BANK POLICY INSTITUTE

March 15, 2019

Via Electronic Mail to submissions@banking.senate.gov

Hon. Mike Crapo, Chairman
Hon. Sherrod Brown, Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate
534 Dirksen Senate Office Building
Washington, D.C. 20510-6075

Dear Chairman Crapo and Ranking Member Brown:

The Bank Policy Institute ("BPI")[1] appreciates the opportunity to respond to your February 13, 2019 invitation for stakeholder feedback on the collection, use, and protection of personal information by financial regulators and private companies. We appreciate the Committee's interest in protecting personal information.[2] BPI shares your commitment to safeguarding personal information and protecting the interests of all Americans in understanding and appropriately controlling how their information is collected and used.

Financial services firms have long been subject to comprehensive federal, state, and foreign standards relating to the privacy and security of customer information. The need to protect the confidentiality and privacy of customer information has been deeply embedded in bank policies and operations for many years. Indeed, few other sectors have as extensive a set of legal and regulatory requirements that, together with industry standards, govern the collection, use, control, and transparency of customer data. These requirements include the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations, including the Interagency Guidelines Establishing Information Security Standards ("Interagency Guidelines"), which require financial institutions to adopt robust information security programs with administrative, technical, and physical safeguards.

This submission surveys the regulation of financial institutions' collection and use of personal information. First, we provide an overview of how and why banks collect and use personal information, consistent with applicable data security and privacy laws. Second, the submission outlines the comprehensive federal legal framework that has long governed how banks collect, use, and protect consumer information. Third, we provide an overview of various state laws and industry guidelines that exist in addition to the robust federal framework. Finally, we explain why a

---

1 The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

2 In light of the numerous definitions in different federal, state, local, and foreign laws, and the variations in the types of data our member banks collect (e.g., including data about both individual consumers and institutional customers), this response uses the term "personal information" to refer to "nonpublic personal information" within the meaning of the Gramm-Leach-Bliley Act ("GLBA"), *i.e.*, "personally identifiable financial information" that a financial institution collects about a consumer in connection with providing a financial product or service. *See* 15 U.S.C. § 6809(4) and implementing regulations.

uniform national standard for data security and privacy would enhance consumer protections by clarifying consumers' rights and by defining compliance obligations to maximize effectiveness.

As trusted custodians of consumers' personal data, and as stewards of the GLBA, the Fair Credit Reporting Act ("FCRA"), and various other applicable statutory and regulatory banking and consumer protection laws, the banking industry is very focused on these issues. We are committed to continuing to consider ways in which Congress and industry can work together to enhance consumer protections, control, accuracy, and transparency.

I. Banks' Collection and Use of Consumer Information

Much of the present policy discussion about the privacy of personal information centers on the collection and use of personal information in the technology industry and in other industries subject to relatively little data and privacy regulation. Financial institutions face an entirely different regulatory regime. Their collection and use of personal information is subject to robust and thorough regulation and oversight, at essentially every stage of the data lifecycle. In fact, much of the personal information collected by financial institutions is itself due to regulatory compliance requirements—for example, requirements that banks verify the identity of a consumer prior to providing services. Congress long ago enacted comprehensive regimes governing financial institutions' collection and use of financial information, in recognition of the distinctive functions of financial institutions. As a result, the banking sector is often regarded as a model for data security and privacy governance and oversight.

Banks obtain personal information in connection with providing financial products or services to consumers, including information that is required to establish and maintain an account, information collected for the purpose of making credit eligibility determinations, and information collected to comply with "Know Your Customer" ("KYC") requirements.[3] This information is obtained through several channels, including (i) from consumers in applications, and (ii) from consumer reporting agencies ("CRA") (such as Equifax, Experian, TransUnion) for the purpose of making a credit eligibility determination.

Banks also collect and maintain other consumer account information, such as authentication-related information (e.g., usernames and passwords to online accounts or biometric data that may be used for authentication purposes), financial account numbers (for accounts maintained at the financial institution as well as accounts at other institutions linked by the account holder), transaction and payment history, and check images. Banks also may obtain personal information from third-party sources to support marketing directed at existing customers, including marketing of products or services that may be of particular interest to those consumers. Finally, banks gather information on consumers' use of banks' digital channels, including mobile banking applications and bank websites.

