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.