MBA Data Protection Principles

The responsible use of data is essential to the mortgage finance industry. These principles act as guideposts to ensure consumer data privacy and data security are addressed uniformly, clearly and efficiently.

As technology advances, consumer expectations about how it works, or should work, evolve. This evolution arises from growing familiarity with new technologies and becoming comfortable with what it changes. The gap found in this process is natural because innovation necessarily comes first. Often, the regulatory response arises during the time between introduction of new technology and consumers fully understanding its beneficial uses and inherent trade-offs.

Ensuring responsible innovation without creating unnecessary barriers to widespread use raises a policy challenge. While consumers may enjoy the convenience certain innovations provide, there must be parallel development of oversight and regulation to address the issues raised when consumer information is provided or collected to enable these benefits. For instance, the increasing 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. Due to the unique legal and regulatory requirements of the real estate finance industry, the ability to obtain, transfer, and develop data must not be impeded. Mortgage lenders understand the importance of protecting their customer's information and privacy and are acutely aware of their responsibility to protect consumer information and ensure that the data they collect is used for appropriate purposes.

PURPOSE

This document serves to provide foundational principles regarding consumer data protection for the real estate finance industry. As the conversation surrounding data protection continues to develop and new issues arise, these principles are expected to remain high-level guideposts. By following these principles in our industry's advocacy efforts, any novel legislative or regulatory effort can remain conscious of consumer concerns, barriers to innovation, and consistent regulatory application.

CONTEXT

In response to well-publicized international cyber-attacks or data breaches, many national governments have begun moving forward with comprehensive and sometimes conflicting changes to their privacy and data security laws and regulations.[1] In the U.S., Congress and other federal regulators have also initiated several parallel proceedings to address the perceived threat.

Every state currently has a data breach notification law on their books. While some have overlapping requirements, finding a common thread through all 50+ laws would be difficult.[2] Companies that operate in multiple states face significant challenges with the ever changing environment and patchwork of different statutes and regulations that attempt to address the same concerns. Moreover, a national framework is necessary as the nature of the threats to the mortgage markets are the same as to the larger U.S. economy and are often being perpetrated by hostile governments, criminal organizations, or even terrorist groups. MBA believes consumer data privacy and data security must be addressed uniformly at the national level to ensure robust and consistent consumer protection and avoid confusion for both consumers and businesses.

CORE PRINCIPLES

Data protection encompasses two areas: (1) privacy; and (2) security. While these two issues are interconnected and routinely conflated, it's imperative that any legislation that aims to tackle these issues differentiates between consumer data privacy and the necessary data security processes and controls.

1 The California Consumer Protection Act (CCPA) was the first comprehensive reform and was drafted and enacted in haste, thus it is likely that there may be several potential amendments before its effective date of January 1, 2020. Despite these concerns, states are introducing replicas of the CCPA while others are incorporating variations.

2 As of April 2018, all 50 states have a breach notification law. In addition to the 50 states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands also have their own data breach notification laws. Though some states have some overlapping requirements, their contents generally vary. States regularly enact amendments to their breach notification laws, further complicating matters.

Advances in technology are raising new questions. Consumer expectations of privacy involve what information is being collected, how it may be used, who it's being shared with, whether the information can be used at all for a certain purpose, and in what ways a consumer can interact with this information. This includes whether and how a consumer can request copies of their information, corrections to their information, and deletion of their information.

Data security focuses on the responsibilities of a business as it relates to the information it receives on consumers and the need to ensure the confidentiality, integrity, and availability of that information. This includes how data is safeguarded, what controls must be in place to ensure sensitive information remains protected, and what processes must be in place if a security event occurs.

The principles below reflect issues that have a significant impact on the real estate finance industry. They highlight the necessity of uniformity and promote the ability to foster innovation while maintaining a modern and consistent framework.

- **National standards are critical.**

  Consumer data privacy and data security should be addressed at the federal level. Congress should consider a framework for both issues that encourages compliance by employing an approach that allows flexibility to facilitate adaptability in the face of an ever-changing security environment. A patchwork of state laws and federal regulations will only serve to confuse businesses and harm consumers.

- **Data breach notifications should be standardized.**

  Congress must pass a federally preemptive data breach notification law with clear requirements to notify impacted consumers as well as state and federal regulators. Notifications should be made within a reasonable time frame and when there is a risk of harm to consumers resulting from unauthorized access of unsecured non-public personally identifiable information.[3]

- **Any designated framework must be technology neutral.**

  A privacy or security framework must not be prescriptive or static. No single solution will be sufficient to defend against cyber threats because threats are increasingly sophisticated and constantly evolving. No one-size-fits-all solution exists for industries that vary wildly in size and nature. Overly prescriptive requirements would force businesses to adopt identical technologies, creating difficulties for small businesses and providing bad actors a single target. Rather, any framework should remain

3 "Unsecured" in this instance relates to customer information that is not encrypted or otherwise protected in a reasonably similar manner.

technology neutral to ensure businesses can remain flexible and adapt to evolving threats. The Federal Trade Commission (FTC) has historically supported a "process-based" approach that facilitates adjustments based on business size and nature. Any legislation should codify such an approach.

- **State legislation should adopt a clear Gramm-Leach-Bliley Exemption.**

  While MBA does not support state-specific legislation, at an absolute minimum any data privacy and security legislation must include entity-level exemptions for those subject to, and in compliance with, the Gramm-Leach-Bliley Act (GLBA). Congress's statutory design and the FTC's and Consumer Financial Protection Bureau's (CFPB) regulations under GLBA should be controlling for entities that are covered by them. Provisions that detail a GLBA exemption should not require businesses to engage in a burdensome and possibly ambiguous conflict analysis to determine which standards apply.

- **There should be defined channels for opt-outs and industry specific disclosures and delivery methods.**

  While privacy legislation seeks to provide consumers with greater control over their information, opt-out mechanisms that provide consumers the ability to withdraw from data sharing should be clearly defined and must recognize the necessities of transaction-based data transfers. Both businesses and consumers would benefit from defined opt-out channels. Legislators should adopt the well-known and widely implemented GLBA opt-out mechanisms when implementing a similar privacy requirement and provide exceptions for transaction-based needs.

  What constitutes an adequate disclosure to consumers varies significantly with the type of transaction. Consumers are inundated with information. In order to effectively convey necessary information, regulators should set guidelines for the general message that must be delivered, while allowing industry to determine the adequate breadth of content necessary to ensure consumers are not overwhelmed and gain a proper understanding of information communicated in the disclosure.

  Whether it is an electronic or paper-based disclosure, industry has adopted various methods of delivering information to consumers. Some are email-based, web-based, mobile-based, or paper deliveries. The effectiveness of the disclosure will vary with the type of transaction and the entity performing the transaction. Federal regulators should set guidelines for the general message that must be delivered, while allowing industry to determine the best form of delivery.

- **Those that follow the rules should have a defined safe harbor.**

  The implementation of new consumer data control channels and protection mechanisms require considerable resources, all of which raise significant costs. Providing safe harbors will help ensure legal certainity and encourage adoption of and investment in new security protocols.

FOR MORE INFORMATION, CONTACT:

Justin Wiseman
Associate Vice President & Managing Regulatory Counsel
Mortgage Bankers Association
jwiseman@mba.org
(202) 557-2854