

FRAMEWORK FOR THE FUTURE: REVIEWING DATA PRIVACY IN TODAY'S FINANCIAL SYSTEM

HEARING BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS OF THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED NINETEENTH CONGRESS FIRST SESSION

JUNE 5, 2025

Serial No. 119-26

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

60-987 PDF

WASHINGTON : 2026

HOUSE COMMITTEE ON FINANCIAL SERVICES

FRENCH HILL, Arkansas, *Chairman*

BILL HUIZENGA, Michigan, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	SYLVIA R. GARCIA, Texas, <i>Vice Ranking Member</i>
PETE SESSIONS, Texas	NYDIA M. VELÁZQUEZ, New York
ANN WAGNER, Missouri	BRAD SHERMAN, California
ANDY BARR, Kentucky	GREGORY W. MEEKS, New York
ROGER WILLIAMS, Texas	DAVID SCOTT, Georgia
TOM EMMER, Minnesota	STEPHEN F. LYNCH, Massachusetts
BARRY LOUDERMILK, Georgia	AL GREEN, Texas
WARREN DAVIDSON, Ohio	EMANUEL CLEAVER, Missouri
JOHN W. ROSE, Tennessee	JAMES A. HIMES, Connecticut
BRYAN STEIL, Wisconsin	BILL FOSTER, Illinois
WILLIAM R. TIMMONS, IV, South Carolina	JOYCE BEATTY, Ohio
MARLIN STUTZMAN, Indiana	JUAN VARGAS, California
RALPH NORMAN, South Carolina	JOSH GOTTHEIMER, New Jersey
DANIEL MEUSER, Pennsylvania	VICENTE GONZALEZ, Texas
YOUNG KIM, California	SEAN CASTEN, Illinois
BYRON DONALDS, Florida	AYANNA PRESSLEY, Massachusetts
ANDREW R. GARBARINO, New York	RASHIDA TLAI, Michigan
SCOTT FITZGERALD, Wisconsin	RITCHIE TORRES, New York
MIKE FLOOD, Nebraska	NIKEMA WILLIAMS, Georgia
MICHAEL LAWLER, New York	BRITTANY PETTERSEN, Colorado
MONICA DE LA CRUZ, Texas	CLEO FIELDS, Louisiana
ANDREW OGLES, Tennessee	JANELLE BYNUM, Oregon
ZACHARY NUNN, Iowa	SAM LICCARDO, California
LISA McCLAIN, Michigan	
MARIA SALAZAR, Florida	
TROY DOWNING, Montana	
MIKE HARIDOPOLOS, Florida	
TIM MOORE, North Carolina	

Ben Johnson, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS

ANDY BARR, Kentucky, *Chairman*

BARRY LOUDERMILK, Georgia, <i>Vice Chairman</i>	BILL FOSTER, Illinois, <i>Ranking Member</i>
BILL HUIZENGA, Michigan	NYDIA M. VELÁZQUEZ, New York
ROGER WILLIAMS, Texas	GREGORY W. MEEKS, New York
JOHN W. ROSE, Tennessee	DAVID SCOTT, Georgia
WILLIAM R. TIMMONS IV, South Carolina	BRAD SHERMAN, California
RALPH NORMAN, South Carolina	AL GREEN, Texas
DANIEL MEUSER, Pennsylvania	JUAN VARGAS, California
YOUNG KIM, California	SEAN CASTEN, Illinois
BYRON DONALDS, Florida	STEPHEN F. LYNCH, Massachusetts
SCOTT FITZGERALD, Wisconsin	JOYCE BEATTY, Ohio
MIKE FLOOD, Nebraska	CLEO FIELDS, Louisiana
MONICA DE LA CRUZ, Texas	
TIM MOORE, North Carolina	

C O N T E N T S

Thursday, June 5, 2025

OPENING STATEMENTS

	Page
Hon. Andy Barr, Chairman of the Subcommittee on Financial Institutions, a U.S. Representative from Kentucky	1
Hon. Bill Foster, Ranking Member of the Subcommittee on Financial Institutions, a U.S. Representative from Illinois	3

STATEMENTS

Hon. French Hill, Chairman of the Committee on Financial Services, a U.S. Representative from Arkansas	4
Hon. Maxine Waters, Ranking Member of the Committee on Financial Services, a U.S. Representative from California	4

WITNESSES

Mr. Scott Talbott, Executive Vice President, Electronic Transactions Association	5
Prepared Statement	8
Mr. Andrew Morris, Director of Innovation and Technology, America's Credit Unions (ACU)	14
Prepared Statement	16
Ms. Rebecca Kuehn, Partner, Hudson Cook, LLP	29
Prepared Statement	31
Ms. Jennifer Huddleston, Fellow in Technology Policy, CATO Institute	38
Prepared Statement	40
Ms. Zoë Strickland, Senior Fellow, Future Of Privacy Forum	46
Prepared Statement	48

APPENDIX

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Representative Maxine Waters	
Mr. Scott Talbott	88
Mr. Andrew Morris	90
Ms. Rebecca Kuehn	91
Ms. Zoë Strickland	92
Written responses to questions for the record from Representative Gregory Meeks	
Ms. Zoë Strickland	93

LEGISLATION

H.R. —, the Advancing the Mentor Protégé Program for Small Financial Institutions Act	97
H.R. —, the Systemic Risk Authority Transparency Act	102

FRAMEWORK FOR THE FUTURE: REVIEWING DATA PRIVACY IN TODAY'S FINANCIAL SYSTEM

Thursday, June 5, 2025

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:09 a.m., in room 2128, Rayburn House Office Building, Hon. Andy Barr [chairman of the subcommittee] presiding.

Present: Representatives Barr, Huizenga, Williams of Texas, Loudermilk, Rose, Timmons, Kim, Fitzgerald, Flood, De La Cruz, Moore, Foster, Scott, Sherman, Green, Vargas, Casten, Beatty, and Fields.

Also present: Representatives Hill, Davidson, and Waters.

Chairman BARR. The Subcommittee on Financial Institutions will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

This hearing is titled "Framework for the Future: Reviewing Data Privacy in Today's Financial System."

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record.

I now recognize myself for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. ANDY BARR, CHAIRMAN OF THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS, A U.S. REPRESENTATIVE FROM KENTUCKY

Thank you to our witnesses for being here today and lending your expertise to this complex and critical conversation.

Today's hearing focuses on financial data privacy, where we will assess how Congress can ensure consumers' data is used only as authorized while protecting the innovation that has transformed our financial system since the Gramm-Leach-Bliley Act, or GLBA, became law more than 25 years ago.

Since GLBA's passage, technological advances have revolutionized how Americans access financial services. We have seen the rise of mobile banking apps, peer-to-peer payment platforms, and a shift away from cash toward digital transactions. These innovations have expanded financial products and increased access for millions of Americans in rural communities and urban centers.

Alongside these developments, the volume and sensitivity of financial data have surged dramatically. Every transaction and interaction creates data points that financial institutions and fintech firms analyze to improve services, assess risk, and detect fraud and tailor products.

While these capabilities bring benefits, they also raise serious privacy and security concerns.

A key driver of innovation is open banking, allowing consumers to securely share their financial data with third-party providers through application programming interfaces, or APIs. Open banking can empower consumers with more control over their financial information, foster competition, and spur the development of new tools and services, but it also raises questions about data privacy, liability, standard-setting, and GLBA's applicability.

GLBA's broad framework has served us well, setting key protections for consumer data but a quarter of a century is a long time in tech. So, we must ask, is GLBA still fit for purpose in today's fast-paced, data-driven environment? Does it provide the clarity, flexibility, and protection needed in the digital age?

As we consider modernization, we must proceed cautiously. Changes that are too restrictive risk choking off access to financial options on which consumers rely. Conversely, overly lax rules could leave Americans vulnerable to misuse of their sensitive data. Striking the right balance is critical.

We also cannot examine GLBA in isolation. Data privacy laws have proliferated at the State level, with 20 States enacting comprehensive privacy laws. Some exempt financial institutions that comply with GLBA, while others layer on more stringent requirements.

This patchwork creates a complex, costly compliance landscape, potentially increasing costs and reducing access. This also risks some States setting de facto national standards, bypassing Congress and creating uncertainty for businesses and consumers alike.

For these reasons, Congress should consider the benefits of a uniform national data privacy standard that offers clear, consistent, preemptive rules for financial institutions while protecting consumers.

As our colleagues on the Energy and Commerce Committee work on broader privacy legislation, we must also ask whether sector-specific laws, like GLBA, warrant carve-outs or tailored treatment. GLBA already imposes strong data protection requirements, and financial institutions have built compliance programs around these rules. Overlapping or conflicting standards would only add confusion and cost.

Finally, we must address calls to expand enforcement mechanisms by granting consumers private rights of action, which allow individuals to sue firms directly for alleged violations. Private rights of action open the door to frivolous lawsuits, benefiting large firms that can absorb litigation costs and discouraging innovation by increasing legal risks for financial services providers. Ultimately, consumers lose out through reduced access and choice of innovative products.

While these are complex issues requiring thoughtful consideration, we must balance robust privacy protections with innovation, access, and reduced regulatory burden.

I look forward to hearing from our witnesses today and engaging in a productive discussion on the future of data privacy in our financial system.

The chair now recognizes the ranking member of the subcommittee, Dr. Foster, for 4 minutes for an opening statement.

OPENING STATEMENT OF HON. BILL FOSTER, RANKING MEMBER OF THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS, A U.S. REPRESENTATIVE FROM ILLINOIS

Mr. FOSTER. Thank you, Chairman Barr, and to our witnesses for their excellent written testimony.

Today, we will be discussing the framework for data privacy in today's financial system. At its core are the Gramm-Leach-Bliley Act; the Fair Credit Reporting Act (FCRA); and section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Minor changes have been made to this framework over the years. However, there are significant questions about how these laws are adapting to an increasingly digital economy, innovative financial products, cybersecurity risks, artificial intelligence, and the growing role of third-party firms in the financial sector.

I look forward to discussing many of these issues with our panel today.

I was proud to have sat on this committee when we drafted the Dodd-Frank Act and was happy to see the most recent update to the financial privacy framework come out last October, when, after years of bipartisan work under three different Presidents, the Consumer Financial Protection Bureau (CFPB) finalized the Personal Financial Data Rights Rule to implement section 1033 of the act.

This rule is significant because it gives consumers greater rights, privacy, and security over their personal financial data. It makes it easier for consumers to switch between service providers to find better rates, to make secure payments, and to utilize innovative tools to manage their finances. This rule gives consumers the right to revoke access to their data whenever they choose and promotes the development of market-driven data standards.

The rule was developed through a lengthy process spanning multiple Presidential administrations, gathering public feedback at several points, starting in 2016. The first Trump Administration started the process of implementing the rule, with an advance notice of proposed rulemaking in 2020.

Despite the work of the first Trump Administration and our former Chair, Patrick McHenry, supporting the final rule, the Trump Administration is now apparently working to repeal the rule.

This morning, I led 12 of my colleagues from the committee in sending a letter to acting CFPB Director Russell Vought urging him not to rescind this rule but, rather, to address outstanding issues through targeted amendments and future guidance.

It has been nearly 15 years since the passage of Dodd-Frank, and rewriting this rule in its entirety would cause an unnecessary delay that will hurt privacy, hurt innovation, and hurt competition.

Finally, while I support this committee's renewed focus on data privacy legislation, I am also deeply concerned by other actions taken by this administration related to Americans' sensitive data.

The President and Elon Musk sent members of their Department of Government Efficiency (DOGE) team to raid government agencies of their data across our government, where they accessed and gathered sensitive data on millions of Americans. This includes data from the Social Security Administration, from Treasury, from Health and Human Services, and even the Consumer Financial Protection Bureau, which holds information on companies that, for example, would directly compete with Elon Musk's payment company, X Money.

These efforts pose great risk to the privacy of all Americans, and anyone that truly cares about privacy should be calling for immediate accountability and transparency from all those involved.

Thank you, and I yield back.

Chairman BARR. The gentleman yields back.

The chair now recognizes the chairman of the full committee, Mr. Hill, for 1 minute.

STATEMENT OF HON. FRENCH HILL, CHAIRMAN OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM ARKANSAS

Chairman HILL. Thank you, Chairman Barr.

Since 1999, when the Gramm-Leach-Bliley Act was passed, most Americans were still watching movies on their VCRs and arguing over who was tying up the dial-up internet connection. Since then, technology has advanced at an extraordinary pace and so has the amount of sensitivity of personal financial information being collected and shared.

Remarkably, GLBA has kept the pace of many of these changes but given the magnitude of today's technological complexity and the increase of data availability and collection, we must ensure Americans' privacy is protected while continuing to support the seamless delivery of the financial services that they rely on.

Congress has a major role to play in crafting strong, modernized guardrails that keep pace with innovation, preserve consumer trust, and future-proof our laws. Over the last several Congresses, committee Republicans have worked to craft a narrowly tailored legislation to modernize our financial data. We look forward to working on that in this Congress now with the leadership and partnership of the House Energy and Commerce Committee.

I yield back to you, Mr. Barr.

Chairman BARR. The gentleman yields back.

The chair now recognizes the ranking member of the full committee, Ms. Waters, for 1 minute.

STATEMENT OF HON. MAXINE WATERS, RANKING MEMBER OF THE COMMITTEE ON FINANCIAL SERVICES, A U.S. REPRESENTATIVE FROM CALIFORNIA

Ms. WATERS. Thank you very much.

Today, we are considering the important issue of data privacy. However, I find it rich that any Republican here would claim to support data privacy, when they have said nothing about Trump

letting Elon Musk and his DOGE minions steal the sensitive data of hundreds of millions of Americans—everything from their health records and consumer data to Social Security numbers and tax data.

Trump did not stop there. In addition to shuttering the Consumer Financial Protection Bureau, which fights fraudsters and helps Americans get remedies from predatory financial firms, Trump also wrongly vacated the CFPB's Open Banking Rule that promotes data privacy.

I would like to think there is bipartisan support to protect Americans' data, but we must first start by stopping the biggest threat: Donald J. Trump.

I yield back.

Chairman BARR. The gentlelady yields back.

Today, we welcome the testimony of Mr. Scott Talbott, Executive Vice President of the Electronic Transactions Association; Mr. Andrew Morris, Director of Innovation and Technology at America's Credit Unions; Ms. Rebecca Kuehn, Partner at Hudson Cook; Ms. Jennifer Huddleston, Fellow in Technology Policy at the Cato Institute; and Ms. Zoë Strickland, senior fellow at the Future of Privacy Forum.

We thank you for taking the time to be here. You each will be recognized for 5 minutes to give an oral presentation of your testimony. Without objection, your written statements will be made part of the record.

Mr. Talbott, you are now recognized for 5 minutes.

**STATEMENT OF SCOTT TALBOTT, EXECUTIVE VICE
PRESIDENT, ELECTRONIC TRANSACTIONS ASSOCIATION**

Mr. TALBOTT. Good morning, Chairman Barr, Ranking Member Foster, and members of the Financial Institutions Subcommittee. I am Scott Talbott. It is my privilege, as the Executive Vice President at the Electronic Transactions Association (ETA), to speak with you today on the future of privacy and the modern payments system.

ETA is a trade association representing a broad group of companies from banks to processors and fintechs who provide electronic products and services, including mobile wallets, peer-to-peer products, credit, debit, and prepaid cards, as well as other forms of digital payments.

Last year, our industry helped consumers and merchants in the United States make over \$11 trillion in card and peer-to-peer (P2P) payments securely, reliably, and quickly. In fact, during the 5 minutes I will speak this morning, roughly 1.5 million transactions will be processed in the United States.

In each of these transactions, there is a shared expectation between consumers and the payments industry that personal data will be kept both private and secure. Given ETA's members' role in the payments industry, both privacy and security are top priorities for our members.

Entities in the payments industry are covered directly or indirectly by the Gramm-Leach-Bliley Act and a handful of State privacy laws. The core structure of GLBA imposes both privacy and data security requirements on the industry. This is accomplished

through the Privacy Rule and the Safeguards Rule. These requirements in GLBA are tailored to the unique and complex nature of the financial services industry.

For financial services, all transactions involve at least two and quite possibly more entities working together to execute the customer's request. A prime example is a single credit card purchase where at least three or sometimes four entities are involved in moving the data as well as the payment. GLBA recognizes this reality and allows multiple entities to share data to work together seamlessly and quickly to serve customers' needs.

While GLBA is largely working well for the financial services industry, a challenge comes with the patchwork of nearly two dozen State privacy laws, eight of which went into effect this year alone. These State laws have different approaches to privacy as well as key definitions that create confusion for consumers, small businesses, as well as challenges and expense to financial services and other businesses working to comply. Sometimes the State laws even conflict with each other, and in my written testimony I have given examples of this.

As Congress considers changes to the privacy laws, there are a few key things that we urge you to consider.

First, is the need for a uniform national standard. ETA member companies serve consumers and businesses, especially small businesses, in all 50 States. A single, strong, uniform national privacy standard would serve all American consumers and businesses by providing common expectations as they conduct their everyday transactions.

Any new Federal privacy law should be technology-neutral and sector-neutral. However, given the complexity of financial services and its unique needs, the financial services industry should continue to be governed by GLBA.

Next, consumers should have rights within this Federal privacy law. Privacy is a two-way street. For consumers, the Federal privacy law should include consumer rights such as disclosure, access, correction, deletion, and opting out of targeted marketing. We also support using appropriate data minimization and data usage standards that are reasonably suited to execute the underlying transaction.

These key aspects will ensure that institutions know their responsibilities and consumers know what to expect. This approach will work to eliminate redundancies, inconsistencies, and confusion created by the existing State privacy regimes.

Any privacy law must retain permissible use of data to fight fraud. The payments industry works tirelessly to detect and minimize fraud. These efforts to fight fraud benefit consumers, merchants, as well as the economy. It is important that any privacy law contains permissible use of the data to fight fraud. Permissible use exists now in GLBA as well as in every State privacy law. Other countries' privacy laws also include this important use case.

The scenario here that we are focused on is that a thief commits fraud and then asks for the data to be deleted or forgotten. This would create a blind spot, allowing fraudsters room to fester. By including a permissible use of data to fight fraud in privacy law, the

payments industry will continue to have a 360-degree view of fraud or potential fraud in the payments space.

Enforcement by Federal regulators. We encourage any privacy law to assign enforcement to the appropriate Federal regulators.

Next, a key goal of the payments industry is continuous innovation, and we are constantly developing and deploying new products and services to make payments safer, faster, and more convenient for consumers.

Two new ideas on the horizon include open banking, or consumer-driven banking, and artificial intelligence. Both of these are in use in the market today, and both of these utilize data-sharing between multiple parties.

Open banking contemplates consumers directing the sharing of data, and artificial intelligence allows for faster and more efficient use of the data. Both of these are covered by existing Federal laws, including GLBA as well as fair lending. In both examples, policymakers should rely on these existing laws and look for any gaps and avoid rushing to legislate new privacy laws here.

On behalf of ETA and our member companies, thank you once again for the opportunity to participate in this important discussion. I look forward to any questions you may have.

[The prepared statement of Mr. Talbott follows:]

Testimony of Scott Talbott
Executive Vice President
Electronic Transactions Association

Financial Institutions Subcommittee of the House Financial Services Committee
Hearing on the Framework for the Future: Reviewing Data Privacy in Today's Financial
System
June 5, 2025

Chairman Barr, Ranking Member Foster, and Members of the Subcommittee:

Thank you for the opportunity to testify on the important issue of data privacy in the financial system. I am Scott Talbott, and I serve as Executive Vice President at the Electronic Transactions Association (ETA). ETA is the leading trade association representing the entire electronic payments industry. Our more than 300 member companies facilitate safe, efficient, and innovative digital transactions in every state and across global markets, amounting to over \$52 trillion globally. ETA members include payment processors, fintech firms, banks, hardware providers, and software platforms that form the backbone of the modern financial ecosystem.

ETA believes Congress should enact a single, uniform, comprehensive federal data privacy and data protection framework that protects consumers, supports innovation and operational agility, and ensures consistent national standards for the financial system. The law should exempt financial institutions and data currently subject to Title V of Gramm-Leach-Bliley Act.

Every day, our industry safely and securely helps power the American economy—whether enabling a small business to process its first digital transaction or facilitating contactless payments that enable consumers to make everyday purchases and to send money to each other. In every transaction, there is a shared expectation: that personal and financial data will be kept secure and handled responsibly.

Consumers rightly expect strong privacy protections and data security for their personal information and their money, and ETA fully supports the creation of comprehensive, uniform, federal data privacy legislation that upholds those expectations. But a federal data privacy framework must be thoughtful, workable, and grounded in how the financial system actually functions. It should provide consumers with the right to access, correct, and delete their information. It must balance strong consumer protections with the operational realities of protecting against fraud, enabling innovation, and supporting compliance. And it must preempt the growing patchwork of state laws that threaten to fragment the privacy landscape in ways that harm consumers and businesses alike.

The need for federal preemption is not theoretical. It is essential. As the University of Chicago Law Review noted in a 2020 article, “[a] fragmented legal regime can lead to inconsistent consumer outcomes, duplicative compliance costs, and reduced innovation in data-driven markets” (Richards & Hartzog, 2020). Privacy frameworks should provide clarity, not complexity. Consumers deserve consistent rights, and businesses deserve consistent rules, regardless of geography.

Today, two dozen states have enacted varying data privacy laws, with varying definitions, requirements, and enforcement regimes. This legal fragmentation creates extraordinary compliance burdens, especially for small and mid-sized companies that lack the resources of large multinationals.¹ A study by PwC found that over 50% of companies surveyed had to reengineer internal processes to meet divergent state privacy laws, with associated costs exceeding \$1 million annually in many cases (PwC US, “Consumer Intelligence Series: Protect.me,” 2022). Another study² found that state privacy laws could impose costs of between \$98 billion and \$112 billion annually. Over a 10-year period, these out-of-state costs would exceed \$1 trillion. Of these costs, small businesses would bear \$20–23 billion of this out-of-state burden annually.

The payments industry is not alone in calling for a federal solution. In a widely cited paper published in the Harvard Journal of Law & Technology, legal scholar Omer Tene observed: “The absence of a unified U.S. federal privacy regime has created both legal uncertainty and competitive disadvantages for American firms” (Tene, 2018). Moreover, organizations from the National Governors Association to leading consumer protection organizations like the Center for Democracy and Technology, Electronic Privacy Information Center, and Consumer Action, have supported legislation that harmonizes privacy rights and responsibilities under a federal umbrella.

A federal standard must also allow for the use of data to protect against fraud in order to protect consumers. The permissible use of data for fraud protection is essential to the safe operation of financial systems. ETA members use behavioral analytics, device recognition, biometric verification, and real-time pattern recognition to detect and mitigate identity theft, account takeovers, and fraudulent transactions. These systems rely on the responsible and secure use of consumer data.

For example, when a transaction originating in New York is suddenly attempted from Eastern Europe, fraud detection protocols may flag the discrepancy and seek to verify the transaction. We have all received notifications from our bank asking to verify a transaction. These systems—built over decades—are essential to the trust that underpins our financial system. That trust, and

¹ At the end of the document: ETA chart with examples of where state privacy laws conflict with each other.

