SPPI
Southwest Public Policy Institute

NO. 8 | NOVEMBER 2025

THE CENTER FOR ECONOMIC OPPORTUNITY

1033 Error: Rule Not Sound

The CFPB's Open-Banking Mandate Endangers Consumers

Patrick M. Brenner & Lucas J. Parker

"Nobody spends somebody else's money as carefully as he spends his own."

— Milton Friedman

This paper, in its entirety, can be found at **https://southwestpolicy.com/sppi08**

505.386.1139 | southwestpolicy.com | info@southwestpolicy.com
PO Box 1746 | Bernalillo, New Mexico 87004

Southwest Public Policy Institute | *Better living through better policy*

SOUTHWEST PUBLIC POLICY INSTITUTE

The Southwest Public Policy Institute (SPPI) is an independent research organization committed to strengthening America's economic and civic foundations through data-driven, people-focused analysis. Our work centers on expanding financial inclusivity, defending consumer choice, exposing regulatory overreach, and advancing practical solutions that improve daily life for families, workers, and small businesses.

Unlike traditional think tanks that rely on theory, SPPI operates as a consumer-first "do-tank." We replicate real-world experiences—applying for credit, navigating government programs, interacting with financial services, or requesting public records—to reveal how policies actually function outside the political narrative. This method uncovers the unintended consequences of well-meaning regulations, highlights barriers facing underserved communities, and grounds our recommendations in lived experience rather than ideology.

SPPI's research spans the nation but is anchored in the belief that economic freedom, transparency, and accountability are essential to human flourishing. By engaging diverse audiences—micro-targeting constituents on the issues that matter most—we meet people where they are. We build common ground through respectful dialogue, empirical evidence, and a commitment to practical problem-solving over partisanship.

Through rigorous analysis, investigative research, and innovative policy design, SPPI champions reforms that empower individuals, expand entrepreneurship, and restore trust in public institutions. Guided by a simple principle—**We Agree**—we work to deliver what public service should: ***Better living through better policy.***

1033.0 EXECUTIVE SUMMARY

The Consumer Financial Protection Bureau (CFPB) is revisiting the Personal Financial Data Rights (PFDR) rule under Section 1033 of the Dodd-Frank Act. The previous rule, finalized by CFPB Director Rohit Chopra in 2024, sought to mandate an "open banking" regime that exceeded statutory authority, imposed back-door price controls, created asymmetric liability, and introduced significant cybersecurity and national security risks.

A federal court froze the rule's compliance deadlines in 2025, citing significant concerns over the CFPB's interpretation of "consumer," the cumulative effects of the rule on data security, and the arbitrary nature of compliance timelines relative to industry standards. As the CFPB initiates a new rulemaking under the Trump Administration, stakeholders warn that reproducing Chopra's mandates—especially those imposing price controls and obligating costly application programming interfaces (API) development without the ability to receive compensation for these investments—would destabilize a market that has functioned effectively through voluntary, bilateral agreements.

There should be no rulemaking unless it strengthens market-based innovation, eliminates screen scraping altogether, secures liability symmetry, and resists price controls that distort competition and subsidize intermediaries.

SPPI advances five core principles for a lawful, sustainable, pro-innovation Section 1033 framework:

- **No price controls.** Data access fees must be governed by free-market contracts—not government mandates.
- **End screen scraping only when liability is symmetrical.** Aggregators must be treated as covered persons.
- **No exemptions for small banks.** A uniform rule or no rule at all.
- **Full liability for data aggregators.** Entities that store, use, or monetize consumer data must be accountable.
- **Avoid unnecessary regulation.** The market already works, and voluntary

standards continue to evolve.

1033.1 SYSTEM INITIALIZATION FAILURE

Section 1033 of the Dodd-Frank Act (2010) establishes that a covered person must make available to the consumer "information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained." Congress intended to codify the principle that consumers should be able to obtain information about their own accounts, not to mandate an "open banking" regime in which banks must transfer data to third-party technology firms.

