February 7, 2023

The Honorable Patrick McHenry
Chairman
U.S. House Committee on
Financial Services

The Honorable Maxine Waters
Ranking Member
U.S. House Committee on
Financial Services

The Honorable Andy Barr
Chairman
House Subcommittee on Financial
Institutions and Monetary Policy
4340 O'Neill House Office Building
Washington, DC 20515

The Honorable Bill Foster
Ranking Member
House Subcommittee on Financial
Institutions and Monetary Policy
4340 O'Neill House Office Building
Washington, DC 20515

RE: Hearing on "Revamping and Revitalizing Banking in the 21st Century"

Dear Chairman McHenry, Ranking Member Waters, Chairman Barr, and Ranking Member Foster:

The Main Street Privacy Coalition ("MSPC") has long advocated for national data privacy and security regulation and appreciates this opportunity to provide our views on financial data privacy, which is being considered as part of the Financial Institutions Subcommittee's February 8th hearing on Revamping and Revitalizing Banking in the 21st Century.

The MSPC is comprised of 19 national trade associations that together represent more than a million American businesses – a broad array of companies that line America's Main Streets. From retailers to Realtors®, hotels to home builders, grocery stores to restaurants, gas stations to travel plazas, and self-storage to convenience stores, including franchise establishments, MSPC member companies interact with consumers day in and day out. Our members' businesses can be found in every town, city and state in our nation, providing jobs, supporting our economy and serving Americans as a vital part of their communities. Collectively, the industries that MSPC trade groups represent directly employ approximately 34 million Americans and constitute over one-fifth of the U.S. economy by contributing $4.5 trillion (or 21.8%) to the U.S. gross domestic product.[1]

The MSPC advocates for federal privacy legislation that meets basic core principles including the following:

- **Establishing Uniform Nationwide Rules and Enforcement for Data Privacy** – We should have a sensible, uniform federal framework for data privacy legislation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws by enacting a set of nationwide rules for all

[1] Information on the MSPC including a full list of its members can be found at https://mainstreetprivacy.com/about/.

businesses handling consumers' personal data is necessary to achieve the important, national public policy goal of establishing uniform consumer privacy protections.

- **Industry Neutrality and Equal Protection for Consumers Across Business Sectors** – Federal data privacy frameworks should apply requirements to all industries that handle personal data and not place a disproportionate burden on certain sectors of the economy while simultaneously alleviating other sectors from providing equal protection of consumer data. An equivalent data privacy standard should apply, regardless of whether a business directly collected data from a consumer or obtained it in a business-to-business transaction.

- **Direct Legal Obligations (Rather than Contractual Requirements Alone) for All Entities that Handle Consumer Data** – Effective consumer protection law cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. Data service providers and other third parties need direct statutory obligations to ensure they comply with the relevant privacy scheme, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of businesses.

- **Preservation of Customer Rewards and Benefits** – Any federal data privacy framework should preserve the ability of consumers and businesses to voluntarily establish mutually beneficial business-customer relationships and set the terms of those relationships. Legislation should include safe harbors to ensure that consumers can purchase, or otherwise obtain, the goods and services they want by taking advantage of benefits, incentives or enhanced services they earn from being loyal customers, even if other customers choose not to engage in such programs.

- **Transparency and Customer Choice** – Consumers deserve to know what categories of personal data businesses collect and how that data is generally used. These policies should be clearly disclosed in company privacy policies and readily accessible to consumers. These obligations should apply to all businesses handling consumers' personal data, including service providers, third parties, and financial services businesses.

- **Accountability for Business's Own Actions** – Privacy legislation should not include terms that could potentially expose businesses, including contractors and franchises, to liability for the actions or noncompliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if other types of businesses do not fulfill their own obligations under the regulation.

- **Data Security Standards** – A federal data privacy law should include a reasonable data security standard for all businesses handling consumer data, as well as a uniform process for businesses suffering a data security breach to notify affected individuals. Currently, consumer-facing industry sectors are required to comply with 54 state and U.S. territorial laws on data breach notification requirements, and nearly half of the states have enacted data security laws. However, financial institutions and service providers are often exempt from these state breach notice requirements. All businesses handling consumers' data should be statutorily required to protect personal data and provide notice of their own security breaches when they occur.

Particularly with respect to any privacy legislation that the Financial Services Committee will consider, we believe it is important to be industry-neutral and provide equal protection for consumers across business sectors. To do this, the protections applicable to the financial services industry would need to be significantly updated consistent with contemporary privacy laws such as those that have passed in states in recent years.

To illustrate these challenges, we have enclosed with this letter a chart comparing the basic protections in privacy laws in Europe and California to the current regime that applies to the financial services industry through the Gramm Leach Bliley Act ("GLBA"). The chart makes clear that GLBA does not protect privacy in the way that most people have now come to expect.

This Committee has an opportunity to update the law and rectify the imbalance that today, in many states, causes Americans to have far more extensive privacy protections when they buy an ice cream cone than they do when they engage in sensitive financial transactions involving their life savings with their financial institution.

We look forward to the opportunity to work with the Committee constructively going forward to address these issues so that any privacy legislation it considers holds all industry sectors to equivalent standards based upon the sensitivity of the data they collect and handle.

Sincerely,

Main Street Privacy Coalition

Attachment

cc: Members of the Financial Institutions and Monetary Policy Subcommittee of the U.S. House of Representatives Committee on Financial Services

PRIVACY LAW COMPARISON CHART

Consumer Privacy Rights regarding their Personal Information	GDPR (2016)	CCPA (2018)*	GLBA (1999)	Notes
Transparency	✓	✓	!	GLBA: partial transparency; only annually-*mailed* disclosure notice of data uses (w/ some exceptions)
Control (Choices)	✓	✓	✗	GLBA: no meaningful control; opt out *only for* non-affiliate sharing that is not excepted (e.g., some marketing)
Access	✓	✓	✗	
Correction	✓	✓	✗	
Deletion	✓	✓	✗	
Portability	✓	✓	✗	
Breach Notification	✓	!	!	CCPA: CA breach law requires notice, but not CCPA GLBA: Not required (guidance *only* says "should" notify)
Opt-Out of Direct Marketing	✓	✗	✗	GDPR: opt out of processing for direct marketing GLBA: joint marketing agreements override opt-out
Opt-Out of Data Sharing for Targeted Ads	✗	✓	✗	CCPA: opt out of data sharing to third parties for purposes of processing data for targeted advertising
Opt-Out of Data "Sales"	✗	✓	✗	CCPA: opt out of data "sales" to third parties for purposes beyond marketing/advertising (w/ some exceptions)

CCPA, as amended by CPRA (2020)