epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Statement of Alan Butler

Executive Director, Electronic Privacy Information Center (EPIC)

Hearing on "Innovation Revolution: How Technology is Shaping the Future of Finance"

Before the

Committee on Financial Services

United States House of Representatives

December 4, 2024

Chair McHenry, Ranking Member Waters, and Members of Committee, thank you for the opportunity to testify today on *How Technology is Shaping the Future of Finance*. My name is Alan Butler, and I am Executive Director at the Electronic Privacy Information Center. EPIC is an independent nonprofit research organization established in 1994 to secure the right to privacy in the digital age for all people.

EPIC promotes legal and technological standards that strengthen privacy protections for individuals in the digital economy. We support innovations that make financial services more secure, resilient, and accessible for consumers. However, we recognize that many changes can have the opposite effect, especially for the most vulnerable populations, if they increase the speed and severity of financial scams and frauds. We have also seen a broad and troubling trend toward commodifying and monetizing personal data, including sensitive financial data, in ways that enrich data brokers and other businesses at the expense of consumers. In order to promote innovations in this sector that will empower consumers rather than exploiting them, we need privacy and security protections that are fit for the 21st Century.

There is no doubt that the last two decades have seen significant changes in our financial sector with the development of new technologies and new business models. The emergence of cryptocurrencies and other digital assets, new digital payment platforms and applications, and crowdfunding have transformed the consumer financial marketplace. But it is important to recognize the new risks that have emerged over that same period, and to recall that throughout history, cycles of evolution and revolution in the financial sector have called for updates to the guardrails and standards that protect consumers against these new risks.

As we look to the decades ahead, financial technology will continue to evolve and reshape the marketplace and the experience of consumers. And we should work now to guide

these developments toward a more secure, trustworthy, and fair future for consumers, especially when it comes to protecting their personal data. Far too often, the term "innovation" has been used to obscure practices that are, at bottom, extractive and exploitative and do not serve the interests of the individuals who use these services. We can and should aspire for better. Technology has the power to provide people with faster and more secure access to the world around them, to create new opportunities for entrepreneurship and financial security, and to increase trust in the digital marketplace. But those positive innovations will not happen without the proper guardrails and robust oversight.

In this discussion about innovation and the vision of the future for financial services, I would like to focus my remarks on four key concepts that should be central to the conversation: trust, security, privacy, and fairness.

1. **A healthy marketplace requires trust built on a clear set of rules and institutional guardrails.**

In theory, businesses in the financial sector should be well positioned to build trustworthy onramps to the digital economy because this is a service industry that incentivizes providers to deliver on customers want. But when it comes to privacy and security protections, providers have all the power to set the terms and the knowledge about what data is being collected, how it is being used, and how it is being secured. Most consumers of financial services don't know how best to protect themselves against fraud, identity theft, and invasive surveillance of their financial transactions. They rely on providers to establish and meet standards for the security of their assets and their data. But there are significant costs to secure accounts and data, and the best privacy and security practices are often invisible to the consumer. This is precisely why robust oversight and accountability are necessary to ensure that providers of financial services don't cut corners outside the view of consumers to increase their margins.

Many consumers have understandably lost trust in businesses that appear to see them more as products, or a raw material used to build a product, than as customers to serve. The mindset that "data is the new oil" has fueled an expansion over the last two decades in the monetization of consumers' personal data by third-party data brokers and first-party financial service providers.[1] Yet these changes are opaque to the consumers of financial services because they are not given any meaningful choice in or control over what is happening to their data. Those types of practices fundamentally erode trust. We need to re-establish consumer control over data to promote trust in financial technology.

2. Strengthening data security should be a top priority of businesses and policymakers working to shape the future of finance.

