MORTGAGE BANKERS ASSOCIATION

January 24, 2020

The Honorable Frank Pallone
Chairman
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Greg Walden
Ranking Member
House Energy & Commerce Committee
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Pallone and Ranking Member Walden:

On behalf of the Mortgage Bankers Association ("MBA"),[1] we are writing to provide feedback on the collection, use and protection of sensitive information by financial regulators and private companies. As mortgage industry participants interface constantly with individual consumers, financial institutions of all kinds, and regulators, we recognize the collection of consumer information has grown rapidly in recent years. The use of "big data" has been a function of increased technological capacity to collect and analyze information as well as a desire to provide consumers with the most effective customer experience. As consumers continue to provide more of their personal information to businesses, personal privacy and data security becomes an increasingly necessary focus. Our legal system recognizes that our expectations of privacy and security reflect changes in society, but rapid innovation requires education and oversight to ensure consumers are aware of how their information is used. MBA appreciates this effort to understand and offer feedback on how important and beneficial innovations impact consumer privacy.

Since the enactment of the Gramm-Leach-Bliley Act ("GLBA") in 1999, financial institutions have adhered to federal guidelines and standards for data privacy and data security. Consequently, participants in the real estate finance industry are required to implement certain privacy and security controls. Our members are acutely aware of their responsibility to protect consumer information and ensure that the data they collect is used for appropriate purposes. As such, proposed federal privacy laws should recognize the GLBA framework and not impose duplicative or conflicting mandates.

Mortgage lenders understand the importance of protecting their customer's information and privacy. We support efforts to ensure that no consumer unwittingly exposes themselves to harm by unintentionally providing their personal data to unscrupulous actors. However, we also want to be careful not to prevent the responsible use of data to improve the efficiency of mortgage origination.

The need to evaluate how digital information is collected and protected is coming under greater scrutiny across all industries. Over the last several months, states have begun moving forward with comprehensive

[1] The Mortgage Bankers Association (MBA) is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, D.C., the association works to ensure the continued strength of the nation's residential and commercial real estate markets, to expand homeownership, and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,300 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field. For additional information, visit MBA's Web site: www.mba.org.

and sometimes conflicting changes to their privacy and data security laws and regulations. Many of these sweeping changes have come in response to well-publicized attacks but have failed to take account of the difficulties associated with rapidly implementing detailed changes or confronting emerging threats across a broad spectrum of small and large businesses.

Legislators and regulators must understand that a breach does not necessarily indicate that a company did not have robust policies and systems in place to protect consumer privacy. This is especially true in light of the types of attacks the United States has seen in the last several years. Foreign governments, organized crime, and even terrorist organizations have been engaged in cyber warfare with the United States, its citizens, and its businesses. It is especially important that legislators recognize that the data security challenge is also a national security concern that requires the attention of the entire federal government and its regulatory, law enforcement and national security agencies.

Through consultation with our members, MBA has considered potential remedies through legislative or regulatory action, and/or industry best practices in several areas of interest for which we offer our principles below:

Consumer Data Controls and Breach Notification

Breach notification is an area rife with inconsistency and conflicting regulations. While at the federal level there have been data security efforts for specific industries,[2] there is not a widespread standard for breach notifications. Sensitive information is increasingly targeted by foreign governments or transnational criminal organizations. Consumers *and* the entities attempting to protect their data are victims of these attacks. Considering this, data security is a national security issue that crosses jurisdictions and state lines. As such, data security standards and breach notifications merit a preemptive federal requirement.

Currently, the United States has over fifty different data breach notification laws. State governments have created additional standards on top of federal requirements. Their efforts are well-intentioned, and they seek to protect their residents. However, these laws can have significant variations or subtle differences that require increasingly complex systems to ensure compliance. Entities engaged in business across the United States do not have separate computer systems for each state. To develop and maintain systems for each state would be cost prohibitive, with the likely result that some businesses would choose not to offer services in every state. Moreover, conflicting standards and excessive complexity can undermine effective data security.