² [50-State Patchwork of Privacy Laws Could Cost \\$1 Trillion More Than a Single Federal Law, New ITIF Report Finds \(Jan 2022\)](#)

those protections, would be weakened if well-intentioned privacy laws unintentionally restricted fraud mitigation efforts.

The European Union's General Data Protection Regulation (GDPR) acknowledges this balance. Article 6 of the GDPR expressly permits the processing of personal data without consent when "necessary for the purposes of the legitimate interests pursued by the controller" including fraud protection. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) similarly permits the collection and use of data for the purpose of detecting and mitigating fraud, without consumer consent.

Our view on this topic is straightforward: any U.S. federal privacy law should follow suit by embedding protections for the responsible use of data to detect, mitigate, and respond to fraudulent or suspicious activity. The Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and Bank Secrecy Act all provide for these uses under existing law. *The Financial Data Privacy Act*, introduced last Congress by former House Financial Services Committee Chairman McHenry, built on this legacy by incorporating strong privacy rights while explicitly preserving fraud protection capabilities. That approach deserves to be the starting point for further legislative action.

The Financial Data Privacy Act was also notable for what it did not include: a private right of action. Private rights of action often result in class action litigation that does little to protect consumers while imposing significant costs on businesses. According to research by the American Tort Reform Association, the state with broad private rights of action for privacy violations have seen an uptick in lawsuits filed by plaintiffs' firms seeking large settlements, often with limited consumer benefit (ATRA Report, 2021).

Instead, enforcement should continue to reside with the appropriate expert federal regulators—such as the federal banking regulators and the Federal Trade Commission—that understand both the complexity of the data systems and the need for measured responses. Regulators have the expertise, experience, and tools to investigate, remedy, and monitor violations without stifling innovation or overwhelming courts.

Moreover, implementation timelines must be realistic. When California began enforcing the California Consumer Privacy Act (CCPA) during the height of the COVID-19 pandemic, businesses across the country faced significant uncertainty. With final rules issued just months before enforcement began, companies struggled to adjust compliance regimes amid workforce disruptions and supply chain issues. ETA joined a coalition requesting delayed enforcement not to avoid compliance—but to allow companies the time to implement it. Congress should avoid similar missteps in future legislation by ensuring clear, early guidance and extended implementation periods.

ETA and our members fully support strong data privacy rules. What we need are smart, coordinated, and enforceable regulations that protect consumers, enable innovation, and reflect how data powers the financial system. We are already subject to numerous privacy law and data protection laws and standards—including the GLBA Safeguards Rule, Fair Credit

Reporting Act, CAN-SPAM and Telephone Consumer Protection Act, PCI-DSS, and state cybersecurity regulations. Many of our members invest millions annually in data security, employee training, and third-party audits. We want accountability—but under one clear, national framework.

The payments industry constantly develops and deploys new products and services. Two developments in the marketplace are Open Banking and Artificial Intelligence. With Open Banking, financial information is, at the direction of the account holder, shared between banks, data aggregators, also called third-party providers. To the extent any entity engaged in open banking is not subject to privacy laws, policy makers should consider applying privacy laws to them.

On Artificial Intelligence (AI) and other emerging technologies, policymakers should avoid regulating in the moment and instead should look for any gaps in existing laws and study any emerging risks that AI may create. Further, the payments industry is heavily regulated at the federal and state levels, and the long-standing use of rules-based AI by the industry is already subject to a number of laws and regulations, including fair lending laws. Any change in privacy law should consider existing laws and regulations and avoid stifling emerging technology.

Finally, any federal legislation should be technology-neutral. It should apply consistently across platforms and providers, whether the transaction happens on a mobile wallet, through a peer-to-peer app, or at a traditional bank branch. Financial privacy and data security should not depend on whether a consumer uses a fintech app or a debit card. Consistency is fairness.

ETA stands ready to assist Congress in developing and refining legislation that meets these standards. Specifically, we urge Congress to:

- Enact a comprehensive federal privacy and data security law that preempts state laws. The law should exempt financial institutions and data currently subject to Title V of Gramm-Leach-Bliley Act;
- Provide consumers with the ability to access, correct, and delete their data;
- Preserve the use of data for fraud protection and compliance;
- Assign enforcement to federal regulators;
- Provide clear, realistic implementation compliance timelines and guidance;
- Update definitions to focus on identified or identifiable individuals; and
- Establish technology- and sector- neutral standards.

Thank you again for the opportunity testify today. We welcome the opportunity to work with this Subcommittee to develop sound data privacy legislation that protects consumers and strengthens our digital economy.

Examples of Conflicting State Privacy Law Provisions

	Typical Approach	Conflicting State Approach
Applicability: B2B and employee	State privacy laws do not apply to individuals acting in commercial context, i.e., “B2B data” and employee data. <i>See all other state privacy laws.</i>	California applies to B2B data and employee data. Cal. Civ. Code § 1798.140(v)(1).
Scope of “Sensitive Data”	Sensitive data typically includes “personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.” <i>See, e.g.,</i> Va. Code § 59.1-575 “Sensitive data”.	Connecticut and Oregon include individual’s “status as a victim of crime” as sensitive data. Conn. Gen. Stat. § 42-515(38)(E); Or. Rev. Stat. § 646A.570(18)(a)(A).
		Maryland and Oregon also include data revealing “national origin.” Md. Code, Com. Law § 14-4601(GG)(1)(vii); Or. Rev. Stat. § 646A.570(18)(a)(A).
		California additionally includes data revealing “philosophical beliefs” and “union membership,” among a host of other data types, as sensitive data. Cal. Civ. Code § 1798.140(ae).
Data Minimization	Data collection and processing typically must be limited to what is adequate, relevant, and reasonably necessary to the disclosed processing purpose. <i>See, e.g.,</i> Va. Code § 59.1-578(A)(1).	Maryland requires controllers to limit data collection to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to whom the data pertains. Md. Code, Com. Law § 14-4607(B)(1).
		California applies data minimization requirements additionally to data use, retention, and sharing. Cal. Civ. Code § 1798.100(c).
Consumer Rights Request Mechanisms	Many states allow the controller to determine “one or more secure reliable means” for consumers to exercise consumer rights. <i>See, e.g.,</i> Va. Code § 59.1-578(E).	Other states such as California , Florida , Nebraska , and Texas require that there be a method through the controller’s website if the controller maintains a website. <i>See, e.g.,</i> Cal. Civ. Code § 1798.130(a)(1)(B); Fla. Stat. § 501.709(3); Neb. Rev. Stat. § 87-1111(3); Tex. Bus. & Com. Code § 541.055(c).
Responsibilities over Sensitive Data	Processing, including sale, of sensitive data is permitted only with opt-in consent from consumers. <i>See, e.g.,</i> Va. Code § 59.1-578(A)(5).	Maryland prohibits collecting, processing, or sharing sensitive data, even with consent, unless it is “strictly” necessary to provide or maintain a specific product or service requested by the consumer; sale is entirely prohibited. Md. Code, Com. Law § 14-4607(A).
Disclosure of Categories of Recipients of Data	States often allow consumers to request and obtain the categories of third parties to whom the controller shares personal information. <i>See, e.g.,</i> Cal. Civ. Code § 1798.115(a)(2). If no right to request such categories, then	Minnesota allows consumers to request and obtain a list of specific third parties to whom the controller has disclosed personal information of that consumer. Minn. Stat. § 3250.05(h).

	other states require controllers to disclose the categories of third parties on their privacy notice. <i>See, e.g.,</i> Va. Code § 59.1-578(C)(5).	
--	--	--

Chairman BARR. Thank you.

Mr. Morris, you are now recognized for 5 minutes.

**STATEMENT OF ANDREW MORRIS, DIRECTOR OF INNOVATION
AND TECHNOLOGY, AMERICA'S CREDIT UNIONS**

Mr. MORRIS. Good morning, Chairman Barr, Chairman Hill, Ranking Member Foster, and members of the subcommittee. My name is Andrew Morris. I am Director of Innovation Technology at America's Credit Unions.

Thank you for the opportunity to testify about how a comprehensive Federal privacy law can be harmonized with the existing laws and regulations applicable to credit unions and other financial institutions.

First and foremost, America's Credit Unions supports a comprehensive Federal data security and privacy framework that includes robust security standards that apply to all who collect or hold sensitive personal data. It is important that, as the law evolves to match it, credit unions have rules of the road that allow them to meet the needs of their members in the marketplace.

Depository institutions, including credit unions, have long been subject to a framework of laws and regulations designed to ensure a high standard of consumer privacy and data security. Central to this framework is Title V of the GLBA, which acknowledges the need for heightened care when handling sensitive consumer financial information and provides well-established standards for addressing consumer privacy concerns.

America's Credit Unions believes that the Gramm-Leach-Bliley Act should remain the model for depository institution compliance with any future Federal data privacy and security standard.

Credit unions, like many financial institutions, have long prioritized investments in data security to ensure that their members' privacy is protected. The GLBA requires financial regulators to implement safeguards that are comprehensive and designed to ensure the security, confidentiality, integrity, and proper disposal of consumer information and other records.

Under the rules promulgated by the National Credit Union Administration, every credit union must develop and maintain an information security program to protect consumer data. Additionally, the rules require credit unions to ensure that third-party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

As Congress considers potential reforms to data privacy and security, there are various aspects we believe should be included or addressed.

First, there should be an entity-level exemption for credit unions and similarly regulated financial institutions that are subject to the GLBA. An entity-level exemption would recognize the rigor of existing financial institution compliance activities and allow regulators to tailor supervision based on changing privacy or data security risks.

Second, the oversight of credit unions, banks, and other depository institutions should be left to the functional financial institution regulators that have experience in this field.

Third, preemption of State laws is necessary. Today's patchwork of State privacy laws has invited idiosyncratic approaches to data processing activities and technologies. Some States, by choosing to recognize only a data-level exemption, have placed strains on credit unions by demanding more complex procedures for addressing data processing activities. The resulting compliance burdens, magnified each time a new State law is passed, siphon resources away from service to consumers and the core lending activities of credit unions.

Fourth, there should be limits on data deletion requirements. Prohibitions on collecting certain types of data without consumer opt-in or a broad right of deletion can frustrate efforts to comply with recordkeeping rules or to detect and prevent fraud.

Fifth, an opt-out regime should be maintained. The GLBA and Regulation P generally operate to limit sharing of sensitive consumer information through an opt-out process, something we believe should continue and be the standard for financial institutions in any future data privacy regime.

Sixth, as outlined in my written testimony, a comprehensive Federal data privacy framework should provide for principles-based requirements and offer a safe harbor for businesses that take the appropriate steps to comply with the law.

Seventh, any private right of action should be limited. We have serious concerns with any broad private right of action due to the risk of frivolous lawsuits being filed against credit unions, which are already held accountable for violations by their regulator, the National Credit Union Administration (NCUA), as well as the Consumer Financial Protection Bureau (CFPB).

In conclusion, stringent information security and privacy practices have long been a part of the financial sector's business practices and are necessary, as financial institutions are entrusted with consumers' nonpublic personal information. We look forward to working with you to achieve a well-balanced Federal data privacy framework.

Thank you for holding this important hearing and the opportunity to appear before you today. I welcome any questions you may have.

[The prepared statement of Mr. Morris follows:]



Testimony of

Andrew Morris
Director, Innovation and Technology
America's Credit Unions

Hearing: "Framework for the Future: Reviewing Data Privacy in Today's
Financial System"

Before the
Subcommittee on Financial Institutions
House Committee on Financial Services

June 5, 2025

Introduction

Good morning, Chairman Barr, Ranking Member Foster, and Members of the Subcommittee. I am Andrew Morris, Director of Innovation and Technology at America's Credit Unions. America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the credit union industry to effectively meet the needs of their over 142 million members nationwide. Thank you for the opportunity to testify about how a comprehensive federal privacy law can be harmonized with the existing laws and regulations applicable to credit unions.

First and foremost, America's Credit Unions supports a comprehensive federal data security and privacy framework that includes robust security standards that apply to all who collect or hold sensitive personal data. We recognize that the financial services landscape is evolving. It is important that as the law evolves to match it, credit unions have rules of the road that allow them to meet the needs of their members in the marketplace. This includes a data privacy standard that not only protects their members but also allows credit unions to evolve in their service to them.

As Congress considers changes to data privacy requirements, there are three key tenets that credit unions believe must be addressed in any new national data privacy law:

1. A recognition of Gramm-Leach-Bliley Act (GLBA) standards and accompanying regulations in place for financial institutions and a strong exemption from new burdensome requirements;
2. Robust federal preemption from a patchwork of state laws for credit unions in compliance with national privacy and GLBA standards; and
3. Protection from frivolous lawsuits created by a private right of action.

Existing Law on Data Privacy and Security

Depository institutions, including credit unions, have long been subject to a framework of laws and regulations designed to ensure a high standard of consumer privacy and data security. Central to this framework is Title V of the GLBA, which acknowledges the need

for heightened care when handling sensitive consumer financial information and provides well-established standards for addressing consumer privacy concerns. Other laws, such as the Fair Credit Reporting Act (FCRA) and Right to Financial Privacy Act (RFPA) have also operated to protect credit union member privacy for nearly 50 years.

America's Credit Unions believes that the GLBA should remain the model for depository institution compliance with any future federal data security and privacy standard.

The GLBA mandates specific disclosure of how nonpublic personal information is collected and shared by financial institutions. The Consumer Financial Protection Bureau's (CFPB) Regulation P implements the GLBA's privacy provisions. It requires disclosures of privacy policies, places limits on sharing certain information for marketing purposes, and gives consumers the right to opt out of certain types of information sharing with nonaffiliated third parties.¹ In addition to an initial privacy notice, credit union members receive an annual notice describing their credit union's privacy policy which outlines, among other things, the types of information sharing individual members can decline.

In general, federal law gives credit union members the right to decline sharing creditworthiness information for affiliates' everyday business purposes, the use of information by affiliates for marketing purposes, and the sharing of information with nonaffiliates for marketing purposes.² Under Regulation P, if a credit union changes its policies and practices regarding disclosures to nonaffiliated third parties so that its most recent notice is inaccurate, then the credit union may not begin disclosing the information until it provides revised privacy notices and opt-out procedures.³

Additionally, credit unions, like many financial institutions, have long prioritized investments in data security to ensure that their members' privacy is protected. The GLBA requires financial regulators to implement technical safeguards to ensure that financial

¹ See 12 CFR Part 1016.

² See Appendix to Part 1016 - Model Privacy Form.

³ See 12 CFR 1016.8.

institutions are protecting their customers' information.⁴ These safeguards are comprehensive and designed to ensure the (i) security, (ii) confidentiality, (iii) integrity, (iv) and proper disposal of consumer information and other records. Under the rules promulgated by the National Credit Union Administration (NCUA) for credit unions, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require credit unions to ensure that third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

The NCUA also demands regular risk assessments of data security programs, as well as mechanisms to address incidents of unauthorized access to sensitive member information. While the threat of incurring reputational injury already provides a significant incentive to guard member data closely, numerous legal obligations and volumes of regulatory guidance also operate to protect member data.

The NCUA's data security rules are supplemented by a large body of regulatory guidance developed by the Federal Financial Institutions Examination Council (FFIEC) that takes the form of booklets covering various information security topics. The FFIEC, which is comprised of various banking regulators, including the NCUA, has devoted hundreds of pages of guidance to the topics of IT security, architecture, infrastructure and operations, audits, and many other topics. For example, the FFIEC has advised its regulated financial institutions to "restrict and monitor data extraction" and limit the ability to view or modify data to only what is necessary to carry out job responsibilities and automated functions—principles of access control that help achieve the goal of data minimization.⁵

The FFIEC has also documented numerous security controls such as employing an appropriate level of encryption on data in transit and data at rest based on the type and criticality of the information. In the domain of data analytics, the FFIEC has advised regulated financial institutions to identify "processes to remove or destroy data when no

⁴ See 12 CFR Part 748.

⁵ See FFIEC, Architecture, Infrastructure and Operations, 18-19 (2021), *available at* https://ithandbook.ffiec.gov/media/ywfm2ftz/ffiec_itbooklet_aio.pdf.

longer used in the data analytics tools.” Collectively, these principles and controls, along with many others too numerous to name, contribute to a robust data security environment that is designed to guard the privacy of credit union members’ nonpublic personal information.

In addition to the large volume of regulatory guidance derived from the safeguards provisions of the GLBA, examination-based supervision provides another important layer of protection. Not all financial institutions, as defined under the GLBA, are subject to periodic examination by a functional regulator like the NCUA. That difference matters in terms of how a future federal privacy framework accounts for the rigor and scope of existing compliance. It is also a key reason why America’s Credit Unions supports a clear entity-level exemption for credit unions subject to the GLBA.

Key Elements and Issues in Any Future Data Privacy Regime

As Congress considers potential reforms to data privacy and security, there are various aspects we believe should be included or addressed:

An Entity Level Exemption is Appropriate for Depository Institutions

In the context of a future federal privacy framework, an entity-level exemption would recognize the rigor of existing financial institution compliance activities and allow the prudential financial regulators and CFPB, as appropriate, to tailor supervision based on changing privacy or data security risks. An entity-level exemption for financial institutions, such as credit unions, would also address administrability concerns often associated with alternative frameworks that offer only a data-level exemption.

For context, the less preferred data-level exemption typically operates on the principle that specific types or uses of data addressed by other federal laws can be set aside as adequately regulated. However, a data-level exemption provides limited relief in practice. This is because the extent of relief is confined to narrow categories or uses of data which must be matched to federal statutory language.

Unfortunately, the GLBA and other federal privacy laws were written decades ago, and do not articulate in detail all the types of data or data processing activities relied upon by credit unions today. Supervisory guidance developed by the FFIEC and the NCUA supplement the GLBA, but the statutory language itself tends to focus on high level aspects of information exchange. As a consequence, even understanding the scope of a data-level exemption can be a complex undertaking because it requires a credit union to reconcile uniquely defined categories of data with federal laws, which may not afford great specificity. For example, this could require a credit union to grapple with uniquely defined categories of data and perform a top to bottom inventory of every data element being processed by the credit union or any of its affiliates. That consumes time and resources that could be better spent delivering affordable credit to Americans, particularly those in rural and underserved communities.

Recognizing these challenges, various state legislatures have adopted entity-level exemptions in their own privacy laws for financial institutions that comply with the GLBA. Some states have opted for a combination of data-level and entity-level exemptions for added flexibility.

The American Privacy Rights Act from the 118th Congress took the approach of recognizing an exemption for financial institutions but only to the extent of *compliance* with existing federal data privacy or data security laws and only “with respect to the activities governed by the requirements of such law or regulation.”⁶ While this arrangement would have potentially spared certain financial institutions from conflicting provisions related to affiliate data sharing, opt-out procedures, and delivery of disclosures, it would not have covered other uses of data. This left the door open for introducing new compliance procedures for data used in conjunction with artificial intelligence, or data portability standards and any other areas not specifically addressed by the GLBA.⁷ Such a limited exemption would have done little to spare credit unions

⁶ See e.g., Sec. 118(b)(3) of H.R.8818 - American Privacy Rights Act of 2024 [introduced].

⁷ See e.g., Sec. 105 of H.R.8818 - American Privacy Rights Act of 2024.

from the additional compliance costs and burdens associated with analyzing data processing activities not specifically enumerated by the GLBA.

Delegation of Authority to Appropriate Sectoral Regulators

The oversight of credit unions, banks, and other depository institutions is best left to the functional financial institution regulators that have experience in this field. America's Credit Unions does not support an approach to federal privacy regulation which grants overlapping supervisory authority to a secondary agency that does not have direct experience examining credit unions.

For example, the NCUA is the sole regulator equipped with the requisite knowledge and expertise to regulate credit unions. The NCUA is well versed in the unique nature of credit unions and has served as the primary regulator for credit unions since its inception. As such, in the area of privacy enforcement, the NCUA should be the primary regulator of credit unions and collaborate with other regulators on joint rulemaking when necessary. With the appropriate regulatory authority, the NCUA can ensure credit unions maintain a safe and sustainable information system.

Preemption of State Laws is Necessary

For financial institutions already shouldering high compliance burdens associated with examination-based supervision, an entity-level exemption is just one essential component for any comprehensive federal privacy framework. Preemption of a conflicting patchwork of state laws is also needed.

Today's patchwork of state privacy laws has invited idiosyncratic approaches to data processing activities and technologies. Some states, by choosing to recognize only a data-level exemption, have placed strains on credit unions by demanding more complex procedures, such as performing a comprehensive inventory of all institution-held data, in order to comply with specific disclosure requirements. The resulting compliance burdens, magnified each time a new state law is passed, siphon resources away from service to consumers and the core lending activities of credit unions.

Some previous legislative proposals for comprehensive federal privacy legislation contemplated preemption of state laws, but the inclusion of numerous exceptions greatly eroded the intended relief. For example, preservation of state laws related to regulating deceptive, unfair, or unconscionable practices could have easily circumvented intended areas of preemption given that the analysis relied upon when identifying “unconscionable” practices tends to invite jurisdictional expansion—a phenomenon we have witnessed from regulators in the past.⁸

Federal preemption carveouts intended to accommodate state rules for reporting cyber incidents could also give rise to inconsistencies and perpetuate administrative compliance over actual response and recovery activities if an institution does suffer a cyber incident. Credit unions must already notify members “as soon as possible” under Part 748 of the NCUA’s regulations if sensitive member information is accessed by an unauthorized party, and must notify the NCUA within 72 hours if the credit union or a third party handling credit union systems or data experiences a substantial cyber incident. Credit unions are also covered by the Cyber Incident Report for Critical Infrastructure Act and are likely to face additional implementing regulations promulgated by the Cybersecurity and Infrastructure Security Agency later this year.

The purpose of a comprehensive federal privacy standard is to synthesize the current patchwork data protection laws under a uniform national standard. Financial institutions must be able to effectively serve their members across jurisdictions and should not be exposed to the unnecessary compliance burdens of potentially 50 different privacy laws in 50 different states. Even though some existing federal privacy laws do not preempt state laws, there are numerous examples of preemption in existing federal privacy law. Currently, at least three federal privacy statutes have preemption provisions under which states may not regulate the specific area of law covered or enact laws that impose additional requirements or prohibitions. For example, the Children’s Online Privacy Protection Act, the CAN-SPAM Act, and the FCRA all have some state preemption

⁸ See e.g., American Privacy Rights Act.

provision.⁹ The purpose of privacy and cybersecurity laws is only achievable if the protections put in place are both comprehensive and consistent. Without consistent privacy and data security requirements in place, bad actors will simply identify the jurisdictions with the weakest or no requirements and use organizations in those jurisdictions for entry into interconnected networks across the country.

Complexity of Data Deletion

Certain features of proposed privacy frameworks, such as prohibitions on collecting certain types of metadata without consumer opt-in, or a broad right of deletion, similar to what is found in the EU’s General Data Protection Regulation (GDPR), can frustrate efforts to comply with recordkeeping rules, or to detect and prevent fraud.