Importantly:

- The statute does not reference APIs.
- The statute does not authorize or mention data aggregators.
- The statute does not require data sharing with third-party commercial entities.
- The statute does not impose any obligation on financial institutions to share data without compensation.
- The statute does not create a framework for "open banking" or "data portability."

Congress knew how to legislate open banking—after all, it watched the European Union and the United Kingdom do so explicitly through comprehensive statutes and regulatory frameworks. But Congress made no such choice in the United States, deliberately declining to mandate an open-banking regime in Dodd-Frank.

1033.2 INVALID PARAMETER

Before any discussion of Section 1033 can begin, it is essential to recognize that the primary federal law governing privacy and data security for financial institutions is the Gramm-Leach-Bliley Act (GLBA). GLBA establishes the foundation for how financial institutions must handle consumer information. It requires institutions to explain their data-sharing practices to customers, provide opt-out rights for certain types of third-party sharing, and safeguard sensitive consumer information through robust administrative, technical, and physical protections. GLBA also mandates that every covered institution maintain an information security program consistent with the Federal Trade Commission's Safeguards Rule, which sets detailed expectations for risk assessments, oversight, and ongoing monitoring.

Against this backdrop, Chopra's rule sought to impose an entirely separate, and, in many cases, conflicting, regulatory framework. It would have required banks to remain responsible for consumer data even after it left their control, mandated the sharing of sensitive financial information without allowing for reasonable cost recovery, and created no meaningful standards or certification requirements for third parties that receive that data.

Equally problematic, the rule imposed significant obligations on banks while declining to apply equivalent cybersecurity or accountability requirements to data aggregators. This produced a fundamentally asymmetric system that distorted market incentives and undermined the purposes of GLBA. Banks would be exposed to heightened legal and financial risks, while aggregators, many of which face far fewer regulatory constraints, would continue to operate with minimal oversight.

1033.3 AUTO-RESOLVE

The U.S. financial data-sharing ecosystem has developed organically through voluntary, privately negotiated agreements—not through federal regulation. Banks, data aggregators, and fintech firms have spent years building secure, reliable channels for consumer-authorized data access without government mandates. This market-driven evolution has produced a robust and widely adopted infrastructure for financial data portability.

Today, more than 200 million bank accounts connect through Plaid alone, while standardized APIs developed by the Financial Data Exchange (FDX) reach another 94 million accounts. More than 120 data aggregators now operate across the U.S. financial sector. As a result of these private contractual arrangements, screen scraping—an inherently insecure practice—has already declined significantly as API adoption has expanded.

Crucially, this entire ecosystem emerged without federal rulemaking. It avoided the pitfalls experienced in jurisdictions that imposed government-designed open-banking mandates, such as the European Union and the United Kingdom. The U.S. model has effectively balanced consumer access with fraud prevention and maintained healthy competition between banks and fintech innovators.

The only notable gap in this system lies among smaller banks that may lack the

resources to negotiate or implement APIs. This is a localized challenge, and it certainly does not justify sweeping regulatory intervention that would disrupt an ecosystem already functioning efficiently.

1033.4 VOLUNTARY COMPARATOR

Swipe Right provides one of the clearest empirical demonstrations that consumer-permissioned data sharing improves market performance without requiring government mandates or centralized technical standards. The report examines how lead generators, comparison-shopping platforms, and financial marketplaces help consumers evaluate loan options, compare total costs, and find the best product for their needs. These intermediaries like NerdWallet, Credit Karma, and Lending Tree exist entirely because consumers voluntarily choose to share their data to obtain better financial outcomes.

Market actors already match consumers to products more efficiently than any government-designed structure could. Lead generators specialize in lowering search costs, aggregating offers, and increasing transparency—functions that Section 1033 does not need to replicate and that the PFDR rule would likely undermine.

Restricting or imposing price controls on data flows destroys the value of comparison shopping. If regulators limit or eliminate the ability of intermediaries to receive or transmit consumer-permissioned data, the direct result is fewer choices, less transparency, and higher borrowing costs. These outcomes contradict the CFPB's stated goals and reveal the risk inherent in any attempt to centrally redesign financial data markets.

