

Joint Commission on Technology and Science
Advisory Committee on Privacy
August 1, 2005

**Comments of the Virginia Bankers Association on Proposed
Security Breach Legislation**

- Banks are devoting considerable resources to preventing hackers and other criminals from gaining unauthorized access to their customer databases. For banks, protecting customer information is more than just a priority; it is essential. After all, under existing law, it is the bank that generally covers a customer's financial loss due to identity theft. The fact that the bank is on the hook for the loss, however, does not eliminate the aggravation for customers who must reclaim their identity and repair credit records. Stated simply, a breach of a bank's information security system can damage the bank's reputation and subject it to significant financial loss. Thus, banks have as strong an interest as anybody in stopping cyber criminals and others who seek to breach information security systems.
- The banking industry, unlike many other industries, is already subject to significant legal requirements relating to the protection of customers when there is a data security breach. Banks in Virginia shouldn't have to deal with another set of security breach laws. In particular, Section 501(b) of the Gramm-Leach-Bliley Act, and regulations promulgated thereunder, require banks to notify customers of incidents involving unauthorized access of customer information and to comply with a host of other requirements intended to protect consumers from identity theft. Since banks are already subject to extensive requirements under the Gramm-Leach-Bliley Act, and new state law requirements would merely complicate their efforts, any Virginia legislation should create a safe harbor or exemption for financial institutions subject to the Gramm-Leach-Bliley Act. Other states have adopted this approach. Also, proposed legislation under consideration in the United States Congress has a safe harbor for institutions subject to the Gramm-Leach-Bliley Act, such that institutions subject to that Act need not worry about the other requirements set forth in the legislation.
- Indeed, the fact that banks are subject to one uniform set of standards under the Gramm-Leach-Bliley Act is a strength. Not only does one set of standards reduce compliance costs, it avoids complications resulting from a hodgepodge of different state laws that could frustrate the goal of protecting consumers.
- For this reason, proposed legislation in the United States Congress dealing with customer notification of security breaches would preempt state security breach laws. As it appears increasingly likely that a bill will be enacted by Congress this session, it may be prudent for the Joint Commission on Technology and Science to delay consideration of any state security breach legislation at this time.

Questions or comments should be directed to Bruce Whitehurst, VBA Executive Vice President, at 804-819-4701, or Jay Spruill, VBA General Counsel, at 804-819-4710.