Data deletion requirements are particularly challenging for credit unions and other financial institutions that are subject to various recordkeeping requirements. For example, Regulation E requires any person subject to the Electronic Fund Transfer Act (EFTA) to retain evidence of compliance with the EFTA’s requirements for a period of not less than two years from the date disclosures are required to be made or action is required to be taken.¹⁰

Given that compliance with Regulation E practically demands retention of customer transaction data as well as other information that might bear upon the validity of a transaction (e.g., IP address, geolocation, device data, etc.), deletion of such information may frustrate a credit union’s ability to demonstrate that it relied upon appropriate sources of data when investigating an allegedly unauthorized electronic fund transfer. However, the EFTA’s provisions related to investigations of transactions or errors do not necessarily demand the collection of transactional metadata—those are practices adopted by practical necessity. The distinction is critical because states that have adopted data deletion rights sometimes condition exceptions to that right on the existence of a “legal obligation” or a specific type of security related activity.¹¹ The EFTA’s error resolution and

⁹ See 15 U.S.C. §§ 6501–6506; 15 U.S.C. §§ 7701–7713; 15 U.S.C. § 1681t(a).

¹⁰ See 12 CFR 1005.13(b).

¹¹ See e.g., California Consumer Privacy Act, Cal Civ. Code 1798.105(d).

investigation requirements, which influence the extent of financial institution liability, are retrospective analyses (meaning they do not prevent fraud in a direct sense) and do not obligate collection of data—so the application of such an exception would be unclear, at best.

Likewise, for credit unions, the NCUA’s regulation implementing the Truth in Savings Act (TISA) provides that a credit union shall retain evidence of compliance for a minimum of two years after the date disclosures are required to be made or action is required to be taken. TISA’s rules regarding consumer advertising may incentivize a credit union to retain technical information about how advertisements are deployed across digital channels, which may involve collection of device and IP address information from consumers. While there is no requirement in TISA that would obligate a credit union to collect or retain metadata about such interactions, it may be useful information to have for documenting compliance. While some privacy frameworks carve out data deletion exceptions for certain internal uses of data, undertaking the analysis to determine whether a particular use is “reasonably aligned with the expectations of the consumer” or “compatible with the context in which the consumer provided the information” can involve significant and repeated analysis. As noted previously, the rigor of existing examination-based supervision already ensures that the use of data complies with privacy and security safeguards established under the GLBA and Part 748 of the NCUA’s regulations.

Broad data deletion rights can also greatly complicate the ability of financial institutions to deploy artificial intelligence (AI) which is trained on consumer transactional history, interactions, or other behavioral characteristics. The discrete events which may involve collection of consumer data will not always implicate an obvious security concern—for example, transcribing a routine customer service interaction—but the historical value of this data is important for retrospective analysis when developing tools to detect anomalous behavior and fraud. Because AI fraud models work best when they understand both normal and abnormal behavior, a patchwork of data deletion rights coupled with idiosyncratic exceptions could impair the usefulness of such technology. It may also be impractical for a credit union that has ingested certain types of training data within a fine-

tuned model to selectively delete information without having to incur the enormous expense of retraining the model from scratch using a new data set every time historical information is removed. Simply put, data deletion requirements done haphazardly could hinder efforts of financial institutions to protect consumers and fight fraud.

Opt-In vs. Opt-Out

The GLBA and Regulation P generally operate to limit sharing of sensitive consumer information through an opt-out process, something we believe should continue and be the standard for financial institutions in any future data privacy regime.

Safe Harbor

A comprehensive federal data privacy framework should provide for principles-based requirements and offer a safe harbor for businesses that take the appropriate steps to comply with the law.¹² For example, the guidelines in the NCUA's Part 748 require credit unions to develop and implement an information security program that includes board approval; oversight and reporting; the assessment, management, and control of appropriate risks surrounding the security of member information; and regular testing and appropriate adjustment of the program. This risk-based approach is appropriate because it requires organizations to assess their own risks and implement protections proportionate to those risks. A prescriptive requirement will necessarily result in a misalignment between the risk to the consumer and the organization and the protections put in place. In general, a financial institution subject to the GLBA that develops tailored privacy and data security processes and procedures based on an appropriate risk assessment should be found to be in compliance with the law.

Private Right of Action

Some state privacy laws and proposed federal privacy legislation have incorporated a private right of action which permits consumers to sue businesses if they fail to comply with specific rules related to safeguarding information. In general, consumers can already bring causes of action against businesses when they suffer injuries related to the

¹² See 15 U.S.C. § 7707(b)(1).

mishandling of data. Those causes of action have traditionally relied upon theories of negligence or breach of contract. A federal private right action would be distinguishable insofar as it could invite lawsuits more focused on compliance violations rather than evidence of actual injury or economic loss. A private right of action would also perpetuate gradual variances in judicial interpretations, undermining the purpose of preemption by establishing different tests for assessing injury or harm.

Some have critiqued the private right of action as inviting trial lawyers to extract lucrative settlements from businesses based on perceived lapses in compliance. It is not uncommon for financial institutions to agree to settlement, even if they have committed no wrong, simply due to the costs of protracted litigation and discovery involving the accounts of potentially millions of consumers. America's Credit Unions has serious concerns with any broad private right of action due to the risk of frivolous lawsuits being filed against credit unions which are already held accountable for compliance violations by their regulator, the NCUA, as well as the CFPB. Furthermore, it is unlikely that a private right of action would offer any meaningful enhancement to the enforcement jurisdiction of the NCUA, which already requires credit unions to report incidents involving unauthorized access to member information to both supervisory points of contact as well as affected members. Adding additional costs to credit unions, and ultimately their members, through contending with lawsuits under an expansive private right of action would do little to improve compliance with the law, while doing more to hinder their ability to provide services to their members.

Conclusion

Stringent information security and privacy practices have long been a part of the financial services industries' business practices and are necessary as financial services are entrusted with consumers' nonpublic personal information. Still, the financial marketplace is evolving. While not the subject of today's hearing, issues such as open banking and AI will interplay with privacy issues in the future. Protection of consumer financial information is an important tenet of the financial services industry. This responsibility is reflected in the strong information security and privacy laws that govern data practices for the financial services industry as set forth in the GLBA, RFPA, FCRA

and other federal laws and regulations. The GLBA's technical safeguards and privacy protections are strengthened by federal and state regulators' examinations, implementing regulations, and robust enforcement for violations of the GLBA's requirements.

Ultimately, America's Credit Unions believes that when considering a comprehensive future federal privacy framework, Congress should prioritize the following features:

- A recognition of GLBA standards and accompanying regulations in place for financial institutions through the adoption of an entity-level exemption;
- Strong federal preemption from the myriad of various state laws for those in compliance with federal privacy and GLBA standards; and
- Protection from frivolous lawsuits created by a private right of action

We look forward to working with you to achieve such a framework.

Thank you for holding this important hearing and the opportunity to appear before you today. I welcome any questions you may have.

Chairman BARR. Thank you, Mr. Morris.
 Ms. Kuehn, you are now recognized for 5 minutes.

**STATEMENT OF REBECCA KUEHN, PARTNER, HUDSON COOK,
 LLP**

Ms. KUEHN. Good morning. Chairman Barr, Chairman Hill, Ranking Member Foster, and members of the subcommittee, thank you for the opportunity to testify today.

I am Rebecca Kuehn. I am a Partner at Hudson Cook, where I lead our credit reporting, data privacy, and data security practice. I formerly served as an Assistant Director at the Federal Trade Commission, where I led efforts related to financial privacy and data security.

Today, I am appearing in my own capacity and not on behalf of my firm or any client.

We are here today to consider the framework governing financial data privacy.

The United States has a longstanding tradition of financial privacy protection that balances consumer rights, market innovation, and regulatory oversight. This balance is important to consumers and the financial system.

The cornerstone of the financial privacy regulation is the Gramm-Leach-Bliley Act, or the GLBA. It requires financial institutions to provide consumers with clear privacy notices explaining what personal information is collected and how it is shared, to offer consumers with the right to opt out of certain types of data-sharing with nonaffiliated third parties, and to implement safeguards to protect the confidentiality and security of consumer financial information.

The GLBA defines “nonpublic personal information” broadly, and it applies to a wide range of entities engaged in financial activities, from banks to auto dealers, ensuring consistent privacy standards across the financial services landscape.

Through what are known as the 502(e) exceptions, the GLBA also recognizes that certain forms of data-sharing are critical to enabling core financial functions such as fraud prevention and public safety. These include disclosures necessary to process transactions, disclosures made with the consumers’ consent, and disclosures meant to prevent fraud or unauthorized transactions. These types of sharing do not require an opt-out because GLBA draws a clear line between essential, operational, and service needs and marketing and other nonessential sharing, where an opt-out is required.

As of 2015, financial institutions that share data only within these carefully crafted exceptions are no longer required to provide duplicative annual notices to consumers as long as they have not changed their privacy practices. This change in GLBA reduces regulatory burden and has incentivized companies to limit their sharing to only those essential purposes. This benefits both consumers and the industry.

I recognize there is a larger discussion about data on consumers and privacy. However, recent proposals, such as the CFPB’s data broker rule, risk undermining this careful balance. The CFPB’s rule proposed to reclassify certain identity and address information

governed by the GLBA as information under the Fair Credit Reporting Act (FCRA) and would have limited the ability of companies to use GLBA information for a number of core purposes, such as fraud prevention.

The proposal came out of a concern about misuse of consumer data, but the proposal conflated the responsible, regulated use of financial data by institutions that serve essential functions with very different and concerning practices of bad actors, such as entities who sell sensitive geolocation data on military personnel.

This conflation is problematic. It overlooks the fact that GLBA-covered entities are already subject to comprehensive privacy and security obligations and that the types of sharing permitted under the GLBA are vital for protecting consumers against fraud and ensuring public safety.

As this subcommittee continues to examine financial privacy, I urge a careful, fact-based approach, one that recognizes the distinction between the well-regulated financial data use and the more opaque or harmful practices of unregulated bad actors.

Oversight and modernization are appropriate, but they should not come at the cost of undermining core consumer protections or essential financial system functions.

I thank you for your attention, and I look forward to your questions.

[The prepared statement of Ms. Kuehn follows:]

**Statement of Rebecca E. Kuehn
Partner, Hudson Cook, LLP**

**Subcommittee on Financial Institutions
Committee on Financial Services
United States House of Representatives**

**Hearing on “Framework for the Future:
Reviewing Data Privacy in Today’s Financial System”**

June 5, 2025

Chairman Barr, Ranking Member Foster, and members of the Subcommittee, thank you for the opportunity to appear before you. My name is Rebecca E. Kuehn, and I am a partner at the law firm Hudson Cook, LLP, where I chair the Credit Reporting, Privacy, and Data Security Practice Group. Earlier in my career, I worked at the Federal Trade Commission (FTC), where I was Assistant Director of the Division of Privacy and Identity Protection in the Bureau of Consumer Protection, which oversees issues related to consumer privacy, credit reporting, identity theft, and information security. While I was at the FTC, I supervised investigations into compliance with the Gramm-Leach-Bliley Act Privacy and Safeguards Rules, and I participated in an interagency research project to develop a model privacy notice for complying with the Gramm-Leach-Bliley Act Privacy Rule. I led the Fair Credit Reporting Act program, and I oversaw the Commission’s enforcement, outreach, and rulemaking activities in that area. I also oversaw investigations and enforcement actions involving the application of Section 5 of the FTC Act, which sets forth the prohibition against unfair and deceptive acts and practices.

I have been privileged to work in the area of consumer financial services on all sides – on behalf of financial services clients, as in-house counsel for companies, and at the FTC. Today, I am appearing in my own capacity, and not on behalf of my firm or any client of the firm.

Thank you for the opportunity to appear before you today to discuss the framework of financial privacy laws in the United States and the important protections they provide to consumers. The United States has a longstanding, though sectoral, tradition of financial privacy protection that balances consumer rights, market innovation, and regulatory oversight.

I. Overview of Financial Privacy Laws

The legal framework for financial privacy in the United States is primarily grounded in the following key statutes:

1. The Gramm-Leach-Bliley Act (GLBA) – 1999

The GLBA is the cornerstone of federal financial privacy regulation. It requires financial institutions to:

- Provide consumers with clear privacy notices explaining what personal information is collected and how it is shared.
- Offer consumers the right to opt out of certain types of data sharing with non-affiliated third parties.
- Implement safeguards to protect the confidentiality and security of consumer financial information.

It also places limits on the use and further disclosure of personal information any entity receives from a financial institution.

The GLBA defines “nonpublic personal information” broadly to include any data provided by a consumer to obtain financial products or services or otherwise obtained in connection with consumer financial products or services, and it imposes disclosure and consent obligations that limit how this data may be shared. “Nonpublic personal information” can include information as limited as a list of customers of a financial institution.

Under the GLBA, the definition of “financial institution” is equally broad to reflect the wide range of entities engaged in financial activities. It includes not only traditional banks, credit unions, and insurance companies, but also non-bank companies that provide financial products or services to consumers, such as mortgage lenders, payday lenders, investment advisers, and even retailers that issue credit cards or finance purchases or automobile dealers involved in the financing of vehicles. This definition encompasses any business that is “significantly engaged” in financial activities. This expansive scope ensures that consumer financial information is protected regardless of the type of entity handling it, thereby promoting consistent privacy standards across an increasingly complex and diversified financial services landscape.

One of the primary responsibilities of the GLBA, set forth in the Privacy Rule, is the requirement of financial institutions to inform consumers and customers (consumers with whom the financial institution establishes an ongoing relationship) of their privacy practices. To facilitate this, the FTC, in coordination with other federal agencies, developed a model privacy notice. This notice was developed following extensive consumer research to ensure that privacy disclosures were both clear and effective. This research included large-scale qualitative testing, cognitive interviews, and quantitative consumer surveys designed to assess how well individuals could understand and use privacy notices. The agencies tested various notice formats, wording, and layouts to determine what most effectively conveyed key information about financial institutions’ data-sharing practices and consumer choices. Results consistently showed that many existing privacy notices were overly complex, leading to confusion and poor comprehension among consumers. The research supported the use of plain language, simplified structure, and a tabular format that allowed for easy comparison and comprehension. The final model notice, which was issued jointly by the FTC, Federal Reserve Board, and other federal banking

agencies, reflected the best practices identified through this empirical work. In testimony before Congress, the FTC emphasized that this evidence-based approach significantly improved the usability and transparency of privacy notices, helping consumers make more informed decisions about how their personal financial information is shared. The Commission also underscored the broader importance of continuing to apply consumer research in crafting effective privacy policies, particularly as financial services and technologies evolve.

The GLBA Privacy Rule requires that financial institutions offer consumers the ability to opt out of sharing information with non-affiliated third parties unless that sharing is permitted under certain defined exceptions. These exceptions are designed to allow necessary and legitimate information sharing for operational, legal, and compliance purposes. For example, financial institutions may disclose information to service providers performing functions on their behalf, to comply with legal or regulatory requirements, to prevent fraud or unauthorized transactions, or in connection with a proposed or actual sale, merger, or transfer of business assets. Importantly, these disclosures are permitted without consumer consent only when they serve specific, limited purposes that support the integrity and functionality of the financial system. These exceptions (referred to as 502(e) exceptions) strike a critical balance between protecting consumer privacy and allowing financial institutions the flexibility needed to operate effectively and responsibly.

The GLBA generally requires that financial institutions provide an annual privacy notice (with the ability to opt out) to their customers. In 2015, Congress amended the GLBA through the enactment of the Fixing America's Surface Transportation (FAST) Act, which included a provision eliminating the requirement for financial institutions to send annual privacy notices to consumers under certain conditions. Specifically, if a financial institution only shares nonpublic personal information in ways that do not require an opt-out under the GLBA (such as the sharing

permitted under the 502(e) exception) and has not changed its privacy policies or practices since the last notice, it is no longer obligated to provide an annual notice. This amendment was intended to reduce unnecessary regulatory burdens and consumer confusion caused by repetitive disclosures, while maintaining strong privacy protections. By streamlining compliance requirements without weakening privacy standards, the amendment reflects a practical balance between effective consumer communication and operational efficiency for financial institutions.

The GLBA Safeguards Rule requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect the confidentiality and integrity of customer information. Updated in 2021, the rule mandates that covered entities assess internal and external risks, designate a qualified individual to oversee the program, implement access controls, encrypt customer data, and regularly test and monitor systems. The rule also requires institutions to oversee service providers and adjust safeguards based on evolving threats. This regulation plays a critical role in ensuring consumer trust by holding financial institutions accountable for protecting sensitive personal data against ever-changing cybersecurity risks.

2. The Fair Credit Reporting Act (FCRA) – 1970

The FCRA regulates how consumer credit information is collected, accessed, and used. It ensures:

- Consumers are informed when their credit reports are used to take adverse action.
- Consumers have the right to access their credit reports and dispute inaccuracies.
- Strict controls are in place to limit who can access consumer reports and under what circumstances.

The FCRA also provides further protections against identity theft, including the right of a consumer to place a security freeze on their credit reports, and requires entities to properly dispose of sensitive consumer data.

3. The Right to Financial Privacy Act (RFPA) – 1978

This law protects the privacy of financial records by prohibiting federal government agencies from accessing personal financial information without the customer's consent or a lawful subpoena, summons, or search warrant.

4. State Laws

State privacy laws, such as the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), have introduced broader data privacy rights for consumers; however, they also include important exemptions for data already governed by federal laws like the GLBA. Specifically, these state laws generally exempt personal information collected, processed, sold, or disclosed pursuant to the GLBA. This means that data already protected under the GLBA's privacy and safeguarding provisions is typically not subject to overlapping state requirements. These exemptions aim to avoid duplicative regulation and legal uncertainty, while recognizing that the GLBA already establishes a robust federal framework for financial data privacy.

II. How These Laws Protect Consumers

Collectively, these statutes provide meaningful protections to consumers, including:

- **Transparency:** Financial institutions must clearly inform consumers about data collection and sharing practices.

- Control: Consumers can limit how their information is shared with third parties.
- Access and Correction: Consumers have the right to access and correct credit and financial data held by consumer reporting agencies.
- Security: Institutions are required to safeguard sensitive information and protect it from unauthorized access or use.
- Government Oversight: Agencies such as the CFPB and FTC have authority to enforce privacy protections and penalize noncompliance.

These protections are essential to maintaining consumer trust in the financial system and preventing misuse of sensitive financial data.

Conclusion

Financial privacy laws in the United States provide a strong foundation for protecting consumers' personal information. They promote transparency, empower individuals with rights over their data, and require financial institutions to uphold rigorous standards of care.

* * *

Thank you again for the opportunity to testify before you today. I am happy to answer any questions.

Chairman BARR. Thank you.

Ms. Huddleston, you are now recognized for 5 minutes.

**STATEMENT OF JENNIFER HUDDLESTON, FELLOW IN
TECHNOLOGY POLICY, CATO INSTITUTE**

Ms. HUDDLESTON. Thank you.

Chair Barr, Ranking Member Foster, and distinguished members of the House Committee on Financial Services Subcommittee on Financial Institutions, my name is Jennifer Huddleston, and I am a senior fellow in Technology Policy at the Cato Institute.

My research focuses on the intersection of law and technology, including its use related to data privacy. Therefore, I welcome the opportunity to testify regarding data privacy in today's financial system.

In this testimony, I will focus on three key points.

First, data privacy in sensitive areas, such as financial services, is already regulated by existing law.

Second, as State or a potential Federal data privacy law continues to emerge, careful attention should be paid to the way they may interact with or conflict with these existing laws and what a patchwork might mean regarding the burden particularly on small players. This is additionally true if enforcement mechanisms, such as private rights of action for statutory damages, could significantly raise the risk of costly litigation.

Finally, I wish to discuss how any conversations around data privacy should consider the impact on innovation, consumer choice, and smaller players, as well as how such laws could interact with or hinder the deployment of potentially better solutions when it comes to data privacy and data security.

So, to begin with, some have criticized the United States as a sort of Wild West when it comes to data privacy. Instead, the United States' approach has been better understood as responding with regulation for particularly vulnerable or sensitive data where consumers may be more likely to face harms should it be abused or insecure, such as the financial services sector.

In this regard, the financial services sector already has consumer-focused data privacy laws, including the Gramm-Leach-Bliley Act that regulates the personal data of consumers held by financial services forums and the Fair Credit Reporting Act that regulates consumer credit data from credit reporting agencies.

To my second point, the potential interactions between comprehensive data privacy laws at both the State and Federal level and the financial services sector, it is important to understand how general consumer privacy laws could impact this already-regulated data. Additional data privacy laws could further add to the regulatory burden or conflict with existing laws.

As the chair mentioned in his opening statement, an emerging patchwork of State laws that are both sector-specific and general in their application could make this more difficult to navigate, with at least 19 States having passed comprehensive consumer privacy laws and more debating similar legislation each year.

While many of these State consumer privacy laws have a carve-out for existing regulated data under laws like the FCRA and the GLBA, this does not mean they do not impact or create potential

conflicts for the financial services sector or financial data. This can include conversations around different definitions of “particularly sensitive data,” including financial information or personally identifiable information, and the timelines and steps that entities must take to respond to consumer requests or potential issues. These conflicts can be particularly felt by smaller and more innovative entities who have to navigate various definitions.

Additionally, such laws provide an example of the impact that different enforcement mechanisms, including private rights of actions with statutory damages, could have in deterring innovation and particularly in already-regulated or risk-averse sectors.

While not related to financial data, for example, the Illinois Biometric Information Privacy Act has such a mechanism, and it is illustrative of the problems such enforcement can create even in data considered particularly sensitive. Because of statutory damages and private right of action, this law has resulted in significant claims against companies ranging from popular social media apps like Meta to Six Flags amusement park, but more for violation than for any actual harm occurring to consumers.

Finally, I would like to spend my last minute discussing how privacy law and innovation can potentially conflict.

While recognizing the specific risks of economic harm and sensitivity of financial data is logical, law is static and innovation is dynamic. This yields the potential need for review of regulation to allow improvements in data privacy security and innovation, as various technologies might provide alternatives that are more protective of privacy and provide better services to consumers who opt in but might not meet the existing definitions.

There are three ways existing data privacy regulation might deter innovation that I would like to highlight.

First, many laws are developed for earlier technologies. This may make it more difficult to use more secure technologies like blockchain that could actually create greater privacy and security for consumers.

Second, enforcement mechanisms around private right of action or the need for government approval could deter companies of all sizes, but particularly smaller companies, from trying to find innovative ways to protect data.

Finally, artificial intelligence may require us to rethink our existing frameworks around data usage, retention, and minimization, including in regulated industries like the financial services sector.

I thank you for your time, and I welcome your questions.

[The prepared statement of Ms. Huddleston follows:]



Statement

of

Jennifer Huddleston

**Technology Policy Senior Fellow
Cato Institute**

before the

**Subcommittee on Financial Institutions
Committee on Financial Services
United States House of Representatives**

June 4, 2025

**RE: "Framework for the Future: Reviewing Data Privacy in Today's Financial
System"**

Chair Barr, Vice-Chair Loudermilk, Ranking Member Foster, and distinguished members of the House Committee on Financial Services Subcommittee on Financial Institutions:

My name is Jennifer Huddleston, and I am a senior fellow in technology policy at the Cato Institute. My research focuses primarily on the intersection of law and technology, including issues related to data privacy. Therefore, I welcome the opportunity to testify regarding data privacy in today's financial system.

In this testimony, I will focus on three key points:

- First, data privacy in sensitive areas such as the financial services sector is already regulated by existing law;
- Second, as state or potential federal data privacy laws continue to emerge, careful attention should be paid to the way they may interact with or conflict with existing law in such regulated industries and what this patchwork might mean regarding the burden on small players, particularly if there are enforcement mechanisms such as private rights of action for statutory damages that could significantly raise the risk of costly litigation;
- Finally, any conversations around data privacy should consider the impact on innovation, consumer choice, and small players, as well as how such laws could interact with or hinder the deployment of better solutions.