Lead generators and marketplaces rely on contractual data access arrangements that balance innovation with consumer protection. Under the Chopra rule, however, banks would be heavily regulated while aggregators and comparison platforms would face fewer obligations, even though these entities handle large volumes of sensitive financial information. There are risks to such imbalances, demonstrating the need for a uniform regulatory framework that applies equally to all entities accessing consumer data.

The financial data ecosystem works best when driven by voluntary market forces rather than top-down directives. Comparison-shopping tools thrive because they respond to consumer demand, not regulatory mandates. The PFDR rule

would have jeopardized these systems by introducing cost controls, mandatory API development, and liability asymmetry. In contrast, a free-market approach preserves innovation, encourages competition, and strengthens consumer protections.

1033.5 PERMISSION DENIED LOPER BRIGHT

In 2024, the Supreme Court's decision in *Loper Bright v. Raimondo* eliminated Chevron deference, a doctrine that, for decades, allowed federal agencies to interpret ambiguous statutes with substantial deference from the courts. With Chevron overturned, agencies can no longer stretch statutory language to fill perceived gaps or pursue expansive regulatory agendas based on broad readings of congressional intent.

Under the post–*Loper Bright* framework, agencies must rely strictly on the plain and unambiguous text of a statute. Courts are no longer required to accept an agency's "reasonable" interpretation of ambiguous language. Instead, the judiciary now independently assesses statutory meaning, ensuring that regulatory actions remain tethered to clearly expressed congressional mandates. The Court also reaffirmed that major policy decisions must rest on explicit and unmistakable congressional authorization under the Major Questions Doctrine.

Section 1033 of the Dodd-Frank Act contains no such authorization. The statute does not empower the CFPB to regulate data aggregators, mandate API development, prohibit fees for data access, create an open-banking regime, impose industry-wide technical standards, or design a comprehensive data-portability framework connecting consumers to fintech applications. Each of these components represents a significant policy expansion far beyond the statutory text.

Viewed through the lens of *Loper Bright* and the Major Questions Doctrine, the Chopra rule ventured into a realm of policymaking that Congress neither contemplated nor sanctioned.

1033.6 PROCESS CORRUPTED

Between 2022 and 2024, Director Chopra advanced an expansive reinterpretation of Section 1033, positioning it not as a consumer-access provision—as Congress originally intended—but as a mandate for a nationwide "open banking" system. Throughout this period, the CFPB framed the rule as transformative infrastructure

for consumer data portability, even though Dodd-Frank includes no explicit authority to establish such a regime. The CFPB's public statements, advisory materials, and draft rulemaking documents consistently revealed an ambitious effort to reshape the financial data ecosystem through administrative action rather than congressional mandate.

This effort culminated in October 2024, when the CFPB finalized the PFDR Rule. The rule required financial institutions to build and maintain API-based data portals, prohibited the recovery of costs associated with data sharing, mandated broad data-access rights for a wide array of third-party firms, and created an entirely new regulatory class of "authorized third parties." Notably, many of these entities operate outside the scope of existing federal privacy and cybersecurity frameworks, yet the rule granted them data-access privileges without imposing comparable regulatory obligations.

In 2025, banks, credit unions, data providers, and industry trade associations challenged the rule in federal court. A U.S. district court granted a preliminary injunction after determining that the plaintiffs were likely to succeed on several core claims. First, the court found substantial evidence that the CFPB had misinterpreted the term "consumer" by extending it far beyond the statutory definition. Second, the Bureau had failed to meaningfully assess the cumulative impacts of the rule on data security—an omission made more significant given the rising prevalence of financial fraud and cyber risk. Third, the court determined that the compliance deadlines were arbitrary and capricious because they did not account for the absence of industry standards necessary for implementation. Finally, the court concluded that the rule likely exceeded the CFPB's statutory authority under Section 1033.

As a result, the court stayed the compliance deadlines indefinitely while the CFPB reevaluates the rule. This stay remains in effect while the CFPB undertakes reconsideration under the new administration.