Most consumers are wary about trusting new digital payment technologies. According to a recent poll from the Pew Research Center, 63% of Americans are not confident in the reliability and safety of cryptocurrencies.[2] Another poll found that almost a third of U.S. adults who use digital payment apps have little or no confidence that their personal information is safe from hackers.[3] And these results should not be surprising given that fraud and identity theft are two of the most pressing problems for consumers according to reports filed with the Federal Trade Commission Consumer Sentinel Network (more than 2.5 million filed already this year, more

[1] *See* Alex Johnson, Fintech Takes, *The Future of the Financial Data Economy* (Sept. 18, 2024), https://fintechtakes.com/articles/2024-09-18/the-future-of-the-financial-data-economy/.
[2] Michelle Faverio, Wyatt Dawson, and Olivia Sidoti, Pew Research Center, *Majority of Americans Aren't Confident in the Safety and Reliability of Cryptocurrency* (Oct. 24, 2024), https://www.pewresearch.org/short-reads/2024/10/24/majority-of-americans-arent-confident-in-the-safety-and-reliability-of-cryptocurrency/.
[3] Monica Anderson, Pew Research Center, *Payment Apps Like Venmo and Cash App Bring Convenience – And Security Concerns – To Some* Users (Sept. 8, 2022), https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/.

than 3.5 million in 2023, and the same in 2022).[4] The financial sector as a whole surpassed healthcare in 2023 as the "most breached industry" according to industry reports.[5]

Trust can be especially difficult to preserve in a digital marketplace that relies on legacy infrastructure for identity management, authentication, and validation. Traditional banks relied on physical interactions with customers, auditable paper trails and signatures, and a slower pace to build and retain trust over many decades. But a digital world requires a completely different approach. That is why it is encouraging to see innovation in the development and adoption of standards based on "Zero Trust" principles.[6] Fintech companies must do more to improve identity management and verification to make it easier for consumers to adopt and use while making it harder for would-be attackers to gain unauthorized access to their accounts.

Despite the increase in breaches, the financial service industry has made significant improvements over the last decade in increasing account security standards for authentication. Multi-factor authentication methods are a good example of the type of positive innovation that should be incentivized and supported to increase trust and security for consumers. And financial regulators have done that in many ways through updated guidance and enforcement actions.[7] But more work is needed to make account security and fraud protection easy and intuitive for consumers.

---

[4] Fed. Trade Comm'n, Tableau Public, *The Big View: All Sentinel Reports* (searched by report type per year, published as of November 8, 2024), https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports.
[5] David White, Kroll, *Data Breach Outlook: Finance Surpasses Healthcare as Most Breached Industry in 2023* (2024), https://www.kroll.com/-/media/kroll-images/pdfs/data-breach-outlook-2024.pdf.
[6] *See* Andrew Kennedy, Bank Policy Institute, *Adaptive Trust: Zero Trust Architecture in a Financial Services Environment* (Mar. 21, 2022), https://bpi.com/adaptive-trust-zero-trust-architecture-in-a-financial-services-environment/.
[7] *See* Andrew Kennedy, Bank Policy Institute, *Multifactor Authentication: Opportunities and Challenges* (Feb. 27, 2023) https://bpi.com/multifactor-authentication-opportunities-and-challenges/.

3. The financial services of the future should not be built on the privacy models of the past, and clear rules limiting data collection and use are needed.

The rapid growth of financial technology over the last decade has revealed major changes in the ways that individuals transact, invest, and store value in a digital ecosystem. One dimension of that change is an exponential growth in the amount of data collected about individuals and a fundamental shift in how that data is used and what impact those uses have on consumers. But as technologies and business practices in the financial services industry have shifted, the privacy protections and standards have not kept pace. Our current financial privacy regime is rooted in outmoded understandings of both the boundaries of the field and the scope of protections necessary to preserve privacy. We need a new approach as we look ahead toward future developments in financial technology over the next two decades.

Most people who have some involvement with the financial system (either on the business or consumer side) likely think of paper notices when they hear the term financial privacy. These notices are ubiquitous in this industry, and yet I doubt many consumers would say that these notices give them any meaningful sense of control over what happens to their data. Indeed, the only control that the law gives to these consumers is a difficult-to-effectuate right to opt out of data transfers to non-affiliated companies—a exceptionally weak form of control that has been scorned by industry analysts and privacy advocates alike.[8]

In the "Innovation Revolution," we do not need to increase the number of privacy notice letters stacked up in consumers' recycling bins. Instead, we need clear rules that align the data privacy practices of firms with the interests of the consumers they aim to serve. Strong data

[8] *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 Minn. L. Rev. 1219, 230 (2002).

minimization rules[9] serve this purpose by enabling data collection and use that is reasonably necessary to provide consumers with the goods and services they seek, while limiting unnecessary data collection and prohibiting secondary uses that do not serve the interests of consumers.[10] These rules also bolster trust because they align financial firms' data collection practices with what consumers expect. And by limiting the collection of personal data to what is actually needed, there would be marked improvements in data security as well. Data that is never collected in the first place cannot be breached.