Understanding Existing Data Privacy Law in the Financial Services Sector

Because of the lack of a comprehensive federal data privacy law, some have criticized the United States as a sort of wild west when it comes to data privacy. Instead, the United States' approach has been to respond with regulation for particularly vulnerable or sensitive data where consumers would be more likely to face harm should it be abused or insecure. These laws are more narrowly focused on the consumer data experience and data privacy or security within these areas or

industries.¹ The financial services sector, for example, already has consumer-focused data privacy laws, including the Graham-Leach-Bliley Act (GLBA) that regulates the personal data of consumers held by financial services firms and the Fair Credit Reporting Act (FCRA) that regulates consumer credit data from credit reporting agencies.

My testimony in this hearing will focus on consumer privacy; however, a number of laws and regulations, including the Bank Secrecy Act, require reporting from financial services firms and allow warrantless government access to information about individuals' financial transactions. My Cato colleagues in our Center for Monetary and Financial Alternatives have explored the need for reform to protect individuals' financial privacy from government surveillance and to ensure that individuals' Fourth Amendment rights are respected.²

Potential Interactions Between Comprehensive Data Privacy Laws in Financial Services

Consumer privacy in the financial sector has been regulated for several decades. Additional data privacy laws, however, could further add to a regulatory burden or conflict with existing laws. An emerging patchwork of laws that are both sector-specific and general in their applications will make it more difficult for smaller or more innovative players to navigate. To date, at least 19 states have passed comprehensive consumer privacy laws, with many more debating such legislation.³ In addition, there is an ongoing effort to pass general federal consumer privacy legislation.⁴ This is resulting in the emergence of a concerning patchwork that can be

¹ Alan McQuinn, "[Understanding Data Privacy](#)," *RealClearPolicy*, October 25, 2018.

² Norbert Michel, "[Experts Agree That Financial Privacy Needs A Revamp](#)," *Forbes*, September 16, 2024 and Jennifer Schulp, "[Financial Privacy Is Under Fire — The Issue Should Draw the Attention of Both Parties](#)," *The Hill*, August 26, 2024.

³ Jennifer Schulp, "[Financial Privacy Is Under Fire — The Issue Should Draw the Attention of Both Parties](#)," *The Hill*, August 26, 2024.

⁴ See Office of Chairman Brett Guthrie, "[Chairman Guthrie and Vice Chairman Joyce Issue Request for Information to Explore Data Privacy and Security Framework](#)," *House Energy and Commerce Committee*, February 21, 2025.

problematic and confusing for both consumers and regulated entities who are unsure of the requirements or rights when data inevitably involves interactions in multiple states.⁵

Even when such laws are modeled on one another, there could be significant differences that can cause potential conflicts. While most state consumer privacy laws have carve-outs for data already regulated under laws like the FCRA and GLBA, this does not mean that they do not potentially impact or create other conflicts for the financial services sector or financial data.⁶ This can include the definitions of particularly sensitive data — including financial information — and the timelines and steps entities must take to respond to consumer requests or potential issues. These conflicts can be particularly felt by smaller or more innovative entities who will have to navigate various definitions.

Additionally, enforcement mechanisms around private rights of action for statutory damage could deter innovation, particularly in an already highly regulated and risk-averse sector. While not related to financial data, the Illinois Biometric Information Privacy Act has such a mechanism and is illustrative of the problems such enforcement can create, even in data considered particularly sensitive. Because of statutory damages and private right of action, the law has resulted in significant claims against companies based not on actual injury, but mere violation and recovery for the attorneys bringing such actions.⁷ Additionally, this potential has

⁵ See Jennifer Huddleston and Gent Salihu, “[The Patchwork Strikes Back: State Data Privacy Laws after the 2022–2023 Legislative Session](#),” *Cato at Liberty (blog)*, July 6, 2023.

⁶ Consumer Financial Protection Bureau, [State Consumer Privacy Laws and the Monetization of Consumer Financial Data](#) (Consumer Financial Protection Bureau, November 2024).

⁷ See U.S. Chamber of Commerce Institute for Legal Reform, [A Bad Match: Illinois and the Biometric Information Privacy Act](#) (U.S. Chamber of Commerce Institute for Legal Reform, October 2021).

deterred the launch of certain innovative products that might create positive consumer experiences or even improve security.⁸

How Privacy Law and Innovation Could Conflict

While recognizing the specific risks of economic harm and the sensitivity of financial data is logical, law is static and innovation is dynamic, yielding the potential need to review regulation to allow improvements in data privacy, security, and innovation as various technologies might provide alternatives that are more protective of privacy or provide better services to consumers who opt in but might not be able to comply. While consumers value privacy, they also enjoy the improvements and personalized services we have come to expect through data usage. This includes the financial services sector both for its ability to use data to improve consumer security through actions like fraud detection and to better serve its customers.

When it comes to the financial services industry, there are three ways existing data privacy regulation might deter innovation that I'd like to highlight. First, many data privacy laws were created with earlier technologies in mind. This may make it more difficult to use more secure technologies like blockchain or even cloud computing and could also create greater privacy risks through retention requirements than are truly necessary.⁹ Second, enforcement mechanisms around private rights of action or the need for government approval could deter companies of all sizes from trying innovative ways to use or protect data. Finally, artificial intelligence may require us to rethink our existing frameworks around data usage, retention, and minimization.¹⁰

⁸ Amy Korte, "[A New Feature on Google's Arts & Culture App Is Not Available to Illinois Users Because of the State's Strict Biometric Privacy Law](#)," *Illinois Policy*, January 23, 2018 and see Joseph J. Lazzarotti et al., "[From Time Keeping to Dashcams, BIPA Litigation Continues](#)," *JacksonLewis*, January 10, 2022.

⁹ See Virginie Liebermann and Michel Molitor, "[Blockchain vs. Data Protection](#)," *International Network of Privacy Law Professionals*, July 30, 2024 (discussing such issues in the general context of GDPR).

¹⁰ See Orly Lobel, "[The Law of AI For Good](#)," *Florida Law Review* 75, no. 6, January 26, 2023.

In regulated industries like financial services, many of the concerns regarding AI harms — like discrimination — are addressed by existing laws; however, data privacy laws and other regulations could potentially prevent some of the potential improvements for consumers and the industry that this disruptive technology could bring.¹¹

Conclusion

Financial data and the financial services sector's use of data have long been considered more sensitive due to the potential economic impact on consumers and businesses from abuse or breach. It is still important to consider the burden that regulation may place on positive uses of data and how a growing patchwork of laws could deter innovation or create complexity and confusion. As the committee considers its existing laws and new challenges, it should consider not only how to respond to potential risks, but also how to minimize the impact on beneficial uses of data and new applications of technology. We should consider not only what might be possible today, but how the future may provide new and exciting opportunities and solutions that could improve and expand consumer experiences.

¹¹ See Jack Solowey and Jennifer Huddleston, "[Words to Fear: I'm From the State Government, and I'm Here to Help with AI Risk](#)," *Cato at Liberty (blog)*, June 10, 2024.

Chairman BARR. Thank you, Ms. Huddleston.
 Ms. Strickland, you are now recognized for 5 minutes.

**STATEMENT OF ZOË STRICKLAND, SENIOR FELLOW, FUTURE
 OF PRIVACY FORUM**

Ms. STRICKLAND. Thank you. I am grateful for the opportunity on this important topic, financial privacy.

I am a senior fellow at the Future of Privacy Forum, which is a leading privacy think tank which supports developing privacy technology and business practices, and I lead their Open Banking program.

I have spent over 30 years working in privacy—this is at Fortune 20's and a leading agency—across sectors and across technologies. I also led the Business Roundtable financial subgroup in its efforts to reimagine privacy for the financial sector.

I want to touch briefly on general privacy.

There are a lot of benefits to having an omnibus privacy approach in law. It could be a consistent standard for all consumers. Imagine if we could give consumers a clear set of their rights. It would boost awareness in the consumer ecosystem and their sense of control over their data. It would also make our approach more consistent with international approaches where they do have omnibus laws, and it would support data transfers from multinationals.

There are three challenges when we think about omnibus privacy laws.

The first one, of course, is the substance, right? Privacy is principle-based, and so sometimes it is difficult to define it and be thorough about what those rights are, especially as they evolve over time. I have been very pleased with recent bills that have really done a very thorough job in thinking about modern privacy principles.

The second challenge is around enforcement. I would suggest to policymakers to be careful of approaches that amount to strict liability or per-violation penalties. If you think about \$1,000 times a million, you get to a billion pretty fast. On the other hand, be careful to think about tying enforcement to concrete harms. In privacy, there often are not out-of-pocket damages but the violations are real. So, the focus should instead be on the seriousness of the violation and with the efforts the company made to prevent and mitigate the violation.

The third challenge is around existing laws. What do you do with the plethora of State laws that exist and Federal laws that exist in terms of carve-outs or integration? I do think, as policymakers think about what are good privacy standards, that can create some gravity that can enable these other existing laws to fold in and to develop that consistent standard.

I did want to talk about a pressing issue, which is around open banking and the CFPB final rule. I do believe it is and can be a bipartisan approach and issue.

First of all, open banking does represent enormous consumer value. They really do have the right to have their data and control their data. Enormous examples of positive use cases allow better financial planning, to transfer and hold their money as they see fit. Just imagine if we could have a focus on Americans having finan-

cial health early in their life and the benefits to them and to society and I think that feeling of control over their data and their finances will also lend itself in other areas of their life as well.

There is a challenge if open banking means only the consumer has access to their records. Otherwise, they are going to have to collect it and transfer it to desired third parties, they will have to endlessly update it. I think that would frustrate consumers. It also, unfortunately, would not enable rules for data recipients when they obtain that data, and they will have enormous power over the consumers.

There are many good things about the open banking principles. One is eliminating screen-scraping, where consumers give their credentials to a third party. It is a terrible privacy and security practice. The rule incorporated industry standards sensibly. In a way, I think it made it leading in the world and it also enabled privacy and security rules for all parties, even though they are differently regulated.

I do think in the final rule there were some misses. Some of them impacted data providers; some of them impacted third parties. They are detailed in my written testimony.

I do think that those issues can be examined and addressed, and then open banking can look forward, because it needs—and as mentioned in a lot of the consumer and industry feedback that was provided in that rulemaking process—needs to cover more products, things like loans, investments, payroll, electronic benefits transfer (EBT), to really give that sense of control and that full picture to consumers.

We are very happy to assist in this important effort, and I look forward to taking your questions.

[The prepared statement of Ms. Strickland follows:]



Written Testimony of Zoe Strickland

Senior Fellow, Future of Privacy Forum

Before the U.S. House of Representatives Financial Services Subcommittee on Financial Institutions

"Framework for the Future: Reviewing Data Privacy in Today's Financial System"

June 5, 2025

On behalf of the Future of Privacy Forum (FPF), I thank you for the opportunity to testify about data privacy in the financial system, with a particular focus on rulemaking under Section 1033 of the Dodd-Frank Act, often referred to as open banking. I offer the following remarks to provide observations about data privacy and financial data privacy, and to focus on open banking, including providing some recommendations on how policymakers can progress this important functionality for consumers.

Privacy expertise

My goal in testifying at this fact-finding hearing is to support congressional efforts to advance financial privacy, and to support innovative services that can support competition and new business opportunities that provide consumer value. To this end, I thought it would be helpful to spend a few minutes on my and FPF's privacy expertise. Over 25 years, I have served as global chief privacy officer, among other roles, at Fortune 20 companies in many verticals, including government, retail, healthcare, and finance. At the USPS, I served as the first CPO, and managed Privacy Act, Freedom of Information Act, and records functions, as well as new areas (at the time) relating to internet privacy. At Walmart, I managed global privacy and records, which included financial privacy requirements for its money service centers under the Gramm-Leach-Bliley Act overseen by the Federal Trade Commission. I also served as global CPO for JPMorganChase, addressing all privacy requirements around the world and building a strong privacy compliance program. I am thus deeply familiar with privacy developments over time – such as addressing new technologies and business developments – in a global context – and how to manage privacy practices under different regulatory regimes, whether in highly regulated areas like finance or

healthcare; broadly regulated like retail; or generally regulated in non-U.S. jurisdictions. My focus has been apolitical and very consumer-focused, a bedrock of privacy.

FPF is a non-profit organization that serves as a catalyst for privacy leadership and scholarship and advancing principled data practices in support of emerging technologies. We are supported by leading foundations, as well as by more than 200 companies and law firms, with an advisory board representing academics, industry, and civil society.¹ We bring together privacy officers, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

We are strong believers in open banking initiatives and growth. Open banking enables consumers to have more control over their data and funds. Properly implemented, it can support numerous consumer benefits and opportunities, enabling better money management, financial health, and privacy. Open banking can be a shining example of modern privacy – consumers should expect to have control over their information – and hopefully this sense of control will permeate other aspects of their lives, leading to better services and competition.

Since initiating our open banking program in 2021, we have:

- Held a joint conference with the Organization for Economic Cooperation & Development and issued a white paper on open banking approaches (2022-23)²;
- Conducted an industry and policy-maker event in 2024 regarding the EU Open Banking regulatory initiative known as Financial Data Access (FIDA); and
- Focused heavily on the U.S. open banking environment, including creating a consumer infographic, and engaging in the CFPB's Section 1033 rulemaking process via meetings, white papers, and comment letters³.

This spring, I was elected to serve on the Board of Directors for the Financial Data Exchange (FDX), as a co-chair representing noncommercial entities. FDX is a nonprofit organization, consisting of hundreds of members, that provides technical specifications and other tools to enable consumer-permissioned data sharing within the growing open banking ecosystem of data providers, recipients, and aggregators. We are grateful to CFPB and FDX efforts to include consumer and privacy groups in leadership roles.

¹ The views herein do not necessarily reflect those of our supporters or our Advisory Board.

² Future of Privacy Forum, "Developments in Open Banking: Key Issues from a Global Perspective" (March, 2022), <https://fpf.org/wp-content/uploads/2022/08/FPF-Open-Banking-Report-R2-Singles.pdf>.

³ See Future of Privacy Forum, "FPF files comments with the Consumer Financial Protection Bureau regarding personal financial data rights" (Jan. 18, 2024),

Privacy Observations

During my career, I managed privacy and other programs globally. As this committee is aware, most countries have omnibus privacy laws that apply to their residents. These general laws can be supplemented by specific regulations where appropriate. An example for the financial sector is bank secrecy laws that protect consumer records. (At times this can create conflicts of law, for instance making compliance with both that jurisdiction's bank secrecy law and this country's anti-money laundering requirements difficult.) In addition, some national and regional privacy obligations have implications for cross-border data transfers, with companies analyzing whether personal data is flowing to jurisdictions that have adequate privacy protections. Multi-nationals in particular pay considerable attention to cross-border privacy compliance.

In contrast, the privacy environment in the U.S. is largely sectoral. In my view, it is not only sectoral but topical. As examples, Congress has passed laws over time that contain protections for health information (Health Insurance Portability & Accountability Act), financial information (Gramm-Leach-Bliley Act), credit (Fair Credit Reporting Act), and children (Children's Online Privacy Protection Act). Other privacy protection laws relate to topics like marketing, such as the CAN-SPAM Act and do-not-call requirements. U.S. laws can give federal agencies power to issue supporting regulations, such as the Federal Trade Commission for CAN-SPAM or the Consumer Financial Protection Bureau for GLBA privacy requirements. As compared to the omnibus approach, sectoral legislation allows for requirements that are more targeted to goals and risks. At the same time, disparate laws are harder to update and harmonize, both with each other and with other countries' more general laws.

In recent years, Congress has introduced bills to either update privacy laws for certain sectors or create a more broad-based privacy law. I appreciate these initiatives, and recognize the challenges. Privacy is a wide-ranging field that can be difficult to get your figurative and legislative arms around. There can also be inertia with existing regulatory environments and real questions about how existing compliance frameworks would interact with new legislation.

Some recent examples of legislative efforts include [H.R. 2977](#), the Consumer Privacy Protection Act of 2015; [H.R. 1165](#), the Data Privacy Act of 2023; and [H.R. 8818](#), the American Privacy Rights Act of 2024. I commend the growing efforts to introduce modern and substantive obligations relating to privacy, in addition to security and anti-breach requirements. Privacy and security are related yet distinct disciplines. Privacy relates to how companies use consumer information entrusted to them, and respect consumers' rights and control over that information. It's important that a company

secures information from hackers. That's a baseline. Does the company also allow consumers to access, or correct, or delete, data held about them? Many bills grant authority to federal agencies to define and regulate certain obligations, while others rely on statutory text to fully articulate core rights and responsibilities. Based on my experience, some of the thornier legislative issues can often relate to items like state law pre-emption and enforcement mechanisms.

It is helpful for companies, and policymakers too, to take a principles-based approach to privacy. Key examples of modern privacy principles relate to notice, consent or control, individual rights, data minimization, ethical data uses, and security. One of the most significant of these principles, sometimes called data portability, relates to individuals' rights to be able to access and transport information about themselves. Data portability can help individuals more easily use different services and enhance market competition, yet can also introduce security risks if portability frameworks are not thoughtful and well-managed. This principle is central to the Section 1033 rulemaking.

Section 1033 Rulemaking

Under Section 1033 of the Dodd-Frank Act, the CFPB is authorized to issue rules that require covered entities to make information about consumers who use their financial products available to them upon request. As mentioned in the introductory section, the Future of Privacy Forum has deeply analyzed the proposed rules, and has worked with stakeholders to understand their implications on a range of business practices and data protection issues. Below I cover the extensive regulatory process undertaken, some positive aspects of the Rule, and some areas of potential improvement.

Regulatory Process

Last year the CFPB issued two final rules under its Section 1033 authority: a rule relating to [Industry Standard-Setting](#) on June 5, 2024, and a rule on [Personal Financial Data Rights](#) on October 22, 2024. The data rights rule covers two types of financial products: checking and savings accounts per Regulation E and credit cards per Regulation Z, as well as facilitation of payments from these accounts. The CFPB recognized the Financial Data Exchange (FDX), mentioned above, as a standard setter under the Rule on January 8, 2025.⁴

⁴ [CFPB Approves Application from Financial Data Exchange to Issue Standards for Open Banking | Consumer Financial Protection Bureau](#)

The CFPB undertook a lengthy and extended process to issue these rules, including the following steps.

- October 2016: the CFPB issued a [Request for Information](#) about access to financial records.
- October 2017: the CFPB published a set of [Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation](#), along with a [summary of stakeholder insights](#) informing those Principles.
- October 2020: the CFPB released an [Advance Notice of Proposed Rulemaking](#).
- October 2022: the CFPB sought feedback on 1033 from small businesses and others in an [Outline of Proposals and Alternatives Under Consideration for the Personal Financial Data Rights Rulemaking](#).
- February 2023: the CFPB convened a Small Business Review Panel.
- April 2023: the CFPB released the [Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights](#).
- October 19, 2023: the CFPB released the [Notice of Proposed Rulemaking for the Required Rulemaking on Personal Financial Data Rights](#).

As part of this process, the CFPB engaged with numerous stakeholders and closely monitored market developments to promote consumer interests, innovation, and competition. Engagement included meetings with stakeholders, such as FPF. Meetings that occurred during the rulemaking process were captured as ex parte conversations and posted on their rulemaking website. Given the rule's breadth and depth, many stakeholders weighed in. In response to the proposed rule, over 11,000 comments were submitted. In addition to the sheer number of comments, the depth and content of the feedback is noteworthy as well. Many comments delved deeply into several corners of the rule, and were lengthy and detailed. Although there were recommended areas for improvement, including in FPF's comment letters, there was considerable support for the rule across industry sectors and consumer groups. Indeed, many commenters – including consumer and industry groups – recommended that the rule cover more products and move more quickly. Similarly, the recognition of FDX as a

standard setter was a thorough process, including formal submission and approval, with a public comment period.⁵

Positive Aspects of the Rule

There are a number of valuable aspects to the rule, as listed in our NPRM comment letter.

- First and foremost, consumer control and benefits are core to the rule. The consumer and their direction drive industry obligations and activities.
- The rule phases out the practice of screen scraping. Screen scraping is an extremely poor privacy and security practice. Under this practice, a data recipient obtains log-in credentials and passwords from a consumer, and uses these credentials to access a data provider's website (like chase.com) and take actions on the consumer's behalf. Security experts typically advise that consumers should never provide their credentials and passwords to third parties, which then have unrestricted access to the consumer's account. This practice can create serious consumer harms, and promotes risky behavior that undermines consumer protection campaigns. In addition, screen scraping destabilizes website security of data providers, which need to distinguish between actual consumer access, screen scraping, and bad actor intrusions. The Rule's requirement that data sharing occur via developer interfaces, or Application Programming Interfaces (APIs) given current technology, is the right outcome. The transition from screen scraping to APIs should be legally mandated and occur as soon as possible.⁶
- The rule creates privacy and security obligations for data recipients. I applaud the inclusion of modern privacy obligations for data recipients, including data collection, use, and retention requirements. It is critical that recipients, often fintechs that may be new entrants to the financial ecosystem, only use information for purposes that the consumer has requested. Consumers should

⁵ <https://www.consumerfinance.gov/personal-financial-data-rights/applications-for-open-banking-standard-setter-recognition/>

⁶ I am sympathetic to the criticism that the rule should place the restriction on the data recipient directly, rather than requiring data providers that offer compliant APIs to prohibit screen scraping. Perhaps the CFPB was concerned about its authority over the full data recipient community. In any event, the rule still accomplishes the same result—data providers need to establish compliant APIs, and then screen scraping can be prevented.

be able to trust that recipients operate this way, rather than having to pore through privacy policies and legalese to (perhaps) understand how their information will be used – and trust me, some policies seek to allow more uses than the consumer requested. Indeed, in some ways, 1033 privacy rules exceed those that apply to data providers. The rule also requires recipients to employ security protections that seek to parallel the highly-regulated data provider environment.

- The rule provides a constructive role for industry standards within a regulatory framework. The CFPB recognized that industry was much better placed to devise technical standards for data sharing. Industry is closer to the technology, business functions, and users, and can also make updates and advances more easily than the government. The CFPB relied on long-standing regulatory guidance, OMB Circular A-119,⁷ for how and when to incorporate industry standards. The CFPB provided topical areas for industry standards, particularly related to data sharing interfaces, and also governance requirements to make sure standard setters had transparency, balance in decision making, and oversight. It is one of the strengths of the Rule. One of the areas where the U.S. is ahead of other jurisdictions in open banking, despite their sometimes earlier start and coverage of more products, is in development of industry standards. This advantage should be promoted.

Areas for improvement

Unfortunately, the CFPB in its Final Rule did not incorporate some of the comments that it received that would have improved the rule. If the Bureau had made these changes, the rule would have been stronger for consumers and more palatable to industry. I will touch on five topics.

