

## Congressmen Stearns and Barton Release Draft Data Security Legislation

### EXECUTIVE SUMMARY

Following the introduction of data security legislation by Senators Specter and Leahy last week, Representative Joe Barton (R-TX), Chairman of the House Energy and Commerce Committee, and Representative Cliff Stearns (R-FL), Chairman of the Energy and Commerce Committee's Subcommittee on Consumer Protection, released a working draft of a similar (but less comprehensive) data security bill. The legislation is likely to be introduced in the next couple of weeks.

Representative Stearns introduced a more narrow data security bill this past March – H.R. 1263, The Consumer Privacy Protection Act of 2005 – which focused on the practices of “data collection organizations” only. In response to concerns that were provided at recent Congressional hearings on security breaches and data security practices, the recently-introduced bill has a broader scope that applies to all businesses that own or use consumers’ personal data, steps to take in the event of a security breach, and a number of specific requirements that apply to “information brokers.”

Chairman Barton and Chairman Stearns have indicated that they intend to work on a bipartisan basis to move this bill forward and have sought comments from those interested in providing feedback on the bill at two stages:

1. Before July 11 (prior to introducing the bill); and
2. After the subcommittee mark-up.

Kelley Drye Collier Shannon is actively engaged in the legislative debate on data protection. If you are interested in commenting on the current version and would like assistance in formulating those comments, please do not hesitate to contact us at [azeltzer@kelleydrye.com](mailto:azeltzer@kelleydrye.com).

Key features of the legislation include:

- Requiring businesses that own or possess personal information to establish a security program to protect such information;
- Requiring businesses to distribute notice to affected individuals and law enforcement when there is a possibility that personally identifiable information has been compromised;
- Requiring businesses that own or possess personal information to provide affected individuals with free credit reports and a subscription to a credit monitoring service if an individual's personal information has been compromised; and
- Requiring information brokers to annually submit their security policies to the Federal Trade Commission (“FTC”).

A more detailed summary and analysis of the key provisions of the bill are provided below.

## SUMMARY AND ANALYSIS OF THE ACT

### Data Privacy and Security Safeguards

The Act is intended to protect consumers' "personal information," which is defined as:

An individual's first and last name in combination with any one or more of the following data elements for that individual:

1. Social Security number;
2. Driver's license number or other state identification number; or
3. Financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.<sup>1</sup>

The bill would require persons or entities that conduct interstate commerce and that own or possess personal information in electronic form to implement policies and procedures that would protect the security of the personal information (i.e., a security program). The policies and procedures must include:

- Security policy that addresses the "collection, use, sale, other dissemination, and security of such personal information;"
- Appointment of an officer who will be the point of contact for information security issues; and
- An established process for taking pre-

<sup>1</sup> This definition is narrower than the earlier-introduced H.R. 1263's definition of "personally identifiable information," that definition included both e-mail addresses and telephone numbers.

ventive and corrective action, including encryption technologies, to solve weaknesses in and problems with a business's security.

### Notification Requirements

The bill defines "breach of security" as the "compromise of the security, confidentiality, or integrity of data that results in, or there is a reasonable basis to conclude has resulted in, the acquisition of personal information by an unauthorized person that may result in identity theft."

If a security breach occurs, the bill would require any person or entity engaging in interstate commerce that owns or possesses electronic personal information to notify three parties:

1. Individual whose personal information was reasonably believed to have been compromised;
2. the FTC; and
3. Financial institution that issued the account if the breach compromised financial account information. All notices must be made "as promptly as possible and without unreasonable delay."

Persons or entities that discover a security breach would be required to provide written notice and email notification, assuming the person or entity has the individual's email address and the consumer has consented to receive such email notifications. Persons or entities that discover a security breach also would be required to place a "conspicuous" notice on their website if they maintain a website.

The content of the notice must include:

- Description of the personal information that is reasonably believed to have been compromised;
- Toll-free telephone number that individuals may call to inquire about the security
- breach or the nature of their personal information that was maintained;
- Toll-free contact numbers and addresses for the major credit reporting bureaus and credit repair services; and
- Toll-free telephone number and website address for the FTC where an individual can find information on identity theft.

The bill would permit a substitute form of notice but only when the cost to notify an affected individual is excessive in relation to the person's or entity's resources, or when the person or entity does not have access to the contact information necessary to notify an affected individual. If either of these circumstances applies, the person or entity may provide substitute notice by advertising the breach of security in major print and broadcast media outlets in the areas where affected individuals reside. Alternatively, responsible persons or entities may provide substitute notice by posting a "conspicuous" notice on their website. Substitute notifications are to include a toll-free phone number where individuals can learn whether their personal information was affected by the security breach.

Persons or entities that discover a security breach of their system(s) also are required to arrange for affected individuals to receive their credit report from each of the major credit reporting agencies and a one-year subscription to a credit monitoring service, all at no charge to the affected individual.

### Information Brokers

The bill defines an "information broker" as:

a commercial entity whose business is to collect, assemble, or maintain personal information for the sale or transmission 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.

The bill would require information brokers to submit their security policies to the FTC on an annual basis. In addition, at least once per year, an information broker would be required to permit an individual to review their personal information maintained by the information broker upon the individual's request and at no cost to the individual. Information brokers also would be required to post a "conspicuous notice" on their websites that provide details on how individuals can access their personally identifiable information.

### Violations

Violations would be treated as an unfair or deceptive act or practice in violation of the FTC Act, 15 U.S.C. § 57a(a)(1)(B).

### Preemption

The bill would supersede state laws only to the extent that they are inconsistent. Among other provisions, laws regulating electronic data security breaches or notices of a security breach would be preempted.

## KELLEY DRYE COLLIER SHANNON

## FOR MORE INFORMATION

**ADVERTISING AND MARKETING LAW  
PRACTICE GROUP**

Kelley Drye Collier Shannon's Advertising & Marketing practice comprises attorneys with proven success in advertising litigation and NAD proceedings; expertise in the area of advertising, promotion marketing, and privacy law; and experience at the FTC, FDA, and the Offices of State Attorneys General. We help leading companies identify risks, respond effectively to inquiries, and prevail in contested proceedings.

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 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 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.

Kelley Drye Collier Shannon is on the forefront of developing privacy industry guidelines and regulations. Please visit [www.kelleydrye.com](http://www.kelleydrye.com) for more information or if you would like to receive our daily privacy e-newsletter.

If you have any questions about this alert, please contact one of our team members at (202) 342-8400 or via email:

**Partners**

William C. Macleod  
[wmacleod@kelleydrye.com](mailto:wmacleod@kelleydrye.com)

Lewis Rose  
[lrose@kelleydrye.com](mailto:lrose@kelleydrye.com)

John E. Villafranco  
[jvