WRITTEN STATEMENT
Offered to the House Commerce Committee on
HB 1201 PN 1272 re Data Privacy

PA Bankers represents approximately 120 banks, trust companies, savings banks and their affiliates operating in the Commonwealth. We appreciate the opportunity to share our members' views on data privacy protection which requires their devotion of enormous and ever-growing time and resources.

Financial institutions have long been strong proponents of data privacy protection and have been subject to federal laws and regulations governing it since the 1970s. Federal financial privacy laws have taken a careful and balanced approach that not only protects the privacy interests of consumers, but also ensures that the financial system can function securely and effectively and provide the innovative products and services that consumers and businesses want and need. Given that many of our members operate in more than one state, we continue to believe that a comprehensive federal approach to data privacy is preferable to a patchwork of inconsistent state laws.

As just one example of federal law and regulation applicable to financial institutions, Title V of the Gramm-Leach-Bliley Act (GLBA) requires financial institutions to:

- protect the security and confidentiality of their customers' records and nonpublic personal information.
- notify their customers of their privacy policies practices.
- give their customers the notice and opportunity to opt-out of the sharing of their information with non-institution-affiliated third parties.
- ensure the privacy and security of their customers' information through protection against anticipated threats, unauthorized access or use that could result in substantial harm or inconvenience.

In addition to the GLBA, financial institutions are also subject to the federal Fair Credit Reporting Act (FCRA), the Right to Financial Privacy Act (RFPA), the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), the CAN-SPAM Act, the Telephone Consumer Protection Act (TCPA), the Electronic Communications Privacy Act (ECPA) and the Drivers' Privacy Protection Act, among others.

Unlike virtually all other entities within the U.S. economy, financial institutions are not simply subject to federal and state privacy laws but are also subject to routine monitoring and testing of their compliance with those laws. Federal regulatory agency examiners are permanently on-site at offices of certain large financial institutions.

Since 2005, federal bank regulations have required banks to install, maintain and regularly update incident response programs to address security incidents including notifying customers of possible data breaches when necessary. To these ends, the Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook includes over 1000 pages of IT and examination guidance to assist regulators in measuring financial institutions' compliance. In addition, institutions must comply with the primary bank regulatory agencies' interagency guidance on response programs for unauthorized access to customer information and customer notice.

Most institutions make their privacy practices available on their websites and use a standardized model template issued by the Consumer Financial Protection Bureau designed along the lines of nutrition labeling on food products. The current disclosures for consumers were developed over several years by federal regulators and the industry.

Given the comprehensive scheme of federal data privacy regulation and examination to which financial institutions are subject, we respectfully request that if HB 1201 is advanced that its nonapplicability section (Section 11, pg. 3) be amended to read:

> (5) A financial institution, an affiliate of a financial institution, or data, subject to 15 U.S.C. Ch. 94 (relating to privacy).

Questions? Contact Duncan Campbell (dcampbell@pabankers.com; 717-255-6916) or Louise Rynd (lrynd@pabankers.com;717/574-8142)

8/28/23