- **Secondary uses of information:** The Final Rule prohibits data recipients from using consumer information for secondary purposes. Data recipients may only use information for primary purposes, and can't cross-sell products, without initiating a new authorization disclosure process. Authorization disclosures are intended to initiate a new product or service. Forcing their use for secondary uses will be awkward and cumbersome to consumers, stifle innovation, and result in inconsistent compliance and experiences. As FPF described in its comment letters, a better outcome for consumers and the ecosystem is to allow

⁷ Office of Management and Budget, Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities* (Jan. 1, 2016), <https://www.federalregister.gov/documents/2016/01/27/2016-01606/revision-of-omb-circular-no-a-119-federal-participation-in-the-development-and-use-of-voluntary>

consumers to opt-in to secondary uses. To be clear, and as articulated in my testimony, I support regulating uses of information, and believe that data recipients should respect consumers, including their expectations of data uses. Obtaining consumer consent for secondary uses is particularly appropriate for open banking, which is all about consumer direction and permissions. The opt-in mechanisms of course must be clear, prominent, and fair. To the extent that the CFPB wished to exclude uses deemed high risk, that is not a reason to abandon the proper privacy approach; either define prohibited uses, or let consumers choose products that are legal in the marketplace.

- **De-identification:** The Final Rule arguably prohibits the use of de-identified data, unless it is the product or service requested via an authorization disclosure. Per our comment letters, we strongly encourage that de-identified data not be subject to the regulation, consistent with other regulatory regimes in the U.S. and globally. The use of de-identified data is a central aspect of data processing for all industry sectors, including the financial sector, encouraging innovation in a privacy-protective manner. In open banking, examples are quality control and product and service improvements. There are numerous public policy research benefits as well. De-identification is also a valuable privacy and security protective measure, greatly reducing risks relating to data misuse and breaches. Its use should be encouraged, not devalued.⁸ I understand there are concerns related to re-identification. As with all risks, appropriate controls should be deployed and monitored. Frankly, as a long-term compliance officer, I know any obligation can be violated, and the risk of data misuse is harder to police for than re-identification risk. In the preamble to the final rule, the CFPB recognized its approach had downsides, and suggested that it may alter its approach in a future rulemaking. That change should happen now.
- **Payment Initiation information:** The Final Rule requires data providers to furnish payment initiation information that allows data recipients to initiate money transfers out of consumers' accounts, often called pay-by-bank. As an initial point, and for consistency with Dodd-Frank language, the rule should instead cover data types (account number and routing number) like it did for the rest of the rule. More broadly, the CFPB should dig deeper into the fraud concerns raised by data providers.⁹ To be clear, pay-by-bank exists in today's ecosystem, such as for account openings and for payments to utilities, landlords and other payees. Consumers want this functionality and convenience, and it needs to be part of the rule. However, with the rule opening the door widely to any authorized third party, and with data providers having limited recourse to deny API access via specific risk management concerns, it is critical to examine

⁸ See Future of Privacy Forum, *A Visual Guide to Practical Data De-identification* (Apr. 25, 2016), <https://fpf.org/blog/a-visual-guide-to-practical-data-de-identification/>.

⁹ <https://www.regulations.gov/comment/CFPB-2023-0052-11099>

any increase in fraud risk. Taking money out of consumer accounts merits higher scrutiny. The CFPB should address these concerns via RFI, enhanced fraud monitoring, more data provider recourses, or shifts in liability.

- **Fees:** The Final Rule prohibits data providers from charging fees related to access to their APIs. Certainly the consumer should not be charged. It is their data and they should be able to direct companies to share it for desired purposes. The rule prohibits data providers from taking actions to evade the rule and discourage access, and should otherwise be silent on fees between companies.
- **Digital Wallets:** The Final Rule covers digital wallets, including pass-through wallets that do not store information. This raises considerable compliance challenges for those providers for no discernable consumer benefit. In my read of comment letters, there appeared to be consensus to exclude pass-through wallet providers.

I consider that the Final Rule unnecessarily stepped back from the NPRM relating to industry standards. The NPRM provided that adherence to a standard issued by a recognized body was deemed compliance for interface obligations. The Final Rule watered this down to an indicia of compliance. In my view, if the CFPB has recognized an industry standard setter, its technical specifications should be considered compliant. This incentivizes industry adoption of consistent standards and good governance. The development of industry standards is a benefit of the U.S. market-led approach, where policymakers can add useful weight.

Finally, in our comment letters, we recommended that the CFPB and other relevant regulators issue guidance relating to risk management and data privacy. The CFPB has issued extensive privacy guidance to data providers under GLBA, and should do the same for data recipients.

Conclusion

I am grateful to this committee for the opportunity to comment on financial privacy and the 1033 Rule. We are hopeful that open banking moves quickly to the future. Rules should incorporate more products and services, so that consumers can truly have a holistic view of their financial picture, and address developing issues like artificial intelligence. We are available to assist in navigating the path forward. It's our mission to progress the intersection of developing technologies, privacy best practices, and consumer interests. Thank you again for this opportunity and I look forward to your questions.

Chairman BARR. Thank you.

We will now turn to member questions. The chair now recognizes himself for 5 minutes.

Mr. Talbott, my first question will be directed to you.

The section 1033 rulemaking that Ms. Strickland was just referencing was a product of the Dodd-Frank Act. In the 15 years since the passage of Dodd-Frank and the rulemaking, the landscape of the financial system has changed massively, as we have all been discussing.

The rulemaking is currently being debated in the courts. However, there needs to be some certainty and stability so institutions can flourish in the technological ecosystem.

Mr. Talbott, should data privacy legislation potentially modify or replace certain provisions of section 1033 of Dodd-Frank to codify the beneficial aspects of the rule while moving away from outdated and unclear aspects of the Dodd-Frank policy as currently written?

Mr. TALBOTT. Sure. Thank you, Mr. Chairman. I appreciate the question.

I think, in general, the open banking or consumer-directed banking is already existing in the marketplace today, and it is done through a series of bespoke contracts between the bank, data aggregators, and fintechs. All of these entities should be subject to GLBA or through these contracts. If they are not, then possession of the data should trigger coverage of the privacy law. If any entity has a consumer's data and they are not covered, they should be covered as a basic principle.

A couple of issues we had with the open banking or consumer-driven banking proposal, the final reg that is subject to the courts is: One, it did not address liability for fraud or for a breach. If one entity is subject to a breach and consumers suffer a loss, that is an area that needs to be addressed either through privacy law or through a future rulemaking, that was one of the misses, I think, that Zoë referenced earlier, and we agree, that there has to be something around dealing with liability for fraud that was not addressed in that.

Additionally, the law prohibited the collection or assessment of fees by the financial institution for the work that they are doing, and that is another area that needs to be addressed.

In general, Mr. Chairman, the answer to your question is that existing privacy laws should cover all the participants in the open banking system.

Chairman BARR. Should our privacy legislation that we are considering, should it modify 1033?

Mr. TALBOTT. I think that, in general, it should consider it, but I do not think there are any gaps, necessarily, in the law other than an entity not being subject to GLBA.

Chairman BARR. Okay.

Private rights of actions create more problems than they solve. They incentivize trial lawyers to file frivolous class-action lawsuits and lead firms to avoid business opportunities that would benefit consumers due to fear of costly litigation.

Ms. Kuehn, based on your experience with the GLBA and similar privacy laws, do you believe adding a private right of action to GLBA would meaningfully enhance consumer data protection or

would it more likely impose litigation risks that hinder innovation and reduce consumer access to financial products?

Ms. KUEHN. Thank you for the question.

What we have not seen, and where I think this concern about do we need to add a private right of action, is whether or not there are gaps or problems happening in financial services data. There do not seem to be.

If you look at the history of enforcement—and there have been a couple of agencies with enforcement authority over Gramm-Leach-Bliley during its existence—there have not been many cases involving privacy of consumers, the use of data.

That tells us that, even though these entities are examined by prudential regulators, looked at by different enforcement entities—and we saw a very aggressive enforcement regime from the last 4 years from the CFPB, yet, what we do not see are cases brought under GLBA.

I think we have the tools that we need if there are problems that exist, and I do not know that additional tools are needed.

Chairman BARR. If we have a nationwide, uniform data privacy standard, the regulatory agencies, the financial regulators could handle enforcement—

Ms. KUEHN. I believe so.

Chairman BARR [continuing]. without a private right of action?

Ms. KUEHN. Yes, sir.

Chairman BARR. Thank you.

Thanks to advancements in technology over the past few decades, financial institutions and firms can partner with more technology-oriented companies in order to compete and serve additional customers with the products and services that work better for them, but State privacy laws have created a patchwork that can complicate these partnerships.

Ms. Huddleston, how has this patchwork harmed market efficiency and consumers and would Federal preemption for GLBA-compliant financial institutions help preserve these innovative partnerships?

Ms. HUDDLESTON. Thank you for your question, Mr. Chair.

When we see this emerging State patchwork, it is particularly burdensome on new ways of using data that might not fit existing models, whether that is firms that would not traditionally be considered financial institutions but may be using financial data in some way to help inform consumers or whether these are just small financial institutions trying to get off the ground.

A patchwork means that they are now going to have to seek to comply in 19 different States. Even if those 19 or 20 different States have the same law on the books, there will be different interpretations of many terms, meaning that these firms have to invest significantly in regulatory compliance rather than focusing on providing their consumers with the best possible product.

Chairman BARR. Thank you for that testimony.

My time has expired.

The gentleman from Illinois, Dr. Foster, is now recognized for 5 minutes.

Mr. FOSTER. Thank you, Chairman Barr.

Quickly, Mr. Talbott, when you mentioned that banks and fintechs already have a limited data-sharing capability between them, it seems to me that the small banks are kind of left out of this. They cannot have the ability to stand up to an application programming interface (API) team that will go and do all this data-sharing.

Are there any solutions on the horizon for that or is this going to be one of the things where we are going to have to try to level the playing field to make sure that small banks and credit unions are not left out?

Mr. TALBOTT. Yes, so banks and credit unions—I will let Andrew speak for himself—but we work together as an industry. We do not want any weak links; so, any data, like an API, for example, through an industry consortium, is shared with all entities to allow for—

Mr. FOSTER. Yes. There is a problem that I think remains unsolved, that the smaller institutions simply do not have the capacity to plug into this very complex ecosystem.

Ms. Strickland, thank you, first of all, for your very thoughtful testimony and your focus on the important work that CFPB has done on data privacy.

As I said in my opening remarks, I am really very uncomfortable with the idea of this administration rescinding completely the rule to implement section 1033 of Dodd-Frank. Not only has it been 15 years since the passage of Dodd-Frank that required the rule-making, but I am also not confident that the CFPB, frankly, currently has the staff necessary to do a full rewrite of the rule.

One thing I think is important to recognize, that this is not a rule that came out of nowhere. There was extensive work on the final rule spanning multiple Presidential administrations that solicited public input on various aspects of the rule, as well as a notice of proposed rulemaking that was initiated during the first Trump Administration.

Can you speak briefly about the extensive work that went into this rule and the huge amount of bipartisan effort by your organization and the financial services industry as a whole to prepare for open banking and the impact of this administration's potential rescinding of this rule?

Ms. STRICKLAND. Thank you, and I very much welcome that question.

I included in the written testimony a very detailed description of the extensive process with the relevant links to all the materials. It was a very long and extensive and thorough process and had engagement across all industry sectors and consumer groups.

If you read the comment letters, which I did—and there are a lot of them. Not only were there a lot, but they were very long and thorough and really delved through all the different aspects of the rule, and largely supportive, that this is a positive to the ecosystem. Yes, it has existed for a while, but there were some areas that benefited from some consistency of the regulatory framework.

You see that in the comment letters. In fact, some of them suggested, again, covering more products. We really need to do that, in terms of giving that full view to consumers, and doing it more quickly since it exists now and it is a consumer benefit.

I do think, as mentioned, in the final rule there were a few misses that I think could be addressed. I think Scott hit on a couple of them accurately. I do think that it will be a good place to look in terms of what happens next, either through Congress or the CFPB, to address those issues and then look forward to where we are trying to take open banking in America.

I did want to comment on your remarks about the smaller players. I do think there is a question whether they stay under a regime that is run by screen-scraping, which is, again, not a good practice but also is not better for them, too, in terms of their understanding of their consumers and their interests.

So, there are efforts to make that API more widely available and to have core providers who can help lift up the smaller players so that they can benefit from this developing ecosystem too and that needs to be paid attention to as well.

I do think the staggering helped, because it allows some of this infrastructure to grow and that they can then get on-ramps onto it. I do think it benefits the whole community that the smaller institutions are ramped on at the right time.

Mr. FOSTER. Yes. Thank you. As someone who has done his fair share of programming of screen-scraping as well as APIs, I share your enthusiasm for getting rid of screen-scraping. It is unstable, it is dangerous to privacy, and it is just a pain in the ass.

Ms. STRICKLAND. Horrifying.

Mr. FOSTER. Right.

The future is probably neither APIs nor the past of screen-scraping but agentic interactions, where the consumer interaction is not going to be directly with the consumer but with an agent.

One of the interesting arguments the Trump Administration CFPB made in the brief that they filed with the court last Friday was that section—they claimed section 1033 of Dodd-Frank requires that the rule only allows consumers themselves to request access to their data, which ignores the language in the Dodd-Frank Act that, quote, an agent, trustee, or representative acting on behalf of the individual, which is obviously meant to include third parties and agents authorized by the individual.

If you could just comment on that for the record, I would appreciate it. That is a big problem.

[The information referred to was not submitted prior to printing.]

Chairman BARR. Thank you.

The gentleman's time has expired.

The gentleman from Michigan, Mr. Huizenga, is now recognized.

Mr. HUIZENGA. Thank you, Mr. Chairman, and I would like to say thanks to the Ranking Member.

For the kids watching out there, that is a technical DC term for difficulties in transactions, what he was expressing, where exactly those pains might occur, earlier.

Apparently, that was funnier in my head than it was when he said it.

Mr. Talbott, good to see you again. I think you got it. You were nodding with me.

Yesterday, we heard from multiple witnesses about the importance of consumer protections when it comes to owning digital assets and when it comes to data privacy. Frankly, I do not see much

difference. Gaining access to a consumer's data is just as lucrative as gaining access to their bank account. In your testimony, you noted, "Consumers rightly expect strong privacy protections and data security for their personal information and their money."

Of course, providing protections does come with some costs. How can Congress strike the balance between consumer protection and excessive compliance—there is compliance, but then there is also excessive compliance—so that small providers—and I think Ms. Huddleston was talking about that a bit or at least alluding to that—that the small providers are not disproportionately affected compared to the larger providers?

Mr. TALBOTT. Sure. I thank you for the question. I appreciate it.

I think first is, areas where we could focus are tightening up the definitions so that all parties know exactly what data is protected. For example, in Gramm-Leach-Bliley, they use the phrase "consumer" and "customer," and they make a distinction between the two, and that may no longer hold or be as clear to all parties, including smaller players. So, tightening up the definitions can help so we all know what we are talking about.

Secondly, you can look at the rights that are provided under the law—right now, the rights include access, correction, deletion, and those—and make sure that those can be applicable for all entities so that consumers get the same rights and benefits regardless of which institution they choose to use and; so, narrowly focusing on those rights and how they are applicable in the real world could help address the issue for all players, not just small players.

Mr. HUIZENG. You touched on definitions, tightening up definitions. I want to ask, does the GLBA's definition of "financial institution" adequately reflect the range of entities handling consumer financial data today?

Ms. Huddleston, you seem to have that—Mr. Morris? Somebody?

Ms. KUEHN. I am happy to address that.

Mr. HUIZENG. Grab it. Yes. All right.

Ms. KUEHN. The definition of "financial institutions" is keyed off to all the variety of activities that financial companies can engage in and that is subject to expansion if, over time, the agencies decide, "Hey, there are some additional things we need to address." So, it is a flexible definition.

It is also pretty broad. I mean, if you think about the definition of "financial institution"—

Mr. HUIZENG. So, broad and flexible could be too broad and flexible or interpretation of it has then locked out some areas?

Ms. KUEHN. It is not locked out, because it is made in reference to the Federal Reserve's definition of what types of financial activities banks engage in. So, it lists everything from credit reporting to making loans to doing financial transactions.

Mr. HUIZENG. Okay.

How about Mr. Morris? Does it apply to credit unions?

Mr. MORRIS. Yes, the financial activities would definitely encapsulate what credit unions are doing. So, we would clearly be—

Mr. HUIZENG. Do you feel like you are adequately covered by this?

Mr. MORRIS. Yes.

Mr. HUIZENG. Okay. Great. I see Mr. Talbott nodding.

Mr. TALBOTT. I would agree.

Mr. HUIZENGA. Okay.

What consumer rights have States incorporated in data privacy laws that Congress should codify at the Federal level? In other words, are there some best practices that we are seeing out in the States?

Mr. Talbott?

Mr. TALBOTT. Yes. I think a couple of—GLBA covers a lot of those rights, but they do not necessarily have so much the right to access a lot of the information or some of the information. So, that could be important to update GLBA with.

Mr. HUIZENGA. So—but are there any States specifically doing that? I mean, as we are seeing, obviously, privacy frameworks need to evolve.

Mr. TALBOTT. Right.

Mr. HUIZENGA. Is there somebody that is actually doing a good job that we ought to be looking at?

Anybody else?

Mr. TALBOTT. I would—Virginia has done a good job. Texas. Both States' privacy laws capture those.

Mr. HUIZENGA. Okay.

Anybody else care to weigh in on that?

Ms. HUDDLESTON. I would just note that I think it is important to consider what enforcement mechanisms, and what timelines are involved in some of these things.

When we look at, for example, a right to access, are there appropriate incentives, particularly for sensitive financial information, to ensure that it is the correct consumer that is getting that information, that we are not seeing something where there is such a short timeline for response that the wrong information is handed over to the wrong consumer.

One can look at, for example, General Data Protection Regulation (GDPR) to see how there have been some incidents where recordings or other information, not financial, have been handed over that way.

Mr. HUIZENGA. Great.

I yield back.

Chairman BARR. The gentleman's time has expired.

The gentleman from Georgia, Mr. Scott, is recognized.

Mr. SCOTT. Thank you, Chairman Barr.

I really agree with you, Chairman, that our Nation is at a crossroads when it comes to financial privacy. Right now, our constituents' banking information, their credit history, their transaction records, and even how they pay their rent is up for grabs, for exploitation, wrongdoing, and even stealing. Without firm protections, that data can be collected, brokered, and misused, often without the consumer ever knowing.

That is precisely why the CFPB section 1033 rulemaking is a step in the right direction. The CFPB 1033 rule has set up a framework that empowers Americans to take more control of their own financial data safely, securely, and on their own terms. It prohibits data brokers from monetizing data without consent, fintech applications to be transparent and non-manipulative, and financial in-

stitutions to provide data access in a secure, machine-readable format.

Here is the problem: These protections, this progress on behalf of our consumers are now under a great threat, for we are watching a dangerous rollback taking shape at the CFPB under the Trump Presidency.

President Trump is appointing people who have spent their whole careers defending data brokers, avoiding regulatory compliance, weakening the CFPB's enforcement capacity, and threatening CFPB's funding and undercutting the CFPB's rulemaking.

Now, Ms. Strickland, the Trump CFPB has argued that rule imposes a burden on data aggregators and fintech companies. Let me ask you, is it not the CFPB's job to protect the consumers and not the business models of companies that profit from opaque or predatory data practices?

Ms. STRICKLAND. Thank you for your question.

Yes, I think one thing that was valuable about the 1033 rule is that it did place obligations on the companies receiving data and, in fact, imposed sort of modern principles around what those privacy rules should be.

To the prior question asked about what are some of those activities that policymakers should look at? There is a developing area called individual rights, which Jennifer alluded to, which is, do I have the right to access, delete, and transport my data? How do I understand the data that belongs to me is about me, and do I have rights with regard to that?

Also, another very useful feature we see in some developing bills is around privacy impact assessments and risk-based assessments, which are extremely familiar to the financial sector, to a lot of risk analysis. So, those sorts of precepts really lend themselves to how we think about privacy.

I do think that is a value in open banking, which is, the data recipients are going to have a lot of information now about these consumers and perhaps even will move money on their behalf. So, it is very important that they actually have rules that apply to them as well and if you do not have open banking rules, you do not have that ability to really put those controls in place.

Mr. SCOTT. Now, many of my friends on the Republican side have talked about rescinding the rule. Tell me, will not rescinding the rule make it easier for bad actors to exploit our consumers?

Ms. STRICKLAND. I do think that the proposed rule really did address some issues between data-sharing amongst the parties. There were some good features for data providers, definitely some good controls over data recipients that really should be included in any future rulemaking activity around this. I think they were very important points.

Mr. SCOTT. Thank you, Ms. Strickland.

Chairman BARR. The gentleman yields back.

The gentleman from Texas, Mr. Williams, is now recognized.

Mr. WILLIAMS of Texas. Thank you, Mr. Chair. Thank you all for being here today.

Community banks have earned the trust of their customers by safeguarding their sensitive financial data because they have long-

standing relationships with their customers and handle personal information with diligence and care.

Now, we need to ensure that any updates to data privacy maintain flexibility for smaller banks. These smaller institutions struggle with mandates that force them to divert resources from lending in their communities and into legal compliance.

Ms. Huddleston, could you elaborate on ways to modernize the GLBA that preserves flexibility for smaller banks?

Ms. HUDDLESTON. I think it is important that we look at this on a Federal level as opposed to the State-by-State patchwork that is often emerging.

Additionally, we need to consider not only the way data may be being used these days by smaller entities but also the ways it may be used in the future. We already see tools like artificial intelligence (AI) being deployed in the fraud alert system and things like that. We certainly would not want to see regulation or changes that may make it more difficult to deploy these tools in the future.

I think when we are talking about concerns about private right of action that is particularly relevant to smaller players, smaller players who could find, even if they win a lawsuit, that it is still potentially business-crippling or even business-ending and so are less able to absorb the cost of that litigation than a larger player, even though larger players also have significant financial regulatory compliance burdens.

Mr. WILLIAMS of Texas. Thank you for that.

One of the most promising developments in financial services over the past decade has been the growing collaboration between banks and fintech companies. These partnerships allow smaller institutions to offer cutting-edge digital tools for underserved customers and compete with the largest national banks.

Now, much of this innovation relies on responsible data-sharing arrangements where consumers can securely grant access to their financial information and improve their banking services.

Mr. Talbott, how do data-sharing arrangements between banks and fintechs improve competition in the marketplace? How can we protect that collaboration while still maintaining strong privacy protections?

Mr. TALBOTT. Sure. Thank you for your question.

I would just note that Texas has a number of provisions in its privacy law which are examples for the rest of the country. They have carve-outs for small businesses as well as rights of cure, which are good examples.

In terms of data-sharing between banks and fintechs, most of this interaction, if not all, is already covered by Gramm-Leach-Bliley, both the privacy as well as the security provisions. If it is not, it is covered by a private contract, bespoke contract, between the two entities.

So there is sufficient coverage there both for privacy as well as data security. We feel those existing laws and existing contracts will help keep the data safe and secure.

Mr. WILLIAMS of Texas. The people I represent in Texas, like many rural communities across the country, a lot of local lenders and community financial institutions with access to credit, mortgages, and basic financial services, and as we consider new data

privacy rules, we have to be careful not to cutoff these vital lifelines. If regulations are too complex or restrictive, small banks and credit unions may scale back services or exit certain markets entirely.

Mr. Morris, this question is to you. How can we make sure that the privacy regulations do not unintentionally limit consumer access to financial products, and particularly for those in rural areas like I represent in Texas?

Mr. MORRIS. Thank you for the question. I think one area where a Federal privacy framework could focus to preserve that access is by preserving the current opt-out framework that is present in the Gramm-Leach-Bliley Act that facilitates a lot of joint marketing activities, which allows community financial institutions, small credit unions, small community banks to partner with fintechs and others to promote the availability of their services in banking deserts and other places where there may be limited access to affordable products.

Having an opt-out framework for sharing information is an intelligent way that the GLBA has balanced those concerns. Whereas the more onerous opt-in framework could curtail that and limit access to services in those communities.

Mr. WILLIAMS of Texas. Thank you, Mr. Chair, and I yield my time back.

Chairman BARR. The gentleman yields.

The gentleman from California, Mr. Sherman, is now recognized.

Mr. SHERMAN. When I saw the title of this hearing, I thought I would spend my full 5 minutes talking about Elon Musk, looking at all the Social Security data of millions and millions of Americans, but I think I am going to focus on things within the jurisdiction of our committee.

The CFPB plays a critical role with data privacy. The decision of the Trump Administration to destroy, dismantle, abolish the CFPB means that not only will Americans not be protected from rip-offs, not only will they not get the information they need to make intelligent decisions and financial matters, but we will talk grandly about their privacy, but there will not be an agency there to ensure that their private data is kept private.

One of the issues that arises is one we have seen for a long time, and that is what happens if there is hacking. We have seen this issue with regard to giant retailers having information, getting hacked, and then turning to the banks and saying, "You have to pay all the costs of dealing with consumers on this issue." It has been well-established in tort law theory for well over 100 years that the liability of the cost of an accident should be put on the party who could have invested to prevent that accident.

Whenever a fintech company is the entity that gets hacked, they are the ones that should bear the cost of the consumer repair. The 1033 rule asks fintech companies that want to access to banks' data to comply with the same Gramm-Leach-Bliley financial data protection requirements the bank must comply with, but there is no specific enforcement mechanism for this rule.

The rule also did not ban screen scalping, a practice by which third-party stores your user, your password, then logs into your bank account and collects, maybe sells your financial data.

Mr. Morris, what amendments or guidance, like perhaps banning screen scalping, and having the CFPB regulate fintech companies that store financial data, what should we consider to the personal financial data rights rule to ensure that we are safeguarding this data for consumers?

Mr. MORRIS. Thank you for the question. I think with respect to ways to better protect data and address the concerns that you mentioned, in the context of 1033, it would be prudent for the CFPB to consider a way of allocating liability in the event that data is mishandled by downstream third-party entities, using that information, collecting it from data provider credit unions. The absence of that means that credit unions and other data provider financial institutions and their members only have a course in the courts. So, addressing that in the regulation could be a helpful way to meet the rule.

Mr. SHERMAN. Now, under the CFPB Rule 1031, financial institutions currently cannot charge a fee for third-party fintech companies to access the bank's data through their API application programming interface developer portals.

Mr. Morris, is it costly to develop and maintain these API portals and should we consider at least allowing the smaller institutions to charge a fee to fintech companies to access the data through these relatively expensive portals?

Mr. MORRIS. Thank you for the question. I believe that it is absolutely correct that it is costly to develop and maintain APIs. One of our concerns, again, with the CFPB's rule implementing 1033 was the significant cost that is shouldered primarily by data providers to essentially subsidize API access and development. So, we would like the CFPB to reconsider that aspect of the rule to better balance the cost to our credit unions.

Mr. SHERMAN. I am going to try to squeeze in one more question. Mr. Morris, what protections, like perhaps, banning screen scalping across the board should we consider adding so that small institutions are protected? Even if they are exempt from the rule, what effect on small credit unions and the small banks could there be if there is a massive financial data breach of a third party potentially exposing financial institutions to liability and drying up all its members depository accounts?

Mr. MORRIS. We are certainly supportive of moving away from screen scraping, which is a less secure way of sharing information. As far as tightening up rules that are designed to prevent data breaches and minimizing their consequences, I think one area in 1033 the CFPB explored, which is sharing information necessary to initiate a payment, that is very sensitive information, which if it is shared with a third party it could lead to fraud.

Chairman BARR. All right. The gentleman's time is expired and the gentleman from Georgia, Mr. Loudermilk, is now recognized.

Mr. LOUDERMILK. Thank you, Mr. Chairman. Thank you all for being here. Very important subject. I have 30 years in public and private sectors with dealing with intelligence, data security, and protecting information. Eight years Active-Duty military in the intelligence community, protecting our Nation's secret, 2 years with the Defense contractor, and 20 years with my own business.

Privacy and security are very important to me and the number one key to protecting data was a rule that we lived by in those 30 years is, you only have to protect what you have. Meaning, if you do not absolutely need something, do not keep it.

While the GLBA focused on the private sector, the elephant in the room is not Elon Musk. It is the massive amount of data the government has that he had access to. No one on the other side of the aisle wants to address that this entity, this 800-pound gorilla called the Federal Government, is the largest security risk of personal privacy information.

Now, what we are discussing here is very important, but when we bring up legislation that actually would restrict the amount of data, like updating the Bank Secrecy Act and currency transaction reports to make them reflective of where they should be due to inflation, we do not hear anything from the other side, but they are always anxious to deal with the privacy data when it comes to the private sector. That is important. I am not demeaning it.

We do have to understand that our Nation collects and forces the private sector to turn over massive amounts of personal privacy information and financial information to the government, which is the weakest link in our cybersecurity protection.

With that, Mr. Talbott, dealing with GLBA, what rights do consumers currently have regarding their personal data under the Gramm-Leach-Bliley Act? Yes, Mr. Talbott. I am sorry.

Mr. TALBOTT. Yes, no problem. I appreciate the question, Mr. Loudermilk, as well as your representation of the State of Georgia where 70 percent of all credit card and debit card transactions run through your State.

The rights under GLBA for consumers that exist now is they have a right to correct and a right to talk about earlier somewhat access the information, like to delete the information. These are important rights for consumers. There are disclosure notices that are required depending on where you sit in the system and so, these are all important rights that they have. They have the ability to opt out of target marketing, and that is an important right as well.

Mr. LOUDERMILK. That is one thing in this new era because we often fail to keep up with technology, which allows for some innovation, but also, is defining what is consumer data versus privacy data versus company data, that type of thing.

In what ways do financial institutions share consumer data with affiliated and nonaffiliated third parties?

Mr. TALBOTT. The first and foremost example is with any transaction. Let us say a credit card transaction, there are at least three, sometimes four parties involved. There is the issuing bank, the requiring bank processors, there are networks and that data under GLBA is allowed to be shared for purposes of processing that transaction. As you well know from the credit card space, that is necessary to allow that transaction to move in 1.2 seconds when you are standing in the checkout line.

Mr. LOUDERMILK. How do fintech companies access consumer data to deliver financial products and services and what role does consumer consent play in the process?

Mr. TALBOTT. Sure. Right now the concept of open banking or consumer-directed banking is happening in the marketplace and fintechs will enter into bespoke contracts with banks to allow their shared customers to share the data between the two. That is governed by a private contract at this point, pending the 1033 rules that may come up at some point.

Mr. LOUDERMILK. Okay. Thank you. Mr. Morris, what are three key features that credit unions believe should be included in any new data security regime?

Mr. MORRIS. Thank you. I think the first and most important is an entity level exemption that recognizes existing compliance with the Gramm-Leach-Bliley Act as well as other laws like Fair Credit Reporting Act, the Right to Financial Privacy Act, and others. The other thing we would like to see is preservation of the opt-out framework and a limitation on private rights of action which could hinder innovation and create enormous litigation risks for small credit unions and other institutions.

Mr. LOUDERMILK. Okay. Thank you. Mr. Chairman, I will yield back my time.

Chairman BARR. The gentleman yields back. The gentleman from California, Mr. Vargas, is recognized.

Mr. VARGAS. Thank you very much, Mr. Chair. First of all, I want to thank you and the Ranking Member for convening this hearing, and of course I want to thank the witnesses for being here.

I do want to point out that I was abandoned by Mrs. Beatty who normally sits here next to me. Today, she decided not to, and I think that should be pointed out. I feel hurt.

Secondly, I do want to say this, that I actually agreed with half of what my good friend from Georgia said. I actually do think the government has way too much information. It absolutely does, and it does not protect it as well. In fact, I am a little worried today when you go through the airport now, they get all sorts of biometric information about you. I do not know how they use that either. I think we should be concerned about that, and I do not think that the government does protect the wealth.

I do not agree with Elon Musk. I do think that, in fact, it was very dangerous to have him running around with these young kids doing things that we do not even know what the hell they were doing. I am not sure that they knew either.

All that being said, the CFPB has a job of making sure consumers are getting straight deals and making one of the ways it is done—and one of the ways it is done is by making sure consumers are getting a fair deal when it comes to control of their own data. When consumers are not in control of their own data, financial institutions have to compete on their merits for the people's business and more competition is better, I think, for everyone.

That is what Dodd-Frank Section 1033 is all about. While Section 1033 goes back to the Dodd-Frank Act, the CFPB's finalized rule ensured consumers could be in control of their personal financial data and could be more easily transferred to another provider.

From the Gramm-Leach-Bliley Act dealing with financial information to the Fair Credit Reporting Act dealing with credit information, Congress has continued to adapt privacy protection laws to

an evolving economy. We also have to make sure that we continue to adapt those protections, security of data as a top of mind, especially in the financial sector, and especially in the era as I said earlier of DOGE being given access to sensitive data information.

I was proud to join a letter this week led by the ranking member as he stated urging the CFPB not to vacate and throw out the years of progress we have made on finalizing Section 1033 rule.

Ms. Strickland, when CFPB finalized the Section 1033 rule in October 2014, former Chairman McHenry stated that the CFPB's final rule 1033 is a promising step forward to protect Americans' financial data privacy. Consumers should know where their data is going, how it is used, and be able to terminate—and to terminate collection of their data by certain firms.

Director Chopra also listened to some of our concerns regarding unreasonable restrictions on secondary use of data. Why do you believe there was bipartisan support for this rule at that time?

Ms. STRICKLAND. I am sorry, the question is there were?

Mr. VARGAS. Why do you think we did come together and there was bipartisan support?

Ms. STRICKLAND. I think there was. You saw that from the comment letters as well. It ranged across all the industry sectors as well as the consumer groups. Again, delving very deeply into every aspect of the rule.

I do think a contributing factor was with all the great work that was done to get to the proposed rule—and there was enormous amount of work done, including the small business review panels—and again, digging deeply into how do the parties work together, what are the right obligations? What are the right privacy practices? Right security practices—what products are we covering? How do we think about small entities? A lot of work went into all those aspects.

I do think in the final rule, there were a few items that were not addressed ideally and that creates—

Mr. VARGAS. For example.

Ms. STRICKLAND. So—and, again, in the written testimony, I go through several of them. In my view, the main ones were—and you mentioned them? One is the secondary uses of information. They did not allow those—even consumers to agree to them and that is what open banking is all about. It made for a very awkward sort of consumer experience.

It also did not really allow the use of the identified data, which is a common practice, not only in the financial sector, but in every sector. It is a great privacy and security practice, too, because you made it nonidentifiable and controlled for re-identification.

It did not thoroughly look at the questions raised about increased fraud or liability. There was some information given about what that could look like. Could there be better monitoring done? Some shifts looked at in terms of liability.

Mr. VARGAS. Okay. I do want to stop you there because, again, I think that there are some things that we could do a better job at. I have to say this: It is interesting because this issue came up in California, many, many, years ago back in 2001, when I was the Chairman of the Insurance Committee. At that time we would have had screaming matches here. We do not have that anymore, be-

cause I think we have come a long way, and I do want to praise everyone that has worked on this issue. Thank you. Thank you, Mr. Chair.

Chairman BARR. The gentleman yields back. The gentleman from Tennessee, Mr. Rose, is recognized.

Mr. ROSE. Thank you, Chairman Barr, and also thank you, Ranking Member Foster, for holding this important hearing. Thank you to our witnesses for your time today and being part of this hearing.

Mr. Talbott, in your testimony, you highlight that two dozen States have enacted different data privacy laws. Can you discuss the challenges that members of the Electronic Transactions Association face when it comes to navigating such a large number of potentially inconsistent State laws?

Mr. TALBOTT. Sure. Thank you for the question. The biggest one is what data is covered. Many States provide either provide an entity level exemption, meaning that the bank or the credit union is exempt from that State's privacy law because they are covered under the GLBA. Some States only have a data-level exemption, which means the entity is covered, but certain data, the GLBA data is not covered by that State's privacy law but the State's privacy law definition of what is covered is broader. At that point, and most particularly, California is the lead example. Oregon is similar as well. Business-to-business (B2B) data is exempt under GLBA but is not exempt under California law.

So, any entity that may be GLBA compliant still has to map out all of its data and all of the uses for the business side to ensure that it is in compliance with the California State law—the California State privacy laws.

There is a perfect example of how different States with different definitions can create issues. That creates a lot of problems and challenges.

Mr. ROSE. Sure. Can you—and it may be beyond what you just gave as an example, are there examples where—that you can provide where State data privacy laws are in conflict at such a level that it is impossible to comply with those inconsistencies?

Mr. TALBOTT. I do not know if I would say impossible necessarily but definitely creates some conflicts. I have a list in my written testimony, and the biggest example is with California. Where I just talked about where B2B is covered under the California privacy law, but it is not covered at the Federal law. That is the biggest challenge. Others relate to timing, the nature of the disclosures, what data can be excluded or not, what opt-out rights the consumer has. Maryland has a very stringent opt-out on what can and cannot be covered or cannot be shared. Those are just some examples where the challenges—

Mr. ROSE. So not really—I do not think I am hearing of examples where you—what you do in one State would actually be a violation if you did it in another State. Is that fair to say?

Mr. TALBOTT. That is correct. It is fair, yes, sir. It is on the implementation side.

Mr. ROSE. I guess that is good news. Obviously, we need to avoid that.

Mr. Morris, in your testimony, you touch on the fact that the credit unions, like many financial institutions, have long prioritized investments in data security to ensure that their members or customers' privacy is protected. I think it would be helpful if you could expand on just how much credit unions have already invested in data security.

Mr. MORRIS. Thank you for the question. I am happy to share more statistical information perhaps after, but I can say that we have run surveys in the past and consistently year after year after year reflecting enormous cost of data breaches and the risk of fraud. Credit unions are prioritizing investments in cybersecurity and data security. Those things are part of the Gramm-Leah-Bliley Act, which mandates that the National Credit Union Administration, other financial regulators, and other regulators of financial institutions implement technical safeguards to ensure that those institutions are adopting appropriate data security practices. That drives a lot of cost, but it is important for keeping trust.

Mr. ROSE. Very good. Mr. Talbott, back to you. Would you like to discuss the significant investments that the Electronic Transactions Association members have already made in data security?

Mr. TALBOTT. I think the number would be in the billions. We spend equal amounts on developing and deploying new products and services to make payments easier, faster, more secure. We also spend similar amounts to fight and protect fraud to protect both consumers, merchants, as well as the economy. The number is easily in the billions of dollars.

Mr. ROSE. In light of some of the discussion we have had about the role of employees of institutions in safeguarding data—and I might open this up, but I will start with you, Mr. Talbott, any—and we do not have much time—but any criteria in any of the law as to the credentialing or qualifications of employees of organizations that are charged with protecting consumer data that you would like to speak to or take note of?

Mr. TALBOTT. Yes, sir. I appreciate the question. The Federal Trade Commission (FTC) safeguard rules as well as good business practice require companies to develop a robust system internally for security purposes, and that includes addressing which of their employees have access to it, how to cutoff that access, passwords, et cetera. I mean, all the usual security protocols that you would think would go into protecting data as well as payments.

Mr. ROSE. Thank you. My time has expired. I yield back. I would appreciate insight from the rest of the panel about that question of credentialing of employees that deal with consumer information. Thank you. I yield back, Mr. Chairman.

Chairman BARR. The gentleman yields. The gentleman from Illinois, Mr. Casten, is recognized.

Mr. CASTEN. Thank you, Mr. Chair. Last year the CFPB finalized their open banking rule that would have given consumers greater access and control over their financial data, including making it easier for consumers to move their financial data from institutions.

Ms. Strickland, can you just talk about how that rule would increase competition and make our markets more efficient?

Ms. STRICKLAND. Yes, so on that actually—and thank you for the question—has been a key driver of open banking initiatives in the

United States as well as in other jurisdictions which is how do you make all the players compete for the consumer's business, both in terms of good price, but also in terms of product offerings? Really encouraging new technology and new business models to say, Hey, I have a brand-new idea. How do I do this but recognizing they are not always regulated in the same way as banks are, which is deep and thorough.

So, open banking really does enable these different companies to work together and to put both a framework around how the data exchanges occur, but also, as I mentioned, put some rules on the data recipient who are not regulated in the same way. The open banking rule created to the prior question on this roll around what you collect, what you can use it for, how long you can retain it, which are really important safeguards

Mr. CASTEN. To that point, we had, a couple years ago on this committee, we had a discussion with former Director Chopra about how Facebook had no obligation to ensure that in hoovering up your data, they were not essentially violating the Fair Lending Act by only promoting certain credit card products to one individual or another.

Would the open banking rule have fixed some of those gaps so that third parties like Facebook are not using your data to target you in ways that may be, if not illegal, certainly unethical?

Ms. STRICKLAND. Yes, I think that is right. I mean, presently for large companies, if they are not regulated by sectorial law, they are under general FTC jurisdiction which is unfair and deceptive; so, their privacy policy is accurate. They can proceed as well as the State laws that exist.

I do think an open banking benefit was to create modern privacy rules for the recipients of this data which are very important because they are getting sensitive financial information and sometimes the ability to move money. So, having that bar and those requirements on data recipients was a real value to the rule.

Mr. CASTEN. Just as an aside, I consistently struggle with the fact that my extreme libertarian colleagues are petrified of the government getting your data but seem to have no problem if a private company gets your data and monetizes it and refuses to let you see what they have. Rand is pissed is all I have to say about that.

You mentioned the FTC. This matters, of course, because last week the Trump Administration's CFPB filed a motion to vacate that rulemaking, which is going to open up this gap. A lot of these data privacy rules, as you mentioned under Gramm-Leach-Bliley, CFPB has some jurisdiction, the FTC has jurisdiction, our balancing regulators have jurisdiction.

I guess I will turn to you, Ms. Kuehn. Given your past role at the FTC, if the CFPB cannot fulfill their roles to protect data privacy and were left with whoever remains standing, what are the gaps that emerge in our ability under current law to protect the people we represent and their data privacy?

Ms. KUEHN. One of the benefits that the Federal Trade Commission has is a broad rule related to unfair deceptive action practices. There was some discussion about retailers getting data and what happens if there is a breach at a retailer. The FTC has brought a

number of cases involving data security, many, many, years ago, just under its general Section 5 authority where it has found a gap.

So, one of the benefits of the Federal Trade Commission's jurisdiction is that it does have this sort of flexible oversight and ability to bring cases where it sees developing threats emerging.

Mr. CASTEN. So, I guess the concern—maybe I will turn back to you, Ms. Strickland—in theory, I agree with you. In practice, we have an entire industry saying I want complete absolution of any liability from any of my AI models. In fact, all of our Republican colleagues just voted last week to pass a piece of legislation that says, there shall be no liability for anybody using the AI model.

So I steal your data, I put it into the system, I violate the deceptive practices, but you are totally absolved because I did not do it. The AI optimized an algorithm to solve this, and how was I to know? All I did was just not comply—did not say that AI would comply.

So I guess, Ms. Strickland—there may not be enough time—but I would welcome your thoughts on how we might regulate AI. In this world, where the CFPB is broken, data privacy still matters, what should we be doing to close this barn door, especially in light of this big ugly bill that we passed out of the House last week if the Senate goes along with that?

Chairman BARR. The gentleman's time has expired. The witnesses can answer for the record. The gentleman from South Carolina, Mr. Timmons, is now recognized.

Mr. TIMMONS. Thank you, Mr. Chairman, and thank you to the witnesses for joining us this morning. I often hear from constituent companies about the challenges posed by the complex State-by-State patchwork of data privacy laws, which makes compliance across jurisdictions burdensome and undermines consistent consumer protection. Many States vary restrictions and laws based on the side of the company. This is understandable until you realize that many States have vastly different thresholds based on the institutions in common handling of consumer data.

This issue is compounded by the fact that the Gramm-Leach-Bliley Act serves only as a Federal floor for consumer financial data privacy, allowing States to impose more or less stringent requirements.

For instance, California mandates opt-in consent for sharing consumer data with nonaffiliate third parties, going beyond the GLBA's opt-out standard. While other States, such as Alabama, align more closely with the Federal baseline and impose fewer additional obligations.

This uneven regulatory landscape complicates compliance efforts and creates uncertainty for institutions operating nationwide.

Ms. Kuehn, what challenges do California's law in similar State regulations create for consumer access to financial services within those States and how do they affect financial institutions seeking to enter or operate in those markets?

Ms. KUEHN. The former preemption that GLBA has, which basically keeps States from going below the standards does allow States to set different standards above that. To date, until these more recent privacy laws, States have not really ventured into that very far. The problem is that as the States are looking at these pri-

vacy issues, and they want to set different or varying standards, that is going to make compliance very difficult, particularly for financial institutions who operate throughout the United States.

So, I am going to have to have an investment in State-by-State rules and compliance and controls that is going to take away from my ability to provide other products and services to consumers. The patchwork is of great concern. If this committee were to relook at GLBA, I think revisiting the form of preemption that exists in law will be very important in order to preserve this sort of uniform approach that financial institutions take across the country.

Mr. TIMMONS. Is it fair to say that larger financial institutions comply with the patchwork framework more easily than smaller?

Ms. KUEHN. They have more money to invest in compliance. I mean, let us face it, the smaller guys, particularly in a competition area, have a tougher time because they have to build the kind of processes and services and have the personnel to deal with consumer inquiries, for example, you name it. It is the big investment for the clients that I work on. It is often a hardship.

Mr. TIMMONS. It really stifles entrepreneurship because startups are unable to comply, and it really creates a major, and we need to address it.

Mr. Talbott, what problems do these regulations create for innovative institutions trying to deliver a seamless experience for consumers, especially when offering products and services if those consumers have actively requested?

Mr. TALBOTT. Thank you for the question. We will deliver the products and services as the market demands, but the challenge will be in compliance with the various State laws. You have disclosures, you got opt-ins, you have opt-outs. All of those will slow down the process of getting customers on-boarded in the first instance.

Once they are on-boarded, once that has been addressed, then the products will be delivered quickly, accurately, seamlessly. The challenge would be in the compliance side we are doing.

Mr. TIMMONS. Thank you for that. How do these frictions hinder new market participants, such as fintechs, to compete with larger more established institutions?

Mr. TALBOTT. They too must comply with the privacy and data security rules. There are cost, time, and expense associated with compliance. In addition, they have to navigate all the different States, depending on which States they operate in, as well as GLBA, depending on where the State exemption is. That creates enormous amounts of complexity, challenge, compliance costs.

Mr. TIMMONS. As we consider how to address this problem, I think the general perspective is that Europe has gone too far, and they have really restricted competitiveness. What would your recommendation be—obviously, California has a standard, and the European standard is the most developed—how do we thread this needle to accomplish the objective without being overly burdensome?

