV. Implementation Must Balance Needs With Consumer Protection - Expeditious Implementation With Appropriate Support

Questions 35-36: Implementation should proceed without indefinite delays while providing appropriate assistance.

Consumers Need Protections Now
Section 1033 was enacted in 2010—fifteen years ago. During this period, millions of consumers have used data-sharing services without adequate protections. The risks are well-documented: screen scraping creates security vulnerabilities, unclear authorization procedures confuse

consumers, inconsistent privacy protections leave consumers exposed, and variable security standards create risks.

Research shows real-world impact of delays. The 26 million credit-invisible Americans[12] could benefit from alternative data underwriting—each month of delay means continued credit exclusion. Consumers paid over $5.8 billion in overdraft fees in 2023.[13] Personal financial management tools could help many avoid these fees, but without Section 1033 protections, consumers rely on risky screen scraping. Without implementation, existing market structures may limit competition and reduce consumer choice in financial services.

Implementation Priorities Serving Consumers

If timeline extensions are necessary, structure them to prioritize consumer benefit:

1. Consumer Education and Awareness: Any implementation period should include robust consumer education:

- Public awareness campaigns about data rights
- Plain-language guides for exercising rights
- Resources showing available services
- Targeted outreach to underserved communities

Consumer Reports stands ready to support education through our publications, website, and consumer-facing resources.

2. Phased Rollouts Based on Consumer Impact: If phased implementation is necessary, prioritize based on consumer benefit including largest institutions first (serving the most consumers), products with highest consumer demand, services where screen-scraping alternatives are most risky, and institutions serving communities with limited banking options.

Consider consumer impact, not just institution size, when setting priorities.

3. Technical Assistance: Support smaller institutions through assistance:

---

[12] Consumer Financial Protection Bureau, "Data Point: Credit Invisibles" (May 2015)
[13] Consumer Financial Protection Bureau, "CFPB Closes Overdraft Loophole to Save Americans Billions in Fees" (December 2024), available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-closes-overdraft-loophole-to-save-americans-billions-in-fees/

- CFPB coordination of technical resources
- Industry standards bodies (like FDX) providing support
- Shared infrastructure for smaller institutions
- Phased requirements giving smaller entities more time while larger ones proceed

4. Clear Enforcement: Even during implementation, enforcement should be consistent:

- No tolerance for bad actors exploiting delays
- Clear standards so compliant entities aren't disadvantaged
- Consumer complaint processes operating immediately
- Consequences for entities missing deadlines without cause

VI. Conclusion: Protect and Strengthen Consumer Rights

Consumer Reports urges the CFPB to strengthen, not weaken, consumer data rights. This reconsideration should enhance consumer protections while addressing legitimate implementation concerns through technical assistance and reasonable timelines—not by undermining fundamental consumer rights.

Key Recommendations:

1. **Maintain Fee Prohibition:** This is the critical consumer protection issue. Fees would create insurmountable barriers for consumers who need data-enabled services most—including working families trying to avoid overdraft fees, young adults building credit histories, and small businesses seeking capital. Data providers and other entities in the financial ecosystem already generate revenue through multiple channels; implementation costs should be addressed through industry standardization, phased timelines, and technical assistance rather than charging consumers for accessing their own data.

2. **Implement Consumer-Protective Security:** Our product testing shows effective security requires standardized requirements, clear liability, and transparency—backed by strong regulatory mandates. While market incentives and consumer tools play important roles, they cannot substitute for mandatory security standards that protect all consumers, regardless of which institution or service they use.

3. **Enable Access While Protecting Privacy Through Balanced Controls:** Based on our Fair Digital Finance testing and privacy research, consumers need simple, meaningful

control through clear dashboards, easy permission management, and transparent reporting. We support a balanced approach: prohibiting data sales to third parties, allowing reasonable internal uses like product improvements with strong data minimization requirements, and requiring opt-in consent for marketing and external data sharing. Critical security functions like fraud prevention should proceed without opt-out while maintaining transparency.

4. **Support Expeditious Implementation:** Section 1033 was enacted fifteen years ago in 2010. Millions of consumers already use data-sharing services without adequate protections. Address implementation challenges through technical assistance and coordination while ensuring consumers can access beneficial services without unnecessary delays. Consumers have waited long enough.

The CFPB can strengthen consumer financial data rights while addressing implementation challenges. Consumer Reports stands ready to assist through our product testing expertise and consumer advocacy experience.

Respectfully submitted,

Delicia Reynolds Hand
Senior Director, Digital Marketplace
Consumer Reports