Statement of Deborah Sousa, Executive Director, on the behalf of the
Massachusetts Mortgage Bankers Association
Legislation regarding Data Security and Privacy
Joint Committee on Consumer Protection and Professional Licensure
October 7, 2019

Chairman Feeney, Chairman Chan, members of the Joint Committee, my name is Deborah Sousa and I am Executive Director of the Massachusetts Mortgage Bankers Association (MMBA). The MMBA represents 239 lending institutions made up of equal representation between depository institutions (banks and credit unions) and non-depository institutions (mortgage banker/lender companies, mortgage brokers and all ancillary companies which touch the mortgage transaction throughout the Commonwealth

The MMBA and its members share your concern with protecting consumers and data privacy. This is a national security problem where foreign governments, organized crime and terrorist organizations are targeting American governments, institutions and businesses, including the real estate finance industry. Our members are already spending significant dollars to protect themselves and their customers to adhere to existing federal laws and regulations.

There are several federal and state laws which already require financial institutions to protect the data privacy of consumers:

The Fair Credit Reporting Act (FCRA) is a federal law that regulates the collection of consumers' credit information and access to their credit reports. It was passed in 1970 to address the fairness, accuracy and privacy of the personal information contained in the files of credit reporting agencies. Protections within the FCRA include protected access to credit files, truncation of account numbers and social security numbers.

Fair and Accurate Credit Transactions Act of 2003
This Act, amending the Fair Credit Reporting Act (FCRA), adds provisions designed to improve the accuracy of consumers' credit-related records. The Act also adds provisions designed to prevent and mitigate identity theft, including a section that enables consumers to place fraud alerts in their credit files, as well as other enhancements to the Fair Credit Reporting Act. Certain provisions related to data security ("red flags" of possible identity theft) were amended by the Red Flag Program Clarification Act of 2010 to clarify and narrow the meaning of "creditor" for purposes of those provisions.

The Red Flags Rule[1] requires many businesses and organizations including financial institutions to implement a written identity theft prevention program designed to detect the “red flags” of identity theft in their day-to-day operations, take steps to prevent the crime, and mitigate its damage.

The Gramm-Leach-Bliley Act (GLB) also known as the Financial Services Modernization Act of 1999, requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. The GLB includes provisions in Title V to protect and regulate consumer's personal financial information. There are three principle parts to the Title V privacy requirements: The Financial Privacy Rule; Safeguard Rule and Pretexting Provisions.

The Financial Privacy Rule require financial institutions to provide notices and to comply with certain limitations on disclosure of nonpublic personal information. A financial institution must provide a notice of its privacy policies and practices with respect to both affiliated and nonaffiliated third parties and allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure is outside of the exceptions.

The **Pretexting provisions**, which prohibit the practice of **pretexting** (accessing private information using false pretenses).

The Safeguards Rule requires companies to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program, and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure your contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

In March, 2019 the Federal Trade Commission (FTC) issued a Notice of Proposed Rulemaking (NPRM) on Standards for Safeguarding Customer Information (Safeguards Rule).

> "We are proposing to amend our data security rules for financial institutions to better protect consumers and provide more certainty for business," said Andrew Smith, Director of the FTC's Bureau of Consumer Protection. "While our original groundbreaking Safeguards Rule from 2003 has served consumers well, the proposed changes are informed by the FTC's almost 20 years of enforcement experience. It also shows that, where we have rulemaking authority, we will exercise it as necessary to keep up with marketplace trends and respond to technological developments."

The Massachusetts data security regulations (201 C.M.R. 17.00 et seq., the "Massachusetts Regulations") went into effect in 2010 require every company that owns or licenses "personal information" about Massachusetts residents to develop, implement, and maintain a Written

Information Security Program (WISP). The WISP must contain certain minimum administrative, technical, and physical safeguards to protect such "personal information".

Looking at other state legislative initiatives, the **California Consumer Privacy Act (CCPA)** goes into effect on January 1, 2020. The initial intent of the CCPA is similar to SB.120. Since the passage of the CCPA, additional corrections and clarity was needed and there are currently five amendments that have passed the California Assembly and the Governor has until October 13th to sign these amendments.

In a recent study prepared for the California Attorney General, independent researchers from Berkeley Economic Advising reported $55 billion is an estimate of initial compliance costs for Implementing the CCPA. After the initial compliance expenses, California businesses could spend an additional $16 billion over the next decade to keep up with changes and other expenses, according to the report.

The MMBA would respectfully ask that the committee send SB.120 into study for the following reasons:

- Data privacy and security is a national issue. The financial service industry has several federal laws governing data security. The Federal Trade Commission (FTC) will be amending data security rules for financial institutions to better protect consumers. Additional time would allow us to see the amendments to ensure there are no conflicts between federal and state regulations.

- It is extremely difficult for a business to be compliant when each state or even each city within a state has different regulations and laws. California has taken the lead in passage of the CCPA but follow-up amendments were needed for clarification. In addition, the Attorney General has not yet published regulations. Additional time would allow us to understand why the amendments were needed to clarify the original language in the CCPA and perhaps make changes in SB.120 as well as other data privacy and security bills before this committee so that there was more conformity between state laws and regulations governing this important issue.

The MMBA would also respectfully suggested language clarifications in SB.120:

- Section 1 Definitions of "Deidentified" (g) and "Personal information" (m 1-3) should match the CCPA amendments of "reasonably capable of being associated with". One of the most operationally complex features of the CCPA is the law's definition of "personal information." As enacted, the term arguably encompasses almost every piece of information a business maintains because nearly all information can in theory be associated with an individual, even if as a practical matter it is nearly impossible to associate that piece of information to a consumer and that data is of minimal or no relevance to privacy. Amendment AB 1355 would narrow this definition by adding the word "reasonably" before the word "capable" so that now the outer boundary of this definition is any information that is "reasonably capable" of being associated with a consumer.

- Elimination of Internet Protocol (IP) address as a unique identifier or have more detailed discussion surrounding this provision. An IP address, while unique is also multifaceted. IP addresses can change or be masked through proxy servers or a virtual private network (VPN).

- Section 2, (B) (b) A business shall not collect additional categories of personal information or use personal information collected for additional purposes without first providing the consumer with notice consistent with this section. We ask for clarification on how specific the categories and purpose disclosures need to be as it is unclear in the language.

- Sections 2 and 4 reference data categories for the purpose of providing disclosures to consumer and mechanism for verifiable consumer requests. How are categories of data created and defined and who defines these categories? The Attorney General is tasked with updating additional categories of information, but who decides categories of data or of 3rd parties up front?

Given that the FTC is likely to amend the data security rules for financial institutions and the California Consumer Protection Act is also being amended, we respectfully suggest that new state legislation be delayed, and a study commission be created so that we can better protect consumers by passing a clear, concise and enforceable Massachusetts Consumer Protection Act.

Conclusion

The MMBA and our member lenders will continue to safeguard data and security to protect customers and adhere to federal and state regulations. We would like to offer the MMBA and our membership as a resource to you for any questions or clarifications on the impact of any bills in this committee.

Thank you for the opportunity to provide you with written testimony before the Committee.