Mr. TALBOTT. Two points: GDPR is the European version. They actually have a good definition that many States borrow from. That is positive. They also allow for a private right of action which cre-

ates off the back end the number of legal issues and challenges and complexities.

Initially, the number of these private rights of action can distort or change or slowly case by case modify the law which creates more challenges in terms of compliance versus having enforcement at the Federal regulatory system.

Mr. TIMMONS. Thank you for that. It is past time for Congress to act, and we need to preempt State law and create one standard so we can compete in the global economy. With that, I yield back. Thank you.

Chairman BARR. The gentleman yields. The gentlewoman from Ohio, Mrs. Beatty, is recognized.

Mrs. BEATTY. Thank you, Mr. Chairman, and Ranking Member.

Ms. Strickland, I will start with you where Ranking Member Foster ran out of time, and so, I will pick it up there. He was making the point that one of the points outlined by the Bureau is that Section 1033 only allows CFPB to write rule-granting consumers access to their financial data, and it does not allow for sharing that data with third parties.

Would consumers not be harmed most if they do not have the ability to share their financial information with third party tools and products to help them manage their financial well-being? Could you elaborate on that?

Ms. STRICKLAND. Yes, I will be happy to. Yes, I do think if consumers get access to their own information in a machine-readable format, that is great. That is progress but the real benefit of open banking is their ability to direct the sharing and transporting of that data from a data provider to authorize third parties who have been adequately vetted to make sure they have the right privacy and security practices. If you do not enable that, I think it will frustrate consumers because what they are going to keep it on, their computer, and then they are to send a data recipients, and they are going to update it. It seems unworkable.

I also think of a downside to that which might be an unintended consequence, which I have touched on is that then the third parties are no longer under an umbrella that requires them to have rules about what they can and cannot do with that data once they receive it. They are not vendors of the data provider. What is it that they can and cannot do with that data? The 1033 rule did put restrictions on what they can use it for, which is the purpose of the transaction, right?

So, it did put some rules around, A, them being vetted and, B, that they actually had some requirements of their own when they received this data. Both of those aspects of the portability piece of this were very important.

Mrs. BEATTY. Okay. Thank you so much for that. Mr. Morris, let me go to you. First, let me thank you for your work with America's Credit Unions. As you may be aware, I have a bill the Advancing the Mentor Protégé Program for Small Financial Institutions Act, which is actually noticed in today's hearing. It would codify the Treasury Department's financial agent Mentor-Protégé Program to encourage partnerships between large and small financial institutions, including credit unions. Codifying this program would help small and community financial institutions across the country in-

crease their capacity, improve their relationship, lending business modeling, and even become a financial agent to Treasury.

Can you briefly discuss how this bill will help credit unions better serve their communities because I also look at it when we talk about open banking and technology? It is supposed to be new ways also to bring institutions together. I would like to hear your comments on that.

Mr. MORRIS. Thank you for the question. I think the Mentor Protégé bill is one that aligns well with the cooperative nature of the credit union industry, and we are certainly supportive of it and ways to enable Minority Depository institutions (MDIs), small institutions to partner with their larger peers to learn best practices, learn how to comply with complex rules and regulations. Today, we have spoken about the costs of complying with a rigorous data privacy regime. It is certainly a mentor protégé arrangement that can help facilitate learning among smaller institutions.

Mrs. BEATTY. Thank you for that. I think I have time for one more question since I am down here on this row by myself that my colleague took great pleasure, Mr. Chair, Ranking Member took great pleasure in telling me that he was going to pull rank on me, and now I see why.

Let me address it also to Mr. Fields, our Ranking Member, thank you for letting me ask this last question. I will come back to you, Ms. Strickland.

Tell me your comments or thoughts on in the time I have left. What would happen if we abandoned Section 1033 which means that all of the consumer protections imposed on those third parties would also be rescinded?

Ms. STRICKLAND. Thank you for your question. As other witnesses have mentioned, open banking does exist today and has been a developing practice in the United States for a few years. It would still continue, it just would not have the same framework around it, around, how does that data sharing work? What are the rules in terms of vetting these third parties? What are the obligations on the third parties?

It does phase out screen scraping. Yes, perhaps, it could have done it more directly, but it did phase it out and say once compliant data sharing APIs are employed, you cannot—screen scraping can be prohibited, which is, I think, very important for both the consumers' benefit as well as website security.

Chairman BARR. The time has expired.

Mrs. BEATTY. My time is up.

Chairman BARR. The gentlewoman from California, Mrs. Kim, is now recognized.

Mrs. KIM. Thank you, Chairman Barr, Ranking Member, thank you for hosting this hearing. I want to thank all our witnesses for joining us today too. As you know, for too long, our Federal laws have not evolved to keep up with the issue of data privacy. As a result, we have seen States take action because we have failed to lead at the Federal level.

In California, we have implemented legislation such as the California Financial Information Privacy Act and the California Consumer Privacy Act. While the intent of these bills has been good, the unfortunate result is that the financial institutions have dual

compliance obligations at the State and Federal levels. That, coupled with patchwork State laws, has made it both costly and very confusing for institutions as they have to comply with the jurisdictions in which they operate.

I want to ask my first question to you, Mr. Talbott. Can you explain how in States like California, which I am sure you are very familiar with the conflicting State privacy laws have created damaging dual compliance?

Mr. TALBOTT. I am sorry, I missed your last part.

Mrs. KIM. Yes, the damaging—how do these conflicting privacy laws have created damaging dual compliance?

Mr. TALBOTT. Sure. Thank you for the question. Thank you for your leadership with the financial literacy and wealth creation caucus as well as you and Mrs. Beatty. The challenge is in terms of the costs of compliance, the complexity, because financial services institutions are not exempt in California at the entity level, only at the data level. Any data that they use is not GLBA-compliant has to be mapped out and evaluated in terms of making sure they are compliant with the California laws that you mentioned. That is costly. That is time-consuming. Additionally, there are—

Mrs. KIM. Yes, can you talk about, like, the regulatory cost? What are the companies looking at when they have to develop these processes to meet those divergent State privacy laws?

Mr. TALBOTT. Sure, they have to assign personnel. They have to assign lawyers. They have to hire regulatory counsel. Outside counsel is usually hired. There are compliance experts that are brought in. The whole team that has been developing system for the financial institutions at the Federal level also has to spend time, if not create a separate team focused on California.

In addition, California changes their law frequently, and currently there is a current proposal to amend it. Now all of those changes have to be discussed and analyzed and executed, and that takes time and resources.

Mrs. KIM. Sure. Another issue I hear a lot about is the question of opt-out versus opt-in as it relates to data privacy. Ms. Kuehn, I want to ask you in the Gramm-Leach-Bliley Act can you explain to us why there was an intentional decision to offer consumers the ability to opt out rather than opt in?

Ms. KUEHN. Yes, so GLBA provides a requirement that financial institutions have to clearly disclose to consumers exactly what happens with their data and where they have choices about that data. They do that at the start of the relationship. If you are going to share data that is subject to an opt-out, you have to tell the consumer every year, hey, I am sharing your data, you can change your mind about it. The reason it did that was because there are a number of things companies do to share data the consumers sort of expect. I might not want to opt out of my bank sharing my data for certain purposes, but I might want to opt out, say, for a car dealer using it. You have those choices on an entity-by-entity level to do that.

Also, the privacy notices, I know people pick on them, but they are the subject of a lot of research and development to make sure that consumers can clearly understand in plain language exactly what is happening with their data and what choices they have.

Mrs. KIM. I think consumers are rightfully concerned that they have limited understanding about how their financial data is being utilized. That is why I think it is important that we also address the annual privacy notice that consumers receive.

Ms. Kuehn, can you talk about the annual privacy notice that a consumer receives, and what kind of research does the agency or agencies conduct to make notices more consumer-friendly?

Ms. KUEHN. Yes, the FTC and the bank regulators worked on the current form of the privacy notice. I think one of the most recent innovations is the understanding that the consumers do not necessarily need to get a repeat annual notice if, number one, their financial institution is not sharing it subject to an exception, meaning that the purpose their financial institution is sharing data for things like fraud prevention and to process their transactions.

Mrs. KIM. Can you quickly talk about when the last time the annual policy model form that FTC posted was revisited or reformed?

Ms. KUEHN. That was back when I was at the Federal Trade Commission, which was about 15 years ago.

Mrs. KIM. Completely outdated. I think that explains the reason why—

Mr. MOORE [presiding]. Representative, the lady's time has expired.

Mrs. KIM [continuing]. Okay. Thank you. Thanks for answering that question.

Mr. MOORE. The gentleman from the great State of Louisiana, Representative Fields is recognized.

Mr. FIELDS. Thank you, Mr. Chairman. Let me thank all the witnesses for being here, and I thank you for this hearing. I just have two very simple questions. The first question I want to ask Ms. Strickland. Lower-income families often rely on free and low-cost, third-party financial tools to plan their financial futures. When big banks restrict these tools by blocking data portability, who gets hurt? How does Section 1033 address this rule inequity?

Ms. STRICKLAND. Yes, thank you for your question. I do think both predating 1033 and then under the 1033 rule, the goal was to encourage consumer commission data sharing and doing it in a responsible fashion so that data providers did not put up unnecessary hurdles to that data portability request. The third party had rules as well in terms of privacy and security obligations because they had that information and then not in the same regulated field as the banks do. There were important steps made to think through those issues to make sure responsible data transfers and data portability occurred at the consumer's direction.

As I mentioned, one of the things that many commenters remarked upon and is still unfinished business in the 1033 rule is how are you making sure that other parts of people's financial health are also included so that they can have that full picture of their financial wherewithal. One of the comments dealt with things like if you would have government benefits, like EBT. There were a lot of comments there about how does that community also able to aggregate the information about themselves? These were items that were considered to be like future rulemakings. I think they are really important so that there really is that complete picture that people can have a full understanding of their financial situa-

tion, are able to direct the use of products and services that benefit them, and that it is done in a way that treats the data providers, data recipients fairly and ethically so that the data transfers are well-managed. I do think it is an important step in terms of that ecosystem as well as future products that should be addressed.

Mr. FIELDS. Thank you. My next question is for Mr. Morris. Section 1033 rule had broad support precisely because it promotes competition and empowers consumers. Credit unions compete on service, not market power. How does maintaining the current system where big banks can block data access harm credit unions' competitive position in serving working families?

Mr. MORRIS. Thank you for the question. I think in terms of competition, 1033 can offer benefits to credit unions in a general sense that data portability is helpful for consumers to switch financial institutions. However, we do have concerns around the CFPB specific implementation of Section 1033, the cost of API development, the lack of a framework for allocating liability of a third party's mis-handled data, as well as concerns around the type of nonstatutorily enumerated data elements that the CFPB will want to see shared, like sensitive payment information.

So, while we think that the statute is good in the sense that it provides a core principle of data portability, there is work to be done, in our view, on refining the final rule.

Mr. FIELDS. I want to thank you, Mr. Chairman. I yield back.

Mr. MOORE. The gentleman yields back. The gentleman from Wisconsin, Representative Fitzgerald, is recognized.

Mr. FITZGERALD. Thank you, Chairman. Mr. Morris, from your perspective, how does overlapping or inconsistent enforcement approach impacted your member credit unions' ability to innovate and serve their customers efficiently? What role should Congress play in ensuring Federal regulators do not stifle credit union-led innovation that is already subject to any different State-level scrutiny?

Mr. MORRIS. Thank you for the question. I think there are areas of inconsistency in terms of the patchwork of State privacy laws just in terms of how different types of data are handled, whether you are opt in, whether you are opt out, whether there is specific regulation targeting a technology, like artificial intelligence. Certainly, those are areas where credit unions can leverage technology to innovate, provide better fraud detection and prevention, for example.

On the Federal regulatory side, I think some of the inconsistency can arise simply due to the fact that these technologies are evolving at a very quick pace. It may be beneficial for there to be pilot programs or other ways to test innovative products without necessarily the fear of compliance driving those innovation decisions.

Mr. FITZGERALD. As a former State Senator, a lot of the work we did at the State level, I now have a different perspective of. Financial institutions like credit unions are always subject to robust Federal privacy requirements, including the regular oversight and enforcement by the regulators. There is a growing concern adding a Federal private right of action would trigger a wave of abuse of class action lawsuits, right? We have seen this in Illinois. We saw it in California with California Consumer Privacy Act (CCPA).

So these suits, obviously, often result in huge settlements with minimal benefit to consumers and kind of leave the small and mid-sized institutions exposed to sue or settle.

How would introducing a private Federal, private right of action for data privacy violations affect credit unions' ability to just serve their members, I guess?

Mr. MORRIS. Thank you. I think it would absolutely have a detrimental effect to include a private right of action and any comprehensive Federal privacy framework. Certainly, when you talk about the individual private right of action that might arise across however many States, that does have an impact across the board. It influences decisions, again, around innovation, but it can also just add to litigation costs and litigation risks. Those settlements can add up and detract from the core mission of credit unions, which is serving their communities with affordable products and services.

So, to the extent that litigation drives compliance costs or litigation costs up, that is money that is coming out of the community.

Mr. FITZGERALD. While the State privacy law wholly exempt banks and other institutions subject to Federal Gramm-Leach-Bliley Act law, there are some others, such as California Consumer Privacy Act, which I just mentioned, and a successor of the California Privacy Act. This obviously means that financial institutions will still implement programs to comply with the laws, even though it only applies to just a limited kind of subset, I guess you would say, of their data.

Ms. Kuehn, what is a level of effort for these compliance products?

Ms. KUEHN. I believe Mr. Talbott testified to this as well. You have to sort of map all of the data that you have. You have to have personnel involved with that. You have to have often bring out third-party technology companies to help you assess and it figure out which data is covered, which data is not. So, there is a compliance investment for financial companies that operate in California that may not exist elsewhere that have an entity-specific exemption, for example.

Mr. FITZGERALD. Chairman, I will just say that it is these kinds of legal burdens that drive financial institutions, like the credit unions and the banks, to kind of pursue the mergers in order to better absorb the compliance costs. With that, I will yield back.

Mr. MOORE. The gentleman yields. The gentleman from Texas, Representative Green, is recognized.

Mr. GREEN. Thank you, Mr. Chairman. I thank the Ranking Member and the witnesses for appearing today. Mr. Chairman, I would also like to thank the Chairman, Mr. Barr, for honoring his commitment to bring H.R. 3716, as it is today, to the attention of the Congress again. This was done at a previous hearing.

Mr. Barr, if you are somewhere within the sound of my voice, or any place where you might find out, I am grateful. I am also grateful to the staff for helping us with this legislation. Many times when we say I, "I" is properly defined as "we." The personal pronoun is rarely efficacious when it comes to passing legislation.

This legislation, H.R. 3716, deals with something that I hold dear, and it is the belief that the public has a right to know what

Congress needs to know. This legislation satiates both of these concerns. I introduced this legislation—remember, “I” as “we”—the Systemic Risk Authority Transparency Act on June 4, 2025. It was first introduced on June 14, 2023, in the 118th Congress. The legislation was developed following the failures of Silicon Valley Bank and Signature Bank in 2023 when the The Federal Deposit Insurance Corporation (FDIC) invoked the systemic risk exception to guarantee uninsured deposits at those banks.

The key provisions of this piece of legislation would include within 60 days of such an invocation of a systemic risk exception, the Government Accountability Office will be required to produce a preliminary post failure report. Within 90 days, the appropriate bank regulator, including the FDIC, the Office of the Comptroller of the Currency (OCC), and the Federal Reserve System (Fed)—or the Fed will be required to issue a preliminary post-failure report. Then, within 180 days, the Government Accountability Office (GAO) and the bank regulators will be required to issue a comprehensive post-failure report.

This timeline provides an opportunity for us to get some initial evidence of what happened, to get a better understanding, and then get a comprehensive report. More appropriately said, these reports will provide Congress and the public with an analysis to identify the causes of the bank failures, including any management, supervisory, or regulatory shortcomings. The committee passed similar legislation by a 50-to-zero vote last year.

Again, I see this as necessary legislation. Congress needs to know certain things, and these are the things that the public has a right to know. When banks fail, I think people need to know why and I think that they should know why without having to speculate.

I have found in life that where you have few facts, you have much speculation. This will provide the facts so that we can avoid speculation.

In closing, members of the panel today, this is a process that I used when I was a litigator. It is called voir dire, or voir dire depending on where you are from. We called it voir dire in Texas, and it requires you to tell the truth. It is the truth-telling portion of a trial.

So, this is a simple question for you. Given what I have shared with you about this legislation, given what you know about banking failures, given what you know about the public right to know what Congress needs to know, do you think this legislation would be helpful? If you think so, kindly extend a hand into the air. Was that question too complicated for you? Do you think the legislation would be helpful?

Mr. TALBOTT. I think we would have to take a closer look at it.

Mr. GREEN. Okay.

Mr. TALBOTT. I am happy to get back to you

Mr. GREEN. I will ask all of you to take a closer look and give me your opinions. Would you do this for me, please?

Mr. TALBOTT. Yes.

Mr. GREEN. Ms. Strickland?

Ms. STRICKLAND. Certainly.

Mr. GREEN. Okay. Thank you. Thank you, Mr. Chairman, I thank all of you for your participation today. I know that this is without the lane that you normally negotiate and navigate and traverse, but I hope that you will give it some thought and give me an answer. Thank you so much. I yield back.

Mr. MOORE. The gentleman yields. The gentleman from Ohio, Representative Davidson, is recognized.

Mr. DAVIDSON. Thank you, Chairman. I am excited about this important hearing. Privacy is one of the most abused portions of the Bill of Rights. I mean, we have seen technology radically change what is possible since Gramm-Leach-Bliley became law. It is timely, relevant, probably a little past due that we update GLBA. Frankly, not long after GLBA laid a great foundation, the Patriot Act passed and massively expanded what the government was doing, and frankly, what the government was directing other people to do on its behalf.

Technology has grown rapidly over these 25 years, but especially fast since the innovation of artificial intelligence. I hope that we can kind of get the horse before the cart and not the other way around.

Privacy is really foundational. Before we can really get a correct framework for artificial intelligence, we really need to look at what is happening to the underlying data because if we have artificial intelligence laid out there, it only functions by having access to the data. If that data in the private hands is not cared for in the proper way, you are going to see it exponentially exploited by the technology that artificial intelligence is making possible.

I hope we get this right in short order.

Ms. Kuehn, your testimony highlights that GLBA's broad definitions of financial institutions in nonpublic personal information cover a wide range of entities and data.

During the evolving financial landscape, including the rise of fintechs, data aggregators, and whatnot, how would you recommend updating GLBA's definitions?

Ms. KUEHN. At this time, in my experience, it has pretty much covered anyone I have looked in the financial sphere. It is a large, flexible definition. It also covers not only the entities who are financial institutions themselves, but also entities that receive information under the Gramm-Leach-Bliley. There are restrictions on their ability to reuse or re-disclose the data they get.

It was surprisingly forward-looking and thinking about all the ways in which financial institutions and the endless financial industry are intertwined. It covers a lot of those uses that exist already.

Mr. DAVIDSON. A lot of times we do regulation here in Congress is because we have committees of jurisdiction, so we do not really holistically solve problems. When you look at GLBA, it kind of says that we have one set of privacy laws for financial firms but then if you run a website or put automation into cars that really does quite a lot of surveillance in your automobile, it is governed by a whole different set of laws. Does it make more sense to have a comprehensive privacy law that recognizes that individuals have a property right in their data versus a sector-based approach? Does anyone have thoughts on that?

Mr. TALBOTT. Happy to, real quickly. Yes. I appreciate the—I think given the unique nature of financial services and the fact that we have both your account numbers as well as your money and your information, that it is unique versus other industries, but I think the rest of the marketplace could benefit from a uniform national standard.

Mr. DAVIDSON. Thanks.

Mr. Morris?

Mr. MORRIS. I would agree that a sectorial approach is appropriate for the financial sector, just because we are already subject to so many laws and regulations. I think, to your point about other sectors maybe not having the same rules of the road. I think a comprehensive Federal privacy framework should address that.

Mr. DAVIDSON. Yes. Here is an example. Google paid a small—for the scale of the size of the entity—fine because they set up the Android operating system, and they said that you could select “do not track,” for your geolocation, in theory, would not be tracked. When they were caught tracking everyone’s geolocation, they said, Oh, no. What we meant was you could select do not track. We, of course, are going to track you.

That was pretty dishonest. I mean, that would not be just simple negligence, not really gross negligence. That was willful misconduct. They should have gotten in trouble for that.

Right now, because the FTC or Federal Communications Commission (FCC) would regulate a product like that, they put terms and conditions down in the fine print, five-point fonts with pop-ups that hit you until you relentlessly click okay, fine. I just want to get on with what I am trying to do, and there is not really much accountability for it.

Financial firms, I would love to say, are totally different, but Wells Fargo did not accidentally do what they did with consumer data and set up false accounts and everything. They paid over \$4 billion in fines, but no one was prosecuted. In other sectors, when you abuse the access to data or you commit fraud, people go to jail. I think we ought to consider much stronger privacy protections, and I hope we do.

I yield back.

Mr. MOORE. The gentleman yields.

The gentleman from Nebraska, Representative Flood, is recognized.

Mr. FLOOD. Thank you, Mr. Chairman.

The topic of today’s hearing is extremely important. Data-sharing is at the center of financial interactions and transactions. In many cases, a consumer’s data has to be shared between many parties in order to even fulfill a transaction. Let us use the example of a consumer applying for a mortgage to demonstrate the point.

The consumer initially applies for their mortgage with their lender. They need to provide documentation verifying their income, their assets, their liabilities, their employment, among other things, in order for that application to be complete. At that point, the lender uses those pieces of information from the consumer’s application to determine whether or not to approve the mortgage.

They have to go to the credit bureaus to get the consumer’s credit report. The consumer’s credit score needs to be polled, involving

the credit scoring companies. They may go to another bank to verify information regarding the borrower's assets. They may go directly to the consumer's employer to verify their employment. Then an underwriting decision needs to be made. Sometimes the lender will work with an outside underwriter who would also need to access all of the same information that we discussed in order to even confirm their credit risk and compliance with local relevant loan programs.

After all of those steps are complete, and many more I did not name for the sake of time, it is possible for the lender to make an informed decision on whether or not to approve the mortgage.

Think about all the different third parties I just mentioned that were involved in completing just one act for the consumer, filing a mortgage application. We live in a world today that is far more complex than it was 10, 20, 30 years ago, and we have relationships between financial institutions and third parties today that did not exist when the Gramm-Leach-Bliley was written. That, in a nutshell, is why we are having this conversation today. When you layer on the fact that some States are now moving in competing directions as it relates to rules around sharing and protecting your consumer financial data, you have even more complexity to the underlying problem.

Mr. Talbott, in your testimony, you mentioned some examples of conflicting State privacy laws. Can you please describe an example of conflicting State law on data privacy that you feel really represents the broader problem that I just talked about?

Mr. TALBOTT. Yes. I think that California, unfortunately again, is probably the lead example where it has both private right of action which do not exist in any other State, as well as it does not exempt GLB entities—does not exempt the—does not exempt the entity. It exempts the data. In California, for example, the B2B transactions are covered by that State's privacy law, whereas the rest of the country, it is not. That is a challenge right there.

