

Privacy Client Advisory

KELLEY DRYE
COLLIER SHANNON

May 26, 2006

House Judiciary Committee Passes Data Security Bill

EXECUTIVE SUMMARY

On Thursday, May 25, 2006, the House Judiciary Committee approved legislation intended to curb identity theft and its resulting harms. On the heels of recent revelations that the personal data of millions of military veterans was stolen, on a voice vote, the House Judiciary Committee passed H.R. 4127, entitled the "Data Accountability and Trust Act" or "DATA." This bill previously passed the House Energy and Commerce Committee in March. The version that passed the House Judiciary Committee yesterday was the same as the Energy and Commerce Committee's bill, except yesterday's bill also included a notification measure that would apply to federal agencies.¹ If enacted, the House Judiciary bill would impose data protection, investigation, and notice obligations on businesses, information brokers, and federal agencies.

Specifically, the DATA bill would:

- 1) Require the Federal Trade Commission ("FTC") to promulgate regulations that require companies to safeguard personal information;
- 2) Require companies to notify U.S. consumers if their personal information is compromised by a data security breach that creates a "reasonable risk" of identity theft, fraud, or other unlawful conduct to the affected individual;
- 3) Require federal agencies to notify U.S. consumers if their personal information is acquired by an unauthorized person;

- 4) Impose a number of safeguard, verification, access, correction, and audit requirements on information brokers;
- 5) Preempt similar state laws; and
- 6) Provide the FTC and state attorneys general with enforcement power.

The DATA bill contrasts in some significant ways with the data security bill that passed the House Financial Services Committee (H.R. 3997). That bill, entitled the "Financial Data Protection Act of 2005," applies only to "consumer reporters"² and restricts enforcement power to the functional federal regulator or the applicable state insurance authority for entities engaged in the business of insurance.

By comparison, the DATA bill is much broader and would apply to all entities that fall within the FTC's jurisdiction under the Federal Trade Commission Act and the jurisdiction of state attorneys general. The provisions of the DATA bill are summarized in more detail below.

DATA SECURITY SAFEGUARDS

The bill would require the FTC to promulgate regulations concerning policies and procedures for safeguarding electronic personal information, including:

- A security policy regarding the collection, use, sale, and other sending or maintenance of personal information;

¹ This amendment was proposed by Reps. Robert Wexler (D-Fla.) and Bobby Scott (D-Va.).

² H.R. 3997 defines a "consumer reporter" as "any consumer reporting agency or financial institution, or any person which, for monetary fees, dues, on a cooperative nonprofit basis, or otherwise regularly engages in whole or in part in the practice of assembling or evaluating consumer reports, consumer credit information, or other information on consumers, for the purpose of furnishing consumer reports to third parties or to provide or collect payment for or market products and services, or for employment purposes, and which uses any means or facility of interstate commerce for such purposes."

- Appointing an individual responsible for managing information security; and
- A process for taking preventive and corrective action to mitigate against reasonably-foreseeable security vulnerabilities (e.g., encryption or other technology that safeguards data, changes to practices, and changes to the architecture, installation, or implementation of network and operating software).

The FTC's regulations on these practices must take into account:

- The size, nature, scope, and complexity of the activities engaged by the business;
- The current administrative, technical, and physical safeguards for electronic information; and
- The cost of implementing such safeguards.

This flexible standard is the same as the one currently enforced by the FTC under the Gramm-Leach-Bliley Act and Federal Trade Commission Act.

PERSONAL INFORMATION

The bill defines "personal information" as an individual's first and last name in combination with any of the following data elements:

- Social Security number;
- Driver's license number or other state identification number; or
- Financial account number, credit or debit card number, required security code, access code, or password that is necessary to permit access to an individual's financial account.

To accomplish the purposes of the Act, the FTC may modify the definition of this term if

necessary to accommodate changes in technology or practices and it will not unreasonably impede interstate commerce.

BREACH

The bill defines a "breach of security" as the compromise of electronic personal information if the business has a "reasonable basis to conclude that there is a reasonable risk of identity theft to the individual to whom the information relates." If, however, the information was encrypted or protected by other methods of technology approved by the FTC, a presumption would apply that there is not a reasonable basis to conclude that identity theft would result. This presumption can be rebutted by facts demonstrating that the encryption or other safeguard method has been or is likely to be compromised.

NOTICE

Following the discovery of a system's breach, the owner or possessor of such system(s) would be required to:

- Notify each individual whose personal information was acquired by the unauthorized access to the system(s);
- Notify the FTC;
- Place a conspicuous notice on the business's website (if it maintains a website) that includes a toll-free telephone number that an individual may use to find out more information about the breach or the information compromised; and
- If the breach involved financial account information of a merchant, notify the financial institution that issued the account.
- The standard for when federal agencies must notify consumers appears to be more stringent than that imposed upon the business

community, requiring notification when the information is *acquired* by an unauthorized person. Businesses, by contrast, must notify consumers when there is a “reasonable basis to conclude” that the unauthorized access of personal information will result in identity theft, fraud, or other unlawful conduct to the affected individual.

The DATA bill also differentiates between government and the private sector in the time frame in which notice of data breaches shall be provided. Businesses are required to provide notice “as promptly as possible and without unreasonable delay,” and the business would be required to take necessary measures to determine the scope of the breach, prevent further breaches or unauthorized disclosures, and reasonably restore the integrity of the data system(s). This provision does not appear to apply to federal agencies that have experienced a breach. The law provides for an affirmative defense if all of the personal information in the breached data was public record information. No affirmative defense would apply to “mixed” information that comprises information from public records and information obtained through other means.