1033.6.1 AUTHORITY OVERFLOW

The Chopra rule exceeded the CFPB's statutory authority in numerous fundamental ways. First, the rule invented an entirely new regulatory category: "authorized third parties." This new class of entities has never appeared before. The statute contemplates consumers and covered financial institutions, not technology firms, data aggregators, app developers, or digital wallets. Yet the rule granted such

third parties expansive rights while applying few corresponding obligations.

Second, the rule imposed a de facto price control by prohibiting financial institutions from charging reasonable fees for providing API access or responding to data-access requests. Nothing authorizes the CFPB to mandate that banks provide services for free. As ATR and NTU emphasize, price controls distort markets, reduce innovation, and effectively require banks—and ultimately consumers—to subsidize the business models of data aggregators.

Third, the rule attempted to override the established federal privacy and security framework under the GLBA. GLBA already governs data protection, information sharing, opt-out rights, and security protocols for financial institutions. Instead of reinforcing that statutory framework, the Chopra rule sought to create a parallel regulatory structure that imposed complex data-management duties on consumers and banks while exempting aggregators from comparable responsibilities. As Ron Shevlin observed, this would place unrealistic and unmanageable burdens on consumers, who are already ill-equipped to navigate the complexities of data privacy, consent tracking, and cybersecurity.

Fourth, the rule ignored the broader context of escalating fraud risk and cybersecurity threats. Data breaches reached record levels in 2023 and 2024, and Reuters reporting shows that platforms like Meta display up to 15 billion scam ads per day—many linked to financial fraud. Aggregators routinely monetize consumer data, and identity-theft losses continue to rise. Despite these realities, the rule required banks to dramatically increase data flows to third parties without adequate safeguards.

Finally, the rule imposed extensive liability on banks while allowing data aggregators to operate with minimal oversight. GLBA applies strict obligations to banks and credit unions, but most aggregators fall outside its scope. Under the Chopra rule, banks would be held accountable for security failures even after data was transferred to unregulated entities—while those entities faced fewer obligations and almost no federal supervision. This asymmetry is both legally unsound and economically indefensible.

1033.7 NARROW SCOPE REQUIRED

Section 1033 is a consumer-access provision, not a blank check authorizing the creation of a national open-banking system. Any rule implementing Section 1033

must remain firmly grounded in the statutory text, the established GLBA privacy and security framework, and the constitutional limits articulated in *Loper Bright* and the Major Questions Doctrine.

The CFPB must recognize the market realities: the financial data-sharing ecosystem already functions effectively through voluntary contracts, bilateral agreements, and industry-driven standards. Regulations that disrupt this balance risk undermining innovation, weakening cybersecurity, and exposing consumers to new and unnecessary risks.

A lawful rule must reinforce consumer safety, respect statutory boundaries, and avoid imposing obligations Congress did not authorize. Any attempt to restructure the U.S. financial data ecosystem or mandate open banking through regulatory fiat belongs to Congress, not to the CFPB.

1033.8 SECURITY EXCEPTION RAISED

A growing body of evidence demonstrates that the most significant risks to consumer financial data come not from regulated banks and credit unions, but from large technology firms and digital platforms operating outside the traditional financial regulatory framework. The recent Reuters investigative report on Meta, parent company of Facebook, Instagram, and WhatsApp, provides one of the most striking illustrations of this threat. According to internal Meta documents reviewed by Reuters, the company's platforms display an astonishing 15 billion scam advertisements every day, many of which impersonate well-known brands, government agencies, or financial institutions. Even more disturbing, Meta internally projected that up to 10% of its total 2024 revenue, roughly $16 billion, would be derived from ads associated with scams or prohibited goods.

The Reuters report also revealed that Meta allows known or suspected scammers to continue advertising so long as the platform's automated systems are less than 95% certain the advertiser is engaged in fraud. In practice, this means vast numbers of high-risk accounts continue to purchase ad placements, even after being flagged by Meta's own internal systems. Additionally, Meta reportedly ignores or incorrectly rejects up to 96% of valid scam reports submitted by users, allowing fraudulent content to spread unchecked across its networks.

