2019 CAPITAL SUMMIT ICBA

DATA SECURITY, PRIVACY, AND FRAUD

Community banks are committed guardians of the security and confidentiality of customer information as a matter of good business practice as well as legal and regulatory compliance. Safeguarding customer information is central to maintaining public trust and retaining customers. Nonetheless, community banks are only one of numerous entities that store consumer financial data. As bad actors continue to look for vulnerabilities in the payments and information systems of various industries, breaches will continue to occur. Data breaches at a national credit bureau, national retailers, major hotel chains, and elsewhere have the potential to jeopardize consumers' financial integrity and confidence in the payments system. ICBA supports legislation to enhance customer data security and strengthen the public trust. Provisions should include:

STRENGTHEN WEAKEST LINKS

Under current law, retailers and other parties that process or store consumer financial data are not subject to the same federal data security standards and oversight as financial institutions. A chain is only as strong as its weakest link. Consumer data safeguarded at financial institutions is exposed at the point-of-sale and other processing points. Gramm-Leach-Bliley Act-like standards should be applied to non-bank entities that handle consumer financial data. The enforcement of these standards should also be similar.

UNIFORM BREACH NOTIFICATION WILL MITIGATE LOSSES

Consumers must be notified in the event of a breach so that they can take steps to protect themselves from identity theft or fraud. While most states have enacted breach notification laws, they differ in key respects from state to state. This patchwork of state laws increases burdens and costs, fosters confusion, and ultimately harms customers. Legislation is needed to replace the state law patchwork with a national data breach notification standard.

ALIGN COST INCENTIVES TO BETTER SECURE DATA

The costs of data breaches should ultimately be borne by the party that incurs the breach, be it a retailer, financial institution, data processor, or other entity that stores consumer data. This is not only a matter of fairness; a liability shift is needed to properly align incentives for entities that store consumer financial and personally identifiable data to strengthen their data security. When breaches have a material impact on entities' bottom lines, they will quickly become more effective at avoiding them. Barring a shift in liability to the breached entity, community banks should continue to be able to access various cost-recovery options after a breach, including account-recovery programs and litigation.

PRIVACY

Any privacy legislation considered by the Congress must recognize the existing requirements community banks undertake to protect customer information and privacy.

MESSAGE FOR YOUR MEMBERS OF CONGRESS

- Support legislation to create a secure, end-to-end payments environment for consumers and businesses, with a national breach notification standard.
- Cost incentives should align with data security. The party that incurs a breach should be liable for all costs associated with the breach.
- Congress must recognize the existing requirements community banks undertake to protect customer information and privacy when considering any privacy legislation.