The notice to consumers of the breach must be written or sent via e-mail (if in compliance with the Electronic Signatures Act), and include a description of the compromised personal information, a toll-free telephone number that an individual may use to find out more information about the breach or the information compromised, a toll-free contact telephone number and addresses for the major credit reporting agencies, and the FTC’s toll-free telephone number and website address.

Substitute notice may be provided in lieu of the bill’s standard notice if direct notice is not feasible due to excessive cost relative to the resources of

the business, or a lack of contact information for the affected individuals. The bill describes the information that must be included in the substitute notice.

INFORMATION BROKERS

The bill would impose additional requirements on data-collecting companies, referred to as “information brokers” (“IBs”). The bill defines an IB as:

a commercial entity whose business is to collect, assemble, or maintain personal information concerning individuals who are not customers of such entity for the sale of such information or the provision of access to such information to any third party, whether such collection, assembly, or maintenance of personal information is performed by the information broker directly, or by contract or subcontract with any other entity.

Businesses that fall within this definition would be required to submit their security policies to the FTC on an annual basis. If an IB incurs a breach in its information system(s), the FTC would audit the IB’s security practices and may conduct additional audits annually until the Commission determines that the IB’s security practices are in compliance.

An IB also would be required to provide annual access to individuals for review of collected personal information if the IB maintains personal information about them (except if access is limited by law, by a legally recognized privilege, or is being used for a government or fraud prevention purpose). The IB also must provide website notice that explains how consumers can request access to review their information. If an individual disputes the accuracy of the information maintained, the IB must clearly note

in its systems and in any subsequent transmission of such information the individual's statement disputing the accuracy of such information, or a clear and concise summary of the dispute (with some exceptions for frivolous or irrelevant disputes).

Additionally, the bill:

- Gives the FTC the authority to deem entities who are in compliance with the Fair Credit Reporting Act to be in compliance with this bill's requirements for IBs.
- Expressly allows entities to sell or transfer information to affiliates without being considered an IB;
- Excludes mailing lists, non-identifying information, and aggregate data from the scope of the IB provisions;
- Requires IBs to establish reasonable procedures to verify the accuracy of information collected and maintained;
- Prohibits pretexting by IBs; and
- Exempts telecommunications carriers, cable operators, information services, and interactive computer services from the IB requirements.

REMEDIAL EFFORTS

Responsible entities must provide or arrange for free credit reports from a major credit reporting agency to be sent to affected consumers on a quarterly basis for two years with instructions on how to request such reports.

FTC WEBSITE POSTING

The bill would require the FTC to post in a clear and conspicuous location on its website a notice of

a breach of security reported to the Commission if it determines that such notice would be in the public interest or would protect consumers.

ENFORCEMENT

A violation of the bill would constitute an unfair or deceptive act under the FTC Act. State attorneys general, state officials, or state agencies also would be permitted to bring an action to enjoin further violations, to compel compliance, and to obtain civil penalties (capped at \$5 million). Private civil actions for violations of the bill are expressly prohibited.

PREEMPTION

The bill generally would preempt state laws that regulate information security safeguards, data breach investigations, and notices of data breaches, but would expressly preserve state consumer protection laws, state trespass, contract, tort laws, and other state laws to the extent that those laws generally relate to acts of fraud.

KELLEY DRYE COLLIER SHANNON

ADVERTISING AND MARKETING PRACTICE GROUP

Kelley Drye Collier Shannon's Advertising and Marketing practice comprises attorneys with proven success in advertising litigation and NAD proceedings; expertise in the area of advertising, promotion marketing, and privacy and data security law; and experience at the FTC, FDA, and the Offices of State Attorneys General.

We are a leader in advising clients on information privacy issues and have been at the forefront of developments in this growing area of law. Our privacy law group regularly

advises clients regarding all aspects of privacy and data security law, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the EU Data Protection Directive (as well as EU members' state laws and the Safe Harbor negotiated between the US and the EU), the FTC Act, and state privacy and data security laws.

**GOVERNMENT RELATIONS AND
PUBLIC POLICY PRACTICE GROUP**

Our Government Relations practice helps clients interpret and shape governing laws, enabling them to maintain or achieve market leadership. Our experienced privacy attorneys work closely with our Government Relations and Public Policy practice group to stay abreast of new laws and regulations.

FOR MORE INFORMATION

For more information about this development, please contact one of our team members at (202) 342-8400 or via email:

Partners

Reed Freeman	RFreeman@KelleyDrye.com
James S. Gilmore, III	JGilmore@KelleyDrye.com
William C. MacLeod	WMacLeod@KelleyDrye.com
Lewis Rose	LRose@KelleyDrye.com
John E. Villafranco	JVillafranco@KelleyDrye.com

Associates

Ponneh Aliabadi	PAliabadi@KelleyDrye.com
Christie Grymes	CGrymes@KelleyDrye.com
Jeffrey A. Kauffman	JKauffman@KelleyDrye.com
Jason K. Levine	JLevine@KelleyDrye.com
Gonzalo Mon	GMon@KelleyDrye.com
Dustin Painter	DPainter@KelleyDrye.com
Alysa N. Zeltzer	AZeltzer@KelleyDrye.com

Independent Contractors

Elisa A. Nemiroff	ENemiroff@KelleyDrye.com
Julie G. O'Neill	JO'Neill@KelleyDrye.com

www.kelleydrye.com