For businesses whose operations span multiple states, variations in requirements result in varied responses with high potential for confusion. Some states require the Attorney General to be notified prior to any notification to affected consumers,[3] while others require the opposite or simultaneous notification.[4] Additionally, there are variations to the *content* of information required in notifications.[5] Though some

[2] Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.400-414; *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 70 Fed. Reg. 15736 (March 29, 2005). *See also*, Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq.*

[3] Maryland Code Ann., Com. Law. §14-3501 *et seq.*; N.J. Stat. Ann. § 56:8-161 *et seq.*; N.Y. Gen. Bus. Law § 899-aa.

[4] Vt. Stat. Ann. Tit. 9, § 2430 *et seq.*; Mont. Code Ann. § 30-14-1701 *et seq.*

[5] The definition of "personal information" varies significantly throughout the fifty states. Some states also further categorize information as "sensitive" or "nonpublic." Additionally, some states provide safe harbors for personal information that is either encrypted or has been de-identified. With these subtle but important differences, the information included in breach notices vary.

states include exceptions for compliance with other federal requirements,[6] these federal requirements are not preemptive, thereby allowing states to continue adding piecemeal requirements on entities operating in multiple states. Inconsistencies across states as well as continual legislative change requires the expenditure of significant funds to comply with differing state requirements, often with no improvement to the protection of consumer data.

Ultimately, this leads to inconsistency for consumers based on their residence despite the identical harms suffered. A clear solution to this problem is a non-prescriptive, preemptive federal data breach notification law with clear requirements to notify affected consumers as well as state and federal regulators. Similar to the cybersecurity framework established by the National Institute of Standards and Technology ("NIST") and other industry-developed frameworks,[7] national guidelines can spur the widespread adoption of best practices. With requirements that describe the necessary controls, industry can work towards developing the framework necessary to implement those controls. Regulated entities and their consumers can be provided with clear expectations and become aware of routine procedures, and the entire response mechanism becomes more fluid for both consumers and the entities reporting. Importantly, this method allows for adaptability of best practices in the face of evolving dangers.

The importance of a comprehensive standard cannot be overstated. During a recent Senate subcommittee hearing, the FTC's Bureau of Consumer Protection Director, Andrew Smith, pointedly restated the FTC's "longstanding bipartisan call for enactment of a comprehensive federal data security law."[8] Preemption is essential here and addressing the issue in any other way would fail to improve the status quo, prescribing varying requirements to a universal problem.

Redress following a data breach is also subject to several conflicting doctrines across the states. Certain states have sought to provide consumers with recourse with expansive private rights of action, but as discussed above, many, if not most, data breaches arise from criminal activity by an external force. Laying fault at a business, which itself is a victim of criminal activity, is targeting punishment at the *wronged* actor. For these reasons, any data security legislation should limit private rights of action to the reckless disregard of a known risk. Knowing disregard of expected harms merits civil liability. Appropriately, this is in contrast to attempting to quantify unknown risks and the associated compliance difficulties, which are correctly addressed by supervision and enforcement from the appropriate regulators.

As it relates to participants in the mortgage industry, another data protection risk is the breadth of information entities are required to collect and then maintain for several years. The Bureau of Consumer Financial Protection's ("CFPB" or "the Bureau") Regulation Z under the Truth-in-Lending Act ("TILA") requires mortgage loan creditors to retain evidence of compliance for three years.[9] Additionally, Regulation Z provides a safe harbor and presumption of compliance for qualified mortgages ("QM").[10] The QM safe harbor is a defense at foreclosure, which requires entities to maintain copious amounts of sensitive information for the life of the loan. As custodians of significant amounts of sensitive consumer information, the risk to the mortgage industry is exacerbated by the necessity to retain information for an

[6] *See supra*, note 1.
[7] *See* NIST Cybersecurity Framework Version 1.1, ISO/IEC 27000 family of information security management systems.
[8] *Examining Private Sector Data Breaches*, Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, 116th Congress, pg. 2 (2019) (Testimony of Andrew Smith).
[9] 12 C.F.R. § 1026.25(c)(1)(i).
[10] 12 C.F.R. § 1026.43(e)(1).

extensive period of time. For purposes of compliance, retaining consumer data is inevitable, but reducing the amount of data collected has the potential to reduce the likelihood and severity of a data breach.