Mr. FLOOD. For those of us, Mr. Talbott, that are interested in open banking, how should we think about a Federal financial data privacy law and how that could ensure that the consumers' information is both protected while also leaving the door open for them to choose to use tools that are offered by third parties?

Mr. TALBOTT. Yes. So, the entities engaged in open banking or consumer-directed banking are already covered by GLBA, so the privacy protections and the data security protections are there. To the extent that an entity, maybe a fourth party, is not, it should be, given the fact it will have data or access to the data. So, that is an important structure that is already in place.

Mr. FLOOD. Ms. Huddleston, can you speak to some of the results of the private right of action connected to the Illinois Biometric Information Privacy Act?

Ms. HUDDLESTON. As mentioned in my written statement, we have seen significant litigation against a variety of entities. This includes small timekeeping entities; this includes large social media companies, like Meta. It also includes people that—or entities that one might not traditionally think of with data, like Six Flags Amusement Park. This litigation has not only been when actual harm occurs. It has also been over statutory issues, such as

the exact method of the language of consent or things like that then become overly burdensome on launching new products.

We have also seen products not being launched in Illinois because of a concern around compliance. This, of course, means that the residents of that State do not have the benefits of some of the better technologies that might improve security through the use of biometrics, as well as fun things like Google's Art Selfie match a few years ago.

Mr. FLOOD. I am a strong believer in States' rights. I served in a legislature, like our Chairman here, both in the role of speaker. This is the one area that I do think we need a national standard. I truly believe that this only happens if Congress acts and we can let people do business. That is the reason I put that mortgage application example in there.

I will go to bat for States' rights whenever I can. This is one of the few times that I think this is a very appropriate direction. I thank Chairman Barr for his leadership on this issue and would love to deal with this in the 119th Congress.

Thank you, and I yield back.

Mr. MOORE. The gentleman yields.

We would like to thank all of our witnesses today for taking the time to be here and for your testimony on behalf of all the committee members. We do appreciate that.

Without objection, all members will have 5 legislative days to submit additional written questions for the witnesses to the chair. The questions will be forwarded to the witnesses for their response. Witnesses, if you receive those, we please ask that you respond no later than July 10th, 2025.

[The information referred to can be found in the appendix.]

There being no further business before the committee, the Chair declares the hearing adjourned.

[Whereupon, at 12:16 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIALS SUBMITTED FOR THE RECORD

Scott Talbott

EVP

Electronic Transactions Association

Questions for the Record

Subcommittee on Financial Institutions Hearing, titled: “Framework for the Future: Reviewing Data Privacy in Today’s Financial System.”

June 5, 2025

From Ranking Member Waters:

1. Which of the following options best describes your self-identified race? (You may choose more than one.)

- a. White or Caucasian ☒ X
- b. Black or African American
- c. Hispanic/Latinx
- d. Asian
- e. Middle Eastern/North African
- f. Choose not to answer
- g. Prefer to self-describe (please specify)

2. Which of the following options best describes your gender identity?

- a. Woman
- b. Man ☒ X
- c. Non-binary
- d. Transgender Man
- e. Transgender Woman
- f. Choose not to answer

g. Prefer to self-describe (please specify)

Responses to Questions for the Record

Respondent: Andrew Morris

From Ranking Member Waters:

1. Which of the following options best describes your self-identified race? (You may choose more than one.)

a. White or Caucasian

2. Which of the following options best describes your gender identity?

b. Man

Questions for the Record

Subcommittee on Financial Institutions Hearing, titled: “Framework for the Future: Reviewing Data Privacy in Today’s Financial System.”

June 5, 2025

From Ranking Member Waters:

1. Which of the following options best describes your self-identified race? (You may choose more than one.)
 - a. White or Caucasian

2. Which of the following options best describes your gender identity?
 - a. Woman



Answers for the Record -- Zoe Strickland

Subcommittee on Financial Institutions Hearing, titled: "Framework for the Future:

Reviewing Data Privacy in Today's Financial System."

August 7, 2025

Thank you for the opportunity to testify before the Subcommittee on June 5, 2025, regarding financial privacy and open banking, and to respond to the Chairman's July 24 letter which contained additional questions from members of Congress. We support the continued focus on privacy generally, and on the Dodd-Frank Act, the Final Rule issued by the CFPB to implement Section 1033 of the Act, and open banking.

In response to Ranking Member Waters' questions, I identify as a white woman (1a and 2a on the questions provided).

Rep. Gregory Meeks

FI Subcommittee Hearing: 6/4/2025

“Framework for the Future: Reviewing Data Privacy in Today's Financial System”

Ms. Strickland: As you know, the CFPB filed its motion of summary judgement last week in which it asks that the court vacate the Section 1033 rulemaking. Part of the Bureau's argument in support of its motion is that statute never gave the agency the authority to provide an open banking rule and that only consumers, or their agent, can access consumer's data. Thus, the Bureau seems to be redefining, overnight, the definition of consumer completely contrary to congressional intent and the agency's own interpretation of the definition since Dodd-Frank was enacted in 2010 and accepted across both Republican and Democratic administrations. **What consumer harms do you see in the CFPB's reversal? What data protections will consumers lose as a result of this ill-conceived reversal?**



Answers for the Record -- Zoe Strickland

Subcommittee on Financial Institutions Hearing, titled: "Framework for the Future:

Reviewing Data Privacy in Today's Financial System."

August 7, 2025

Thank you for the opportunity to testify before the Subcommittee on June 5, 2025, regarding financial privacy and open banking, and to respond to the Chairman's July 24 letter which contained additional questions from members of Congress. We support the continued focus on privacy generally, and on the Dodd-Frank Act, the Final Rule issued by the CFPB to implement Section 1033 of the Act, and open banking.

Below is my response to Congressman Meeks' questions. As I understand them, his questions relate to the policy implications and consumer impacts if the Dodd-Frank Act is interpreted to mean that consumers have a right of access to covered information held about them by data providers, but not to direct a designated third party to access their financial information on their behalf.

Direct access, without the ability to authorize data access, would render open banking essentially unworkable for consumers. Consider the steps and needs of the process.

- Consumers would have to request information from data providers. This is perhaps the most viable step, assuming data providers provide easy user interfaces that explain how the process works, such as what data is available and from which accounts.
- Consumers would need to receive and store information so that it is searchable, retrievable, and importantly, secured.
- Consumers would have to work to get information over to third parties. Options include consumers conducting data transfers, or providing third parties access into their systems, both of which raise logistical and security concerns.
- Consumers would have to periodically refresh and update information they have collected from data providers so that the information is current and accurate. How frequently can and should they do this? Daily, weekly, monthly? Policymakers should be aware that, under today's industry practices, information may be refreshed multiple times daily for certain open banking products to enhance the consumer experience.
- To maintain accuracy, consumers would need to provide refreshed information to appropriate third parties close in time from each time it is updated from data providers.
- Consumers would need to keep records of which information was provided from which data providers to which third parties, and update those records as information, accounts, or relationships change.

- Assuming the collection, storage, updates, and record-keeping all work effectively, there are numerous issues to solve with electronic data transfers, including formatting, authentication, and security functions. Most consumers do not have this expertise. Would the consumer have to engage to solve data formatting and other challenges between the data provider and third party, acting as the middleman?

The above describes some of the challenges with establishing open banking connections. Other issues will arise relating to customer service as well.

Consumers will also lose critical data protections. As two main examples, a vetting process and specific protections tailored to open banking may be lost. First, under the Final Rule, data providers are required to conduct verifications and risk assessments before they provide information to third parties designated by the consumer. If data providers do not perform this function, then the obligation falls onto consumers, who are ill-equipped for this role. What if the third party is a crook? Insolvent? Sells their data to the highest bidder? There are other laws and agencies that do offer some consumer protections, but these are not specific to open banking and tend to come into play after the data (or money) is transferred and when harm has occurred, not as a check beforehand. Policymakers should rightfully seek to avoid these harms from happening, which can be devastating to experience and difficult to remedy.

Second, the Final Rule creates a framework for relationships between the parties, as well as for each of their relationships with the consumer. The framework includes detailed privacy and security requirements for third parties and data aggregators acting on their behalf. The CFPB would have to reconsider how and whether to include these requirements if the open banking framework is changed or if the Rule is rescinded or invalidated.¹ The Rule's requirements create significant protections, including similar standards to banks on the security side, and rules for the collection, use, and retention of consumer data on the privacy side.² These privacy and security rules are important to apply to third parties – and to data aggregators too. The CFPB highlighted that sophisticated data analytics companies could undertake this role, and expressed a goal to ensure that open banking financial data is appropriately protected.

An important consideration for policymakers is that, during the time period when the rulemaking's status is unclear, consumers will be delayed in getting the benefits of open banking. Implementation for credit cards and bank accounts -- which are covered by the Final Rule -- will likely be delayed. The inclusion of other consumer financial products and services will also then be delayed. As a consumer, to get a clear picture of your overall financial health

¹ Some third parties and aggregators may be covered by other regulatory frameworks, such as the Gramm-Leach-Bliley Act or Federal Trade Commission rules. However, the 1033 Final Rule requirements, which are comprehensive, tailored, and modernized to current privacy principles, would be lost unless reapplied in some fashion.

² As described in FPF's comment and other letters to the CFPB, as well as during my remarks during the hearing, the Rule could be improved regarding how it treats data uses (such as secondary uses) and deidentified data.

and goals, you may well want to include more information. Main examples are investments, loans, and employment benefits. In the rulemaking process, many industry and consumer groups asked for these and other products to be included in the Rule, either initially or in future iterations. In addition, many consumer groups, as well as individual consumers, advocated for the inclusion of Electronic Benefits Transfer (EBT) under the open banking regulatory umbrella, arguing these individuals should also be able to manage their funds for their financial health and growth. These delays may result in the United States falling further behind other jurisdictions that are progressing their Open Finance and even Open Data rules.

In sum, if consumers' ability to authorize data access is lost, open banking would no longer function effectively under a legal or regulatory framework, and consumer harms would result. Voluntary industry efforts would presumably continue including via the Financial Data Exchange (FDX) and its data transfer standards based on Application Programming Interfaces (APIs). However, there is no guarantee this will occur. As an example, some data providers may forego APIs altogether, and continue to allow third parties to conduct screen scraping. As well documented, screen scraping is a terrible practice from a privacy and security perspective, whereby consumers give their online credentials to third parties that can then go onto a website and take any action the consumer is authorized to take. The Final Rule rightfully sunset this practice when covered data providers set up appropriate APIs that meet performance and security standards. As another example, as described above, third parties and data aggregators may walk away from open banking privacy and security rules. Open banking will likely take steps backwards from where it is today.

As described in my written testimony, there are specific topics where industry and consumer groups could provide guidance about how the Final Rule could be improved and perhaps preserved. We are happy to assist in those efforts, or in other capacities deemed useful by the Subcommittee. Thank you again for the opportunity to further comment on the value of open banking and to support its growth for consumers.

G:\M\19\BEATTY\BEATTY_011.XML

[~118H7483]

.....
 (Original Signature of Member)

119TH CONGRESS
 1ST SESSION

H. R. _____

To amend the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 to establish a Financial Agent Mentor-Protégé Program within the Department of the Treasury, and for other purposes.

 IN THE HOUSE OF REPRESENTATIVES

Mrs. BEATTY introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 to establish a Financial Agent Mentor-Protégé Program within the Department of the Treasury, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
 2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Advancing the Mentor-
 5 Protégé Program for Small Financial Institutions Act”.

G:\M\19\BEATTY\BEATTY_011.XML

2

1 **SEC. 2. ESTABLISHMENT OF FINANCIAL AGENT MENTOR-**
 2 **PROTÉGÉ PROGRAM.**

3 (a) IN GENERAL.—Section 308 of the Financial In-
 4 stitutions Reform, Recovery, and Enforcement Act of
 5 1989 (12 U.S.C. 1463 note) is amended by adding at the
 6 end the following new subsection:

7 “(d) FINANCIAL AGENT MENTOR-PROTÉGÉ PRO-
 8 GRAM.—

9 “(1) IN GENERAL.—The Secretary of the
 10 Treasury shall establish a program to be known as
 11 the ‘Financial Agent Mentor-Protégé Program’ (in
 12 this subsection referred to as the ‘Program’) under
 13 which a financial agent designated by the Secretary
 14 or a large financial institution may serve as a men-
 15 tor, under guidance or regulations prescribed by the
 16 Secretary, to a small financial institution to allow
 17 such small financial institution—

18 “(A) to be prepared to perform as a finan-
 19 cial agent; or

20 “(B) to improve capacity to provide serv-
 21 ices to the customers of the small financial in-
 22 stitution.

23 “(2) OUTREACH.—The Secretary shall hold
 24 outreach events to promote the participation of fi-
 25 nancial agents, large financial institutions, and small

1 financial institutions in the Program at least once a
2 year.

3 “(3) EXCLUSION.—The Secretary shall issue
4 guidance or regulations to establish a process under
5 which a financial agent, large financial institution,
6 or small financial institution may be excluded from
7 participation in the Program.

8 “(4) REPORT.—The Office of Minority and
9 Women Inclusion of the Department of the Treasury
10 shall include in the report submitted to Congress
11 under section 342(e) of the Dodd-Frank Wall Street
12 Reform and Consumer Protection Act information
13 pertaining to the Program, including—

14 “(A) the number of financial agents, large
15 financial institutions, and small financial insti-
16 tutions participating in such Program; and

17 “(B) the number of outreach events de-
18 scribed in paragraph (2) held during the year
19 covered by such report.

20 “(5) DEFINITIONS.—In this subsection:

21 “(A) FINANCIAL AGENT.—The term ‘fi-
22 nancial agent’ means any national banking as-
23 sociation designated by the Secretary of the
24 Treasury to be employed as a financial agent of
25 the Government.

G:\M\19\BEATTY\BEATTY_011.XML

4

1 “(B) LARGE FINANCIAL INSTITUTION.—

2 The term ‘large financial institution’ means any
3 entity regulated by the Comptroller of the Cur-
4 rency, the Board of Governors of the Federal
5 Reserve System, the Federal Deposit Insurance
6 Corporation, or the National Credit Union Ad-
7 ministration that has total consolidated assets
8 greater than or equal to \$50,000,000,000.

9 “(C) RURAL DEPOSITORY INSTITUTION.—

10 The term ‘rural depository institution’ means a
11 depository institution (as defined in section 3 of
12 the Federal Deposit Insurance Act)—

13 “(i) with total consolidated assets of
14 less than \$10,000,000,000; and

15 “(ii) located in a rural area, as de-
16 fined under section 1026.35(b)(2)(iv)(A) of
17 title 12, Code of Federal Regulations.

18 “(D) SMALL FINANCIAL INSTITUTION.—

19 The term ‘small financial institution’ means—

20 “(i) any entity regulated by the
21 Comptroller of the Currency, the Board of
22 Governors of the Federal Reserve System,
23 the Federal Deposit Insurance Corpora-
24 tion, or the National Credit Union Admin-

G:\M\19\BEATTY\BEATTY_011.XML

5

1 istration that has total consolidated assets
2 lesser than or equal to \$2,000,000,000;
3 “(ii) a minority depository institution;
4 or
5 “(iii) a rural depository institution.”.
6 (b) EFFECTIVE DATE.—This Act and the amend-
7 ments made by this Act shall take effect 90 days after
8 the date of the enactment of this Act.

G:\M\19\GREETE\GREETE_040.XML

[118H4116RH]

.....
 (Original Signature of Member)

119TH CONGRESS
 1ST SESSION

H. R. _____

To amend the Federal Deposit Insurance Act to require reports on the use of the systemic risk authority applicable to winding up a failed insured depository institution, and for other purposes.

 IN THE HOUSE OF REPRESENTATIVES

Mr. GREEN of Texas introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Federal Deposit Insurance Act to require reports on the use of the systemic risk authority applicable to winding up a failed insured depository institution, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
 2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Systemic Risk Author-
 5 ity Transparency Act”.

G:\M\19\GREETE\GREETE_040.XML

2

1 **SEC. 2. BANK FAILURE TRANSPARENCY RELATED TO SYS-**
 2 **TEMIC RISK EXCEPTION.**

3 (a) GAO REVIEW.—Section 13(c)(4)(G)(iv) of the
 4 Federal Deposit Insurance Act (12 U.S.C.
 5 1823(c)(4)(G)(iv)) is amended to read as follows:

6 “(iv) GAO REVIEW.—

7 “(I) IN GENERAL.—The Comp-
 8 troller General of the United States
 9 shall, not later than later than 60
 10 days after a determination is made
 11 under clause (i), and again 180 days
 12 thereafter, review and report to the
 13 Congress on the determination under
 14 clause (i), including—

15 “(aa) the basis for the deter-
 16 mination;

17 “(bb) the purpose for which
 18 any action was taken pursuant to
 19 such clause;

20 “(cc) the likely effect of the
 21 determination and such action on
 22 the incentives and conduct of in-
 23 sured depository institutions and
 24 uninsured depositors;

25 “(dd) any mismanagement
 26 by the executives and board of

G:\M\19\GREETE\GREETE_040.XML

3

1 the insured depository institution
2 that contributed to the failure of
3 the insured depository institu-
4 tion;

5 “(ee) a review of the com-
6 pensation practices of the insured
7 depository institution;

8 “(ff) any supervisory or reg-
9 ulatory shortcomings with respect
10 to the appropriate Federal bank-
11 ing agency of the insured deposi-
12 tory institution;

13 “(gg) any actions taken by
14 the Federal banking regulators,
15 Financial Stability Oversight
16 Council, Treasury Department,
17 and other relevant financial regu-
18 lators in relation to the failure of
19 the insured depository institu-
20 tion; and

21 “(hh) any additional rel-
22 evant entities or activities that
23 may have contributed to the fail-
24 ure of the insured depository in-
25 stitution, including with respect

G:\M\19\GREETE\GREETE_040.XML

4

1 to auditing, accounting, credit
2 rating agencies, investment bank
3 underwriters, and emergency li-
4 quidity options such as loans
5 from the Federal reserve banks
6 or advances through the Federal
7 Home Loan Bank system.

8 “(II) RULE OF CONSTRUC-
9 TION.—Nothing in this clause or a re-
10 port issued pursuant to this clause
11 may be construed to limit the author-
12 ity of a Federal agency to enforce vio-
13 lations of Federal statutes, rules, or
14 orders.”.

15 (b) APPROPRIATE FEDERAL BANKING AGENCY RE-
16 PORT.—Section 13(c) of the Federal Deposit Insurance
17 Act (12 U.S.C. 1823(c)) is amended by adding at the end
18 the following:

19 “(12) APPROPRIATE FEDERAL BANKING AGEN-
20 CY REPORT.—

21 “(A) IN GENERAL.—The appropriate Fed-
22 eral banking agency of an insured depository
23 institution about which a determination is made
24 under paragraph (4)(G)(i) shall, not later than
25 90 days after the date of such determination,

1 and again 210 days thereafter, submit a report
2 to the Congress that discloses the following:

3 “(i) Subject to such redactions as the
4 appropriate Federal banking agency deter-
5 mines appropriate of personally identifiable
6 information about customers and other fi-
7 nancial institutions (as such term is de-
8 fined under section 11(e)(9)(D)), all—

9 “(I) reports of examination and
10 inspection that relate to the failed in-
11 sured depository institution in the
12 previous 3-year period;

13 “(II) formal communications of a
14 material supervisory determination
15 conveyed to the failed insured deposi-
16 tory institution in the previous 3-year
17 period; and

18 “(III) any additional exam re-
19 ports and correspondence that the ap-
20 propriate Federal banking agency de-
21 termines may be relevant to the fail-
22 ure of the insured depository institu-
23 tion.

24 “(ii) An examination of any mis-
25 management by the executives and board

G:\M\19\GREETE\GREETE_040.XML

6

1 of the insured depository institution that
2 contributed to the failure of the insured
3 depository institution.

4 “(iii) Any supervisory or regulatory
5 shortcomings by such appropriate Federal
6 banking agency with respect to the insured
7 depository institution.

8 “(iv) Any dynamics that the appro-
9 priate Federal banking agency determines
10 may have contributed to the failure of the
11 insured depository institution.

12 “(v) Any supervisory, regulatory, and
13 legislative recommendations such appro-
14 priate Federal banking agency may have to
15 improve the safety and soundness of simi-
16 larly situated insured depository institu-
17 tions, the banking system, and financial
18 stability.

19 “(B) PROTECTION OF SENSITIVE INFOR-
20 MATION.—

21 “(i) EFFECT ON PRIVILEGE.—The
22 provision of any information by a Federal
23 banking agency under this paragraph may
24 not be construed as—

G:\M\19\GREETE\GREETE_040.XML

7

1 “(I) waiving, destroying, or oth-
2 erwise affecting any privilege applica-
3 ble to the information; or

4 “(II) waiving any exemption ap-
5 plicable to the information under sec-
6 tion 552 of title 5 United States Code
7 (commonly known as the ‘Freedom of
8 Information Act’).

9 “(ii) TRANSPARENCY.—

10 “(I) IN GENERAL.—A Federal
11 banking agency shall publish mate-
12 rials contained in a report required
13 under subparagraph (A) to the fullest
14 extent possible to promote trans-
15 parency.

16 “(II) CONSULTATION ON OMIT-
17 TING MATERIALS.—If a Federal bank-
18 ing agency determines particular ma-
19 terials described under subclause (I)
20 should not be published, the Federal
21 banking agency shall consult with the
22 chair and ranking member of the
23 Committee on Financial Services of
24 the House of Representatives and the
25 chair and ranking member of the

G:\M\19\GREETE\GREETE_040.XML

8

1 Committee on Banking, Housing, and
 2 Urban Affairs of the Senate.

3 “(III) OMITTING MATERIALS.—
 4 If, after the consultation required
 5 under subclause (II), the Federal
 6 banking agency determines there is a
 7 substantial public interest in not pub-
 8 lishing such materials, the Federal
 9 banking agency shall provide those
 10 materials to the Committee on Finan-
 11 cial Services of the House of Rep-
 12 resentatives and the Committee on
 13 Banking, Housing, and Urban Affairs
 14 of the Senate with a written expla-
 15 nation describing the reasons for not
 16 publishing those materials.

17 “(iii) PRIVILEGE.—For purposes of
 18 this subparagraph, the term ‘privilege’ in-
 19 cludes any work-product, attorney-client,
 20 or other privilege recognized under Federal
 21 or State law.

22 “(C) REPORT EXTENSION.—A Federal
 23 banking agency may extend a deadline de-
 24 scribed under subparagraph (A) for an addi-
 25 tional 60 days, if the Federal banking agency—

G:\M\19\GREETE\GREETE_040.XML

9

1 “(i) faces ongoing circumstances that
2 require the Federal banking agency to
3 prioritize activities to promote stability of
4 the U.S. banking system; and

5 “(ii) notifies the Congress of such ex-
6 tension and the reasons for such extension.

7 “(D) CONSOLIDATED REPORTS.—A Fed-
8 eral banking agency may consolidate multiple
9 reports required under this paragraph so long
10 as the individual reports being consolidated all
11 meet the timing requirements under this para-
12 graph.

13 “(E) RULE OF CONSTRUCTION.—Nothing
14 in this paragraph or reports or materials pro-
15 vided pursuant to this paragraph may be con-
16 strued to limit the authority of a Federal agen-
17 cy to enforce violations of Federal statutes,
18 rules, or orders.”.