The consequences of this lax oversight are profound. Meta's internal research, according to Reuters, concluded that its platforms are involved in one-third of

all successful scams in the United States, making the company one of the single largest vectors for fraud in the modern economy. While banks invest billions annually in cybersecurity and are subject to rigorous oversight under GLBA, the Safeguards Rule, and prudential regulation, large technology companies face few comparable requirements, despite functioning as major gateways through which financial scams proliferate.

Taken together, these findings underscore two critical realities. First, the most serious threats to consumer data security come from unregulated digital intermediaries and data-driven platforms, not from the highly regulated banking sector. Second, any serious regulatory framework for financial data access must impose meaningful liability, enforceable standards, and robust oversight on data aggregators, technology firms, and social-media platforms that store, process, monetize, or disseminate consumer financial information.

In short, the policy debate surrounding Section 1033 must account for the fact that Big Tech platforms, not banks, represent the true weak link in the financial data ecosystem. Until these entities are held to the same standards of accountability, security, and consumer protection as banks, consumers will remain exposed to the very risks that 1033 rulemaking purports to address.

1033.9 STABLE RELEASE

Any rule implementing Section 1033 must reinforce market-driven innovation rather than replace it, respect statutory limits rather than exceed them, and enhance consumer security. To achieve these goals, SPPI advances a principles-based framework grounded in free-market incentives, liability parity, and uniform standards across the data ecosystem.

A foundational requirement of any 1033 rule is the preservation of market pricing for data access. Government-imposed bans or caps on fees constitute price controls, and as the experience with interchange caps demonstrates, such interventions distort markets, suppress investment, and ultimately harm consumers. Banks must be permitted to recover the costs associated with secure data transmission; otherwise, the rule effectively forces them to subsidize data aggregators whose business models depend on monetizing consumer information. Accordingly, Section 1033 implementation should make clear that pricing for data-sharing services should be determined through bilateral contracts, not regulatory fiat.

Another essential principle concerns the long-standing practice of screen scraping. Although screen scraping is insecure and technologically outdated, simply banning it without imposing equivalent obligations on aggregators would exacerbate cybersecurity risks. Banks cannot be compelled to provide sensitive financial data through APIs while aggregators operate without comparable regulatory responsibilities. The elimination of screen scraping is appropriate only in a framework where aggregators assume full liability, comply with uniform security standards, undergo certification or auditing, and adhere to strict retention and revocation requirements.

The notion that small or community banks should be exempt from Section 1033 obligations should be rejected. Exemptions would create a fractured regulatory environment in which screen scraping persists wherever APIs are not mandated, thereby exposing consumers to unnecessary risk. Uniformity is essential: if a 1033 rule is adopted, it must apply to all financial institutions to prevent inconsistent practices, competitive distortions, and security vulnerabilities.

In addition, data aggregators must be treated as covered persons under any Section 1033 rule. If banks are required to share sensitive financial data, aggregators must be held to equivalent standards of data security, oversight, liability, and consumer protection. Today, aggregators often operate outside the scope of GLBA and other federal privacy regimes despite handling vast amounts of consumer financial information. A fair and effective rule must ensure that every entity receiving, storing, or transmitting consumer data is subject to the same regulatory expectations and consequences for misuse or breach.

Finally, the importance of avoiding redundant regulation is paramount. The existing financial data-sharing market already functions effectively through voluntary bilateral agreements that promote innovation, maintain consumer access, and reduce fraud. A Section 1033 rule should not replace these private arrangements or impose a government-designed open-banking structure. Instead, the CFPB should adopt a modest approach that reinforces what is already working, respects statutory boundaries, and avoids unnecessary mandates.

Taken together, these principles lead to a recommendation of a specific policy direction. First, bilateral contracts should remain the foundation of the data-sharing ecosystem, and the CFPB should avoid mandating top-down technical standards or infrastructure requirements. Second, markets must be allowed to set prices for data access, ensuring that costs are not unfairly shifted to consumers or

financial institutions. Third, the rule must impose liability parity across all entities that handle consumer data, acknowledging that banks cannot bear exclusive responsibility for risks created by third-party aggregators. Fourth, any regulatory framework must apply uniformly across institutions of all sizes to prevent security gaps. And fifth, the CFPB should refrain from imposing open-banking mandates that Congress has not authorized, particularly those modeled on the European or U.K. regimes.