Consumer Control Over Data Usage and Dissemination

The use of "big data" is prevalent in several industries, but not all these industries are treated equally. This is particularly true as it relates to protecting consumer information and the level of consumer access. Whether an entity is collecting information, processing information, or sharing that information, ensuring its protection or granting reasonable access are concurrent responsibilities. The financial services industry is subject to legislation and regulations under the GLBA that impose requirements related to privacy, data protection, and disclosure. These requirements are longstanding and appropriately balance the need for privacy against the need for information flows vital to a well-function mortgage market.

With the value of consumer data increasing and its subsequent commercialization, consumers' oversight of their own information is understandably an area of focus. In order to accommodate oversight, however, regulators must be considerate the necessary protection requirements. If data are required to be encrypted or redacted under one regulatory scheme, it may be unlawful, impractical, or impossible to then maintain an identifiable tag for purposes of consumer review.

There is a need to strike a balance between providing access to consumers, while also protecting their information. Regulators should consider allowing entities to provide summarized information in response to a consumer request through a defined channel. As it relates to consumer control over their information, the GLBA currently requires financial institutions to provide an opt-out mechanism for consumers. Any federal data privacy legislation should consider this longstanding opt-out and retain it for entities covered by the GLBA.

It is important to note that many entities make use of third-party vendors to process certain components of a transaction. This form of "sharing data" is necessary and already carries the privacy and security principles applicable to the primary entity. By way of contract and current regulations, a third party vendor is already obligated to maintain the specific level of responsibility that is applied to the primary business. Any form of legislation or regulation must be conscious of this business necessity and exempt third party data sharing, *for the purposes of administering, effecting, or enforcing the underlying transaction*, from any additional onerous requirements.

Consumer Data Accuracy and Protection

Regulators currently maintain significant oversight of the credit bureaus. As discussed above, the FTC has begun consideration of amendments to its Safeguards Rule, which requires financial institutions (including credit reporting agencies) to develop, implement, and maintain a comprehensive information security program.[11] Credit reporting agencies ("CRA") are subject to the requirements of the Safeguards Rule under the GLBA. As the FTC maintains authority over the Safeguards Rule, they are the most appropriate regulator to consider changes to how CRAs protect consumer data. The regulator in this case should be allowed to conduct its ongoing notice-and-comment rulemaking and make any appropriate changes in light of stakeholder and public input.

As it relates to the accuracy of a credit file, the CFPB maintains rulemaking authority over a significant portion of the Fair Credit Reporting Act ("FCRA"), including provisions regarding the accuracy and

[11] Safeguards Rule, 16 C.F.R. § 314.

integrity of consumer information. Similarly to the FTC, the CFPB should be encouraged to engage in notice-and-comment rulemaking to consider any potential changes necessary to ensure the accuracy of consumer information within a credit file.

Consumer Identification and Control of Personal Data

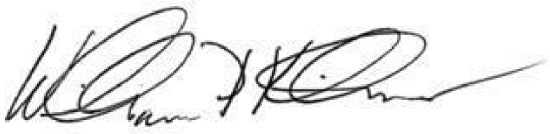
With the growth of data brokers, it is understandable that consumers would seek insight on the information collected about them. This is also an issue that crosses state lines and merits a preemptive national regime, as the data is both accessible nationally and exposure is not limited to a particular state. Legislators should carefully consider the necessity of an appropriate federal regulator and the implications of inconsistent regulations. Similarly, data used in establishing consumer eligibility for credit, insurance, employment, or other purposes involves several unique data sets. Entities that engage in the collection of the relevant information can potentially conduct business in a multitude of regulatory environments. This requires a certain level of expertise that is best exercised by regulators in combination with stakeholder input.

Conclusion

MBA appreciates your consideration of these comments and the Committee's willingness to engage with the public and stakeholders on issues surrounding consumer data privacy and data security. Our association will continue to refine its policy on these important topics, but we believe that a preemptive federal standard is vital considering the national character of the issue and the international nature of the threats.

Should you have any questions or wish to discuss any aspects of these comments, please contact me at (202)-557-2736 or bkillmer@mba.org Ernie Jolly, Associate Vice President of Legislative Affairs, at (202) 557-2741 or ejolly@mba.org or Dan Grattan, Associate Vice President of Legislative Affairs, at (202) 557-2712 or dgrattan@mba.org.

Sincerely,



Bill Killmer
Senior Vice President, Legislative and Political Affairs