Banks generally use personal information to inform an initial decision about whether to offer a consumer a financial product and at what price or rate. Once a consumer establishes a relationship, banks may use personal information to protect customers' accounts from fraud and to enhance the customer experience through tailored product offerings. Banks also gather and use personal information to respond to customer requests and to comply

[3] Although the term "KYC" is not used in regulations, it is generally used in industry and regulator parlance to refer to institutions' obligations to collect, analyze, and use information about their customers to comply with various anti-money laundering and sanctions requirements that require financial institutions to understand, to some extent, the nature and identities of the parties with whom or on whose behalf they are conducting financial transactions.

with regulatory requirements (e.g., anti-money laundering laws,[4] economic sanctions regimes,[5] identity protection requirements,[6] reporting obligations under the Home Mortgage Disclosure Act,[7] and tax laws[8]).

Banks also use personal information in accordance with the requirements of the GLBA Privacy Rule[9] and the FCRA.[10] For example, financial institutions:

- Provide payment history and other information regarding customer loan accounts to CRAs;
- Share personal information that they have collected about an individual consumer with that consumer in accordance with consumer rights to access information related to financial products or services at the consumer's request;[11]
- Share personal information in furtherance of fraud prevention efforts;[12]
- Share data with third parties in response to specific customer requests or when the customer has otherwise authorized the service provider (e.g., tax preparers) to access the information; and
- Share data with third-party service providers, such as bill-pay providers, following third-party service provider due diligence and pursuant to contracts that include provisions protecting the confidentiality and privacy of customer personal information, including prohibiting disclosure or use other than as necessary to carry out the contracted service.[13]

Finally, banks may share personal information among their affiliates for various purposes, as governed by the GLBA and FCRA,[14] subject to consumer opt-out.[15]

---

4 31 C.F.R. subtit. B, ch. X; *see* Federal Financial Institutions Examination Council ("FFIEC"), *Bank Secrecy Act/Anti-Money Laundering Examination Manual, Customer Due Diligence – Overview* (2018), www.ffiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf.

5 *See, e.g.*, 31 C.F.R. § 544.405(a) (Weapons of Mass Destruction Proliferators Sanctions Regulations); 31 C.F.R. § 584.405(a) (Magnitsky Act Sanctions Regulations); OFAC Specially Designated Nationals and Blocked Persons List, www.treasury.gov/ofac/downloads/sdnlist.pdf; U.S. Dep't of Treasury, Sanctions Programs and Country Information, www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

6 *See* 12 C.F.R. pt. 41, subpt. J.

7 12 U.S.C. §§ 2801-2810; 12 C.F.R. pt. 1003.

8 *See, e.g.*, 26 U.S.C. §§ 1471-1474.

9 12 C.F.R. pt. 1016.

10 15 U.S.C. §§ 1681-1681x.

11 12 U.S.C. § 5533.

12 15 U.S.C. § 6802(e)(3)(B).

13 *See* Office of the Comptroller of the Currency, *Risk Management Guidance*, OCC Bulletin 2013-29 (2013) , www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html ("OCC Bulletin"); Fed. Deposit Ins. Corp., *Guidance for Managing Third-Party Risk*, FIL-44-2008 (2008), www.fdic.gov/news/news/financial/2008/fil08044.html; 12 C.F.R. § 1016.13(a)(1)(ii).

14 *See, e.g.*, 15 U.S.C. § 1681s-3(a).

15 *See id.*; 12 C.F.R. § 1016.6(a)(7).

II. Federal Law Provides a Comprehensive Framework for Financial Institutions' Handling and Protection of Personal Information

Federal data security and privacy statutes and regulations comprehensively and specifically[16] regulate financial institutions' collection and use of personal information, as well as related data security requirements.

GLBA and Implementing Regulations

The GLBA and its implementing regulations establish the principal federal requirements governing banks' protection of customer privacy and information security.

The GLBA privacy standards require financial institutions to inform consumers about how their data is collected and shared and, in certain circumstances, to allow consumers to opt out of information sharing. The GLBA provides a number of consumer protections, including prescribing when customer information may be disclosed to nonaffiliated third parties and when financial institutions must allow customers an opportunity to opt out of information sharing. For example, financial institutions are prohibited from disclosing a consumer's nonpublic personal information to a nonaffiliated third party unless: (1) the consumer has received notice and an opportunity to opt out of such sharing and has not opted out; or (2) an exception permitting the disclosure applies, such as to process transactions or maintain or service accounts.[17] Exceptions to the opt-out right are generally limited to the types of disclosures that are necessary to provide the financial product or service. For instance, to process a credit card transaction, a bank must communicate its authorization for the transaction to the relevant payment card network or merchant.