A lawful and effective Section 1033 rule must strengthen markets, not override them; enhance security, not expose consumers to new risks; and stay within statutory boundaries rather than attempting to engineer a sweeping restructuring of the U.S. financial data ecosystem. Any rule inconsistent with these principles is both economically unsound and legally indefensible.

1033.10 SYSTEM EXIT

The United States already possesses a highly functional, market-driven financial data ecosystem. For over a decade, banks, credit unions, data aggregators, and fintech firms have successfully developed bilateral agreements, interoperable APIs, and voluntary technical standards that enable secure consumer-permissioned data sharing. This ecosystem, unlike the mandated European open-banking regimes, evolved organically, minimized fraud, preserved privacy, and enabled world-leading financial innovation without federal intervention. The Chopra 1033 rule attempted to upend this progress by imposing a sweeping, unauthorized, and economically distortive regulatory framework that ignored statutory constraints, contradicted GLBA, and shifted systemic risk onto the very institutions most accountable to consumers.

The rule's core flaws were structural. It attempted to redesign the financial data-sharing market from the top down, mandated APIs without statutory authority, prohibited cost recovery, created new regulatory categories that Congress never enacted, and required banks to share sensitive data with unregulated third parties. These measures weakened cybersecurity protections, contradicted established federal privacy law, and exposed consumers to heightened risks at a time of record-breaking fraud and data breaches. By effectively subsidizing data aggregators, many of which monetize consumer data, the rule undermined incentives for secure system design and forced banks and credit unions to bear asymmetric liability for risks they do not create.

Going forward, the CFPB should adopt a restrained, lawful approach that aligns with the text of Section 1033, the limits imposed by *Loper Bright*, and the realities of the modern fraud environment. Regulation should complement the private contractual arrangements that already govern the financial data ecosystem. A properly structured rule must preserve market pricing for data access, impose liability parity across all entities that touch consumer data, eliminate insecure screen scraping in a responsible manner, and treat data aggregators as covered persons subject to GLBA-equivalent obligations.

Most importantly, the CFPB must avoid replicating the European-style open banking model without congressional authorization. Section 1033 is a consumer-access statute, not a mandate to redesign the U.S. financial system. Any rule that seeks to engineer an industry-wide transformation belongs to Congress, not the CFPB.

The Southwest Public Policy Institute strongly urges the CFPB to embrace a market-based, innovation-preserving approach rooted in statutory fidelity, cybersecurity rigor, and economic evidence. By aligning regulation with the model that is already working, the CFPB can enhance consumer choice, promote competition, and strengthen data security without sacrificing the free-market dynamism that has made the United States the global leader in financial technology.

