Data Privacy Summary

Protecting customer data and preserving consumer trust is critically important to banks. Technology has allowed for an expansive increase in the use of consumer data, however with this growth should come an assurance for customers that their personal information is protected and secure. Banks have long built robust security programs to manage the collection and protection of customers' personal information. These programs, which are subject to a rigorous framework of federal, state, and international regulations, help banks protect customer accounts from fraud, initiate accounts, and respond to customer requests. Beyond their own internal programs, banks also work collaboratively with law enforcement and regulators, as well as each other, to protect consumer data. No industry is more regulated or subject to regulatory review and examination of their privacy standards.

The most extensive law governing banks' privacy and information security requirements is the 1999 Gramm-Leach-Bliley Act (GLBA), which requires banks to develop, implement, and maintain administrative, technical, and physical safeguards to:

- protect the security and confidentiality of customer information;
- protect against any anticipated threats or hazards to the security or integrity of customer information; and
- protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.

Banks test and continually update these programs, which are evaluated and reviewed by executive management and boards of directors as well as regulators during exams.

BPI's Position

Banks already comply with a range of domestic and international privacy and data protection laws. The overlapping and growing patchwork of state laws create complicated, duplicative and often conflicting rules.

Recommendation: The U.S. should adopt a national privacy standard that provides a level playing field for all types of businesses and customer accounts. This federal standard would create clear, robust protections for consumer data across the United States, while ensuring consistent state-by-state adoption of these national requirements.

Creating a Safe System, Protecting Customers from Fraud, and Enhancing the Consumer Experience

Banks use data to support a safe financial system and to comply with legal requirements such as Know Your Customer regulations. This ensures bad actors do not abuse the banking system for illicit purposes. Banks also use customer data to protect customers from fraud, allowing them to better identify when an account may be compromised. Perhaps most importantly, banks use data to serve customers. By knowing and engaging customers, banks are able to better serve clients by identifying products and services that might be of interest, such as opportunities to refinance a home, save for retirement, or extend credit during times of need. Data helps banks protect the system and support the customer.

Patchwork of State Laws Creates Confusion for Consumers

The financial services industry is subject to some of the most robust privacy laws in the U.S., particularly relative to other sectors of the economy. In addition to a comprehensive federal regulatory regime, banks are also subject to a web of state laws governing the security and privacy of customer information. State data privacy laws can create confusion and disparate treatment for consumers, as well as customer confusion and inconvenience, as products or services offered to a customer in one state may not be available to customers from another. Where you live should not determine how your data is used and protected. A harmonized, comprehensive federal regulatory framework governing data security and privacy is better suited to protecting consumers' personal information.