In addition, the GLBA Safeguards Rule and associated guidance require banks to develop, implement, and maintain administrative, technical, and physical safeguards designed to (i) protect the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of such records and information; and (iii) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to consumers.[18]

Pursuant to the Safeguards Rule, banks are required to develop and adhere to written information security programs, tailored to each institution's size, complexity, and risk. These written programs incorporate continuous improvement through evaluation of threats, industry events, and asset values. Banks use a wide range of physical and technical safeguards around the collection, storage, use, access, and delivery of information, such as physical access restrictions, firewalls, intrusion protection and threat monitoring tools, and encryption technologies. Banks' information security programs are also required to follow the requirements laid out in the prudential regulators' Interagency Guidelines,[19] which require those programs to include (i) board of director involvement, including at least annual reporting to the board; (ii) risk assessment; (iii) risk management and control; (iv) oversight of service providers; (v) an incident response program; and (vi) periodic updating.[20]

---

16 In addition to statutory and regulatory regimes that apply specifically to financial institutions, certain bank activities may also be subject to other generally-applicable or sector-specific data security and privacy laws.

17 15 U.S.C. § 6802(b).

18 15 U.S.C. § 6801(b).

19 *See, e.g.*, 12 C.F.R. pt. 30, app. B (as incorporated into regulations for national banks).

20 *See, e.g.*, *id.* § III.

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice (the "Interagency Guidance") expands upon the response program requirements in the Interagency Guidelines. The Interagency Guidance requires banks to adopt policies that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to customer information systems, including making reports to regulatory and law enforcement agencies and notifying customers when warranted.[21]

Banks' data security policies and practices must also comply with the Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbook and various guidance documents issued by the FFIEC agencies. Banks' data security programs are generally required to address issues related to governance; information security program management (including risk identification, measurement, mitigation, monitoring, and reporting); security operations; and information security program effectiveness, as outlined in detail in the FFIEC IT Examination Handbook: Information Security Booklet.[22] Other parts of the FFIEC IT Examination Handbook include relevant information security requirements and standards (*e.g.*, Booklets on Outsourcing Technology Services, E-Banking, and Retail Payment Systems). The FFIEC also regularly publishes guidance based on evolving threats and best practices,[23] which banks use to enhance their information security programs.[24]

Financial regulators have also promulgated regulations governing banks' outsourcing of activities to third parties, including activities related to the collection and use of personal information. Such activities must be performed in a safe and sound manner in compliance with all laws that would apply if the bank were performing these functions directly. Banks also must control any risks arising from their relationships with third parties to the same extent as if the activities were carried out by the institution itself.[25]

---

21 *See, e.g.*, *id.* supp. A § II.A.

22 *See* FFIEC IT Examination Handbook, IT Booklet, *Information Security* (Sept. 2016), ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf.

23 *See, e.g.*, FFIEC, *Joint Statement on Cyber Attacks Compromising Credentials*, www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf; FFIEC, *Joint Statement on Destructive Malware*, www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf; FFIEC, *Joint Statement on Cyber Attacks Involving Extortion*, www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf; FFIEC, *Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs*, www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20Cyber%20Insurance%20FINAL.pdf.

24 In addition to more specific IT and data security standards, banks must also comply with broader risk management standards as applied in the data security context. *See, e.g.*, Office of the Comptroller of the Currency ("OCC") Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches, 12 C.F.R. pt. 30, app. D.; Federal Reserve Board's enhanced prudential standards under Regulation YY, 12 C.F.R. pt. 252. While applicable to various risks beyond cyber, regulators have noted that "operational risk," as covered by these standards, includes cybersecurity. *See, e.g.*, Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Exchequer Club (Sept. 18, 2013), www.occ.treas.gov/news-issuances/speeches/2013/pub-speech-2013-138.pdf ("[A]s important as it is to look back and deal with issues arising from the financial crisis, it is equally urgent that we look ahead and stay on top of emerging threats . . . . The particular issue I have in mind . . . involves the operational risk posed by cyberattacks. . . . It's important to remember that cybersecurity is a safety and soundness issue, and more specifically, an example of operational risk."). The importance of cybersecurity to safety and soundness is discussed in testimony; *Cybersecurity Regulatory Harmonization: Hearing before the Committee on Homeland Security & Governmental Affairs*, Senate, 115th Cong. (2017) (Testimony of Christopher F. Feeney): www.hsgac.senate.gov/imo/media/doc/Testimony-Feeney-2017-06-21.pdf.

