FDPA Addresses Consumer Protection

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Congress of the United States passed the Financial Data Protection Act of 2005 (FDPA, HR 3997) in mid-March (see <http://tinyurl.com/frdcl> to track this bill). The official summary describes the FDPA as follows:

“Declares that each consumer reporter shall have an affirmative obligation to implement policies and procedures to protect the security and confidentiality of any consumer's sensitive financial personal information maintained, serviced, or communicated by or on the reporter's behalf against any unauthorized use reasonably likely to result in substantial harm or inconvenience to the consumer.”

The summary goes on to define a “consumer reporter” in essence as any commercial organization that sells consumer information.

Supporters of the bill enthusiastically point to the establishment of uniform federal rules to supersede the hodge-podge of state laws that currently mandate disclosure of privacy breaches involving consumer data. For example, the Credit Union National Association (CUNA) wrote in their Feb 3 letter <http://tinyurl.com/oaglh> to the House Committee on Financial Services (HCFS) that “CUNA supports the uniform, national standards in H.R. 3997, the Financial Data Protection Act of 2005, to impose data security safeguards and notification requirements on a wide range of entities engaged in the business of collecting or handling sensitive personal financial information. Currently, the privacy and security requirements of the Gramm-Leach-Bliley Act (GLBA) only apply to financial institutions.”

In addition, CUNA wrote, they “support the proposed standard of ‘substantial harm or inconvenience’ for triggering the notice requirement.”

The most problematic issue in the legislation may be that it gives the consumer reporters the unrestricted freedom to determine what constitutes “substantial harm or inconvenience” to their data subjects. A consortium of 12 privacy advocates (including the Consumers Union, the Consumer Federation of America, the National Consumer Law Center and the Privacy Rights Clearinghouse) wrote to the HCFS <http://tinyurl.com/haqt6> complaining that “The ‘trigger’ for notification would leave consumers uninformed in many instances when personal information has been breached.”

Their letter continued, >The bill features what we could call a “don’t know, don’t tell” trigger, meaning that when a company doesn’t know whether there is a risk of harm, individuals are not notified. This gives companies an incentive not to conduct thorough investigations. . . . Had H.R. 3997 been in place, we doubt we would have heard about any of the data breaches that came to light in 2005, which affected tens of millions of Americans. We believe individuals need to know whenever their sensitive personal information has been breached. If there is an exception at all, it should be limited to cases when there is no reasonable risk of harm.<
Other criticisms articulated and discussed by the privacy advocates:

- The bill stops consumers from putting a security freeze on their financial accounts until they have become victims of identity theft;
- It preempts stricter state laws designed to reduce identity theft and financial fraud;
- It may start us on the slippery slope to weakening privacy elements of the Gramm-Leach-Bliley Act;
- Enforcement provisions are weak;
- Provisions for limiting firms’ liability may reduce consumer protection.

I urge security specialists whose organizations are affected by this legislation to study this bill carefully and to work with corporate counsel to understand its implications. I urge all US citizens to do the same from their personal perspective and to communicate with their Senators.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.