A strong data minimization framework is especially important in a rapidly evolving financial sector where consumers seek expanded services beyond banking and payments. These new services require access to and use of data from a wide range of accounts and services.[11] But without strong guardrails, consumers' sensitive financial data would be at risk. Those protections must also apply to a broad range of entities because financial technology innovations have significantly expanded the range and types of financial services being offered. With solid guardrails in place, consumers can better explore and use new and innovative services with the confidence that financial firms are not misusing their data.

4. Policymakers and regulators must also continue to shut down unfair business practices that take advantage of the power and information imbalances inherent in the financial ecosystem.

Not all innovations are good—there are many historical examples of innovations that have harmed consumers by exacerbating fraud or scams (such as the infamous Ponzi scheme).[12]

---

[9] EPIC, *Data Minimization*, https://epic.org/issues/consumer-privacy/data-minimization/.
[10] EPIC, Comments on CFPB Consumer Financial Data Rights Rulemaking (Jan. 25, 2023); EPIC, Comments on CFPB Small Business Advisory Review Panel for Consumer Reporting Rulemaking (Oct. 30, 2023); EPIC, Comments on FTC Proposed Trade Regulation Rule on Commercial Surveillance and Data Security (Nov. 2022).
[11] CFPB Personal Financial Data Rights Rule, 12 C.F.R. § 1001 & 1033 (2024).
[12] Smithsonian Nat'l Postal Museum, *Behind the Badge: Ponzi Scheme* (2024), https://postalmuseum.si.edu/exhibition/behind-the-badge-case-histories-scams-and-schemes/ponzi-scheme.

And even revolutionary technologies that benefit consumers can also bring new risks. That is why, as technology evolves, the standards of fair practice in the financial sector do as well. The challenge in the years ahead will be identifying emerging areas of unique risk that require intervention and oversight.

Fairness was a central focus of policymaking in the financial sector during an earlier transformative period: the 1970s. That decade saw the rapid expansion of consumer credit and the emergence of the credit reporting bureaus subject to the comprehensive oversight framework created by Congress. The Fair Credit Reporting Act (FCRA) was the first consumer privacy law in America, and it was enacted alongside the Equal Credit Opportunity Act and the Fair Credit Billing Act to create a set of significant guardrails for the evolving financial services sector.

These laws addressed the problems of increasing complexity, velocity, and automation in the field by establishing enforceable individual rights for consumers to protect against increased fraud, discrimination, and inaccurate reports that these new technologies and business practices would cause. And without them, consumers would have been much worse off. So too are the industries that grew out of these financial services evolutions, even though some spent decades contesting the legitimacy of those laws. The work of applying and enforcing those laws to meet the moment continues to this day, which is why the Consumer Financial Protection Bureau plays such an important role in overseeing this field. It is essential to keep in mind as we evaluate the current landscape and consider what new or updated guardrails might be necessary to protect consumers and the public interest that the entities regulated by these laws will claim that they are burdensome and unnecessary—but history has shown the opposite.

* * *

There is no doubt that we are witnessing rapid changes due to the advent of innovations in financial technology. There is a real opportunity to build on those innovations to improve consumers' lives by establishing trust in the digital economy, securing people's data from hackers and brokers alike, and shutting down unfair practices before they can take root and spread financial hardship. The shape of this future will be determined in part by the important work of the Members of this Committee. And we look forward to working with you on these issues in the years ahead. The privacy and security of Americans' financial data will only become more critical as financial technology evolves and expands its reach.

Thank you again for the opportunity to testify today.