25 *See* OCC Bulletin *supra* note 39; Fed. Deposit Ins. Corp., *Guidance for Managing Third-Party Risk supra* note 39; FFIEC, IT Examination Handbook, IT Booklet, *Outsourcing Technology Services Booklet* (2004), ithandbook.ffiec.gov/media/274841/ffiec_itbooklet_outsourcingtechnologyservices.pdf ("Outsourcing Technology Services Booklet").

Identity Theft Red Flags

Regulations also require banks to detect and prevent attempted identity theft. The Identity Theft Red Flags Rule requires covered financial institutions to develop and implement a written identity theft prevention program, designed to detect, prevent, and mitigate identity theft in connection with opening or maintaining certain financial accounts (including accounts primarily for personal, family, or household purposes).[26] Identity theft prevention programs are required to include policies and procedures to identify, detect, and respond to "red flags" – i.e., a "pattern, practice, or specific activity that indicates the possible existence of identity theft."[27] Further details on the requirements of these programs, including risk factors financial institutions should consider in identifying red flags, and steps financial institutions should take to prevent and mitigate identity theft, are included in the Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.[28] For example, these Interagency Guidelines require financial institutions to compare personal information provided by a consumer to information from external sources (e.g., to confirm whether the Social Security Number provided has been issued or is associated with a deceased individual according to the Social Security Administration's Death Master File).[29]

Right to Financial Privacy Act

The Right to Financial Privacy Act ("RFPA") restricts the extent to which banks can share financial records with the federal government without customer authorization, including in response to an administrative subpoena or summons, a valid search warrant, a judicial subpoena, or a formal written request such as a civil investigative demand, and subjects banks to certain recordkeeping requirements.[30]

Information Sharing and Industry Coordination

Federal law also promotes robust industry collaboration and cyber threat information sharing. As with many aspects of data security, information-sharing is an area where the financial services industry has served as a model for other industries. The Financial Services Information Sharing and Analysis Center ("FS-ISAC") is the primary information-sharing mechanism for the financial services industry, and the designated Information Sharing and Analysis Organization maintained in response to Presidential Directives and Executive Orders, as well as the Cybersecurity Act of 2015. These authorities encourage public-private security information sharing, often with a particular emphasis on critical infrastructure sectors, such as the financial services sector. Both the Department of the Treasury and the Department of Homeland Security (including the United States Computer Emergency Readiness Team) use the FS-ISAC to disseminate critical security information to the financial services sector. And banks often work collaboratively with public and private sector partners to identify and share cyber threat intelligence and prevent data loss or corruption through early warning systems.

---

26 *See* 12 C.F.R. pt. 41, subpt. J.

27 *Id.* §§ 41.90(b)(10), (d)(2).

28 *Id.* at app. J.

29 *Id.* at app. J, supp. A.

30 12 U.S.C. §§ 3401-3422.

Industry Standards

Many banks also adhere to various public and private standards. These include:

- The NIST Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Cybersecurity Framework"), which was developed through a public-private collaboration. Designed as a risk management framework for owners and operators of critical infrastructure, it provides guidelines to assess, evaluate, and enhance their cybersecurity risk management program;[31]
- The Financial Services Sector Coordinating Council (FSSCC) developed Cybersecurity "Profile," which is a complementary, publicly available non-commercial cybersecurity assessment tool that extends the NIST Cybersecurity Framework, incorporating and synthesizing the myriad of financial services regulatory expectations, into a set of exam-ready assessment questions. The FSSCC works collaboratively with key government agencies to protect U.S. critical infrastructure from cyber and physical incidents. Developed in coordination with numerous financial services regulatory agencies and NIST, with broad subsector representation (e.g., banking, insurance, asset management, market utilities, broker-dealers), the FSSCC held more than 50 working sessions[32], which culminated in the release of the Profile, Version 1.0, on October 25, 2018.[33]
- The Payment Card Industry Data Security Standards ("PCI-DSS"), which require entities that store, process, or transmit payment card data and sensitive card-related authentication data to implement specific data security standards;[34]
- The Sheltered Harbor Specification, which outlines operational and technical requirements for protecting consumer account data;[35] and
- The Financial Data Exchange ("FDX") which is a nonprofit industry-led collaboration dedicated to unifying incumbent and new entrant financial industry players around a common, interoperable, royalty-free standard that allows consumers and businesses to share their data without the sharing or storing of login credentials with third parties.[36]