1033.11 PATCH NOTES

1. Achten, Alex. *Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase over Previous High*, Identity Theft Resource Center, 25 Jan. 2024, www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/.
2. Aiello, Thomas. *Smart Approach to Financial Data Regulation Will Protect Consumers, Innovation*, National Taxpayers Union, 20 Oct. 2025, www.ntu.org/publications/detail/smart-approach-to-financial-data-regulation-will-protect-consumers-innovation.
3. Baer, Greg. "The CFPB's 'open Banking' Rule Is a Solution in Search of a Problem." *American Banker*, Arizent, 20 Nov. 2024, www.americanbanker.com/opinion/the-cfpbs-open-banking-rule-is-a-solution-in-search-of-a-problem.
4. Berlau, John. "Personal Financial Data Rights Rule Reconsideration." Received by Russell Vought, Competitive Enterprise Institute, 21 Oct. 2025, https://cei.org/wp-content/uploads/2025/10/CEI-comments-on-cfpb-1033.pdf. Accessed 20 Nov. 2025.
5. Brenner, Patrick M., and K. Liam Gray. "Scotus Decision Offers Americans Unrealized Gains." *Newsmax*, Newsmax Media, Inc., 4 Nov. 2024, www.newsmax.com/finance/streettalk/supreme-court-executive-action/2024/11/04/id/1186589/.
6. Brenner, Patrick M., et al. ResearchGate, 2025, *Swipe Right*, https://dx.doi.org/10.13140/RG.2.2.35869.01761. Accessed 20 Nov. 2025.
7. Caruso, Jay. "Products Such as Credit Karma and Nerdwallet Benefit Consumers, Do Not Harm Them: Report." *Fox Business*, FOX News Network, 10 May 2025, www.foxbusiness.com/economy/products-credit-karma-nerdwallet-benefit-consumers-not-harm-them-report.
8. Coleman, John, et al. *The CFPB's PFDR Rule Revisited: Comments Reveal Deep Divides on Definition of "Consumer," Fees, Security and Privacy*, Orrick, 30 Oct. 2025, www.orrick.com/en/insights/2025/10/the-cfpbs-pfdr-rule-revisited-comments-reveal-deep-divides-on-definition-of-consumer.
9. "Comments of Americans for Prosperity." Received by Consumer Financial Protection Bureau, Americans for Prosperity, https://americansforprosperity.org/wp-content/uploads/2025/10/CFPB-1033-comment.pdf. Accessed 20 Nov. 2025.
10. Ginn, Vance. *CFPB'S Section 1033 Rule: Balancing Data Access and Consumer Protection*, Americans for Tax Reform, Feb. 2025, atr.org/wp-content/uploads/2025/02/atr_cfpb-1033_report_v2.pdf.
11. Gins, Andrew, and Aiden Wegener. *ATR Submits Comment Letter Urging CFPB to Reject Biden-Era Dodd-Frank Rule*, Americans for Tax Reform, 13 Nov. 2025, atr.org/atr-submits-comment-letter-urging-cfpb-to-reject-biden-era-dodd-frank-rule/.
12. Horwitz, Jeff. *Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show*, Reuters, www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/. Accessed 20 Nov. 2025.
13. Koch, Tom, and Stephanie Nguyen. *Gramm-Leach-Bliley Act*, Federal Trade Commission, 17 June 2025, www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.
14. Pape, Carter. "A Complete Guide to the CFPB's Open Banking Rule." *American Banker*, Arizent, 25 Oct. 2024, www.americanbanker.com/news/a-complete-guide-to-the-cfpbs-new-open-banking-rule.
15. Paridon, Paige Pidano. "Comments on Advance Notice of Proposed Rulemaking." Received by Russell Vought, *Orrick, Herrington & Sutcliffe LLP*, Bank Policy Institute, 21 Oct. 2025, https://infobytes.orrick.com/wp-content/uploads/BPI-Letter-1.pdf. Accessed 20 Nov. 2025.
16. Shevlin, Ron. "The Problems with the CFPB's New Open Banking Rule." *Forbes*, Forbes Magazine, 27 Nov. 2024, www.forbes.com/sites/ronshevlin/2024/11/24/the-problems-with-the-cfpbs-new-open-banking-rule/.
17. Sowell, Thomas. *Price Controls*, Capitalism Magazine, 16 Nov. 2005, capitalismmagazine.com/2005/11/price-controls/.
18. Steven, Jim, and Michael Bruemmer. *2024 Data Breach Industry Forecast*, Experian, www.experian.com/content/dam/marketing/na/data-breach/reports/2024-data-breach-industry-forecast.pdf. Accessed 20 Nov. 2025.

19. Szewczyk, Gregory P., et al. "Trade Associations Sue CFPB on Same Day as It Issues Final Open Banking Rule under Section 1033 of Dodd-Frank." *Consumer Finance Monitor*, Consumer Financial Services Group at Ballard Spahr LLP, 24 Oct. 2024, www.consumerfinancemonitor.com/2024/10/24/trade-associations-sue-cfpb-on-same-day-as-it-issues-final-open-banking-rule-under-section-1033-of-dodd-frank/.
20. Tamny, John. "Information Is Extraordinarily Valuable. How Dangerous To Make It Free." *Forbes*, Forbes Magazine, 24 July 2025, www.forbes.com/sites/johntamny/2025/07/24/information-is-extraordinarily-valuable-how-dangerous-to-make-it-free/.