---

31 NIST, *Framework for Improving Critical Infrastructure Cybersecurity* v1.1 (2018), nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

32 These working sessions included over 150 financial institutions and trade associations and 300 subject matter experts.

33 The Profile materials, an overview, and responses to frequently asked questions can be accessed on BPI's website at bpi.com/financial-services-sector-cybersecurity-profile/.

34 PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures* v.3.2.1 (May 2018), www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

35 *See* Sheltered Harbor, *How It Works*, shelteredharbor.org/how-it-works. The Sheltered Harbor initiative, a not-for-profit, industry-led initiative housed in an FS-ISAC subsidiary founded by 34 financial institutions, clearing houses, core processors, and industry associations with the goal of enhancing the protection of the retail financial services industry, and which has issued the Sheltered Harbor Specification that outlines operational and technical requirements for protecting consumer account data. Sheltered Harbor, *Frequently Asked Questions*, shelteredharbor.org/sh-faqs.

36 Financial Data Exchange, financialdataexchange.org/.

III. Banks Are Subject to An Array of Divergent State Law Data Security and Privacy Requirements

Despite this comprehensive federal regulatory scheme, banks are also subject to a web of state laws governing the security and privacy of personal information. For example, as applicable, banks may be subject to:

- New York's Cybersecurity Requirements for Financial Services Companies, which require covered financial institutions to maintain cybersecurity programs and policies, based on the institution's risk assessment, to address, for example, data governance, systems and network security and monitoring, customer data privacy, vendor management, and incident response;[37]
- Massachusetts' Standards for the Protection of Personal Information of Residents of the Commonwealth, which establish minimum standards for safeguarding personal information to ensure confidentiality, protect against threats or hazards, and protect against unauthorized access;[38]
- The California Financial Information Privacy Act ("CalFIPA"), which explicitly states that it is intended to provide greater protection than the GLBA, and prohibits financial institutions from selling, sharing, transferring, or otherwise disclosing nonpublic personal information to or with any nonaffiliated party without the explicit consent of the consumer or unless an enumerated exception applies;[39]
- The California Consumer Privacy Act ("CCPA"), a sweeping privacy law scheduled to take effect in 2020, which provides consumers with broad notice, access, and deletion rights concerning many types of personal information;[40]
- State laws governing the collection and storage of certain payment card data;[41] and
- State data disposal laws, which have been enacted in over half of the states and require businesses to use specific data disposal and/or destruction requirements for digital and/or paper records containing personal information.[42]

In addition, each of the 50 states, along with the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands has its own set of data breach notification requirements. These laws generally require that consumers (and sometimes state regulators, credit reporting agencies, and/or the media) be notified in the event of a compromise of personal information. These laws vary considerably. For example, state notification laws can vary as to key coverage definitions (such as which data fields constitute personal information or what constitutes a "breach"); whether notice is required if the risk of harm to consumers is unlikely; and the specific content that must be included in any required notice letter.

Some state data breach notification statutes include an exception for financial institutions complying with the notice requirements under the GLBA Interagency Guidance, but several do not. New York's cybersecurity regulations for financial institutions, for example, goes so far as to include a regulator breach reporting requirement

---

37 N.Y. Comp. Codes R. & Regs. tit. 23, § 500.

38 201 Mass. Code Regs. 17.01-17.05.

39 California Financial Code §§ 4050 et. seq.

40 See SB-1121, 2017-2018, California Consumer Privacy Act (Sept. 23, 2018). While the CCPA includes an exemption for personal information "collected, processed, sold, or disclosed pursuant to" the GLBA and its implementing regulations, or CalFIPA, the dramatic expansion of the definition of CCPA will have significant impacts on the financial services sector.

41 *See, e.g.*, Minn. Stat. § 325E.64; Nev. Rev. Stat. § 603A.215.

42 *See* National Conference of State Legislatures, *Data Disposal Laws* (Dec. 1, 2016), www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

specifically applicable *only* to financial institutions, which requires covered institutions to report certain cybersecurity incidents to state financial regulatory officials within 72 hours.[43] A uniform national data breach notification standard would ensure that American consumers are treated the same, wherever they reside, and are provided appropriate transparency about their personal data.

IV. Data Security, Breach Notification, and Customer Privacy Should Be Governed by Uniform National Standards

Given comprehensive federal regulatory oversight of financial institutions' data security, breach notification, and privacy practices, subjecting those same institutions to a patchwork of state privacy laws makes little sense. Duplicative, overlapping, and sometimes conflicting state data security and privacy requirements tend to obscure customers' rights and impose on covered businesses significant technical and administrative compliance burdens. It can be difficult for any consumer to understand how their data is used and protected given the varying definitions, data breach reporting mandates, timelines, and penalties under different state laws. Furthermore, state requirements risk imposing additional administrative burdens on covered institutions without improving consumer data security or privacy. These problems will likely only be exacerbated as additional states move to introduce new statutory and regulatory requirements in this area.

Data security, breach notification, and privacy call for uniform federal standards. We share the Department of Treasury's view, as expressed in a July 2018 report, that Congress should enact a federal data security and breach notification law to protect consumer financial data and notify consumers of a breach in a timely manner, which should "[r]ecognize existing federal data security requirements for financial institutions" and "[e]mploy uniform national standards that preempt state laws."[44] Furthermore, we note that recent research indicates that over eight in ten voters support a national law that requires banks and financial institutions to notify customers in the event of a data breach.[45] For national banks, the National Bank Act preempts state laws that prevent or significantly interfere with the exercise of banks' authorized powers. Some uncertainty remains, however, about the reach of this federal preemption. Companies with non-bank affiliates may not enjoy federal preemption, which could lead to situations in which institutions must treat bank data differently from non-bank data. A uniform federal regulatory scheme governing data security, breach notification, and privacy would better promote consumers' interests in the security and privacy of their personal information. In the context of the data breach notification requirements, for example, a streamlined federal approach would allow banks to more effectively and efficiently notify consumers of any breaches involving their personal information.

As described above, there already exists a strong and comprehensive risk management framework for owners and operators of critical financial services infrastructure in the form of the NIST based Cybersecurity Profile, which has received the widespread public support of numerous financial services regulatory agencies.[46] Given the extensive detail and widespread support for this work, we strongly encourage the Committee to adopt the

---

43 N.Y. Comp. Codes R. & Regs. tit. 23 § 500.17(a).

44 U.S. Department of Treasury, *A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation* (July 2018), home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf.

45 This survey was conducted on behalf of the Bank Policy Institute by Morning Consult. *Available at* bpi.com/dataprivacy/.

46 At the release event, representatives from the Board of Governors of the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Securities and Exchange Commission, and NIST all made statements of support. Baksh, Mariam. "Regulators welcome finance-sector profile based on NIST Framework, but need time to examine implementation." Inside Cybersecurity. 26 Oct. 2018. In a letter to the FSSCC, NIST stated that the Profile was "supportive of a risk-based approach to cybersecurity, and [] one of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to-date. *Available at* www.fsscc.org /files/galleries/NIST_Letter_of_Support_re_FSSCC_Financial_Services_Sector_Cybersecurity_Profile.pdf

organizational structure and taxonomy of the NIST based Cybersecurity Profile to the extent it considers developing legislation to establish federal cybersecurity standards in the future.

In considering any future legislation, Congress should be mindful that any effort to address cybersecurity and privacy risks cannot focus on financial institutions alone. Even within the financial sector, many other entities, including payment processors, retailers, data aggregators, fintech companies, and government agencies, play a significant role in providing financial services. Effective data security and privacy legislation should therefore look beyond banks and other financial institutions that are already subject to extensive regulation. Moreover, to the extent Congress adopts national uniform data security and privacy legislation, such legislation should maintain the current regulatory and supervisory regime governing banks' compliance with data security and privacy requirements.

* * *

BPI appreciates the opportunity to share its perspective as the Committee seeks to assess legislative reform in this area, and we look forward to working with this Committee on reforms that advance consumers' interests.

Respectfully submitted,

Gregory A. Baer
Chief Executive Officer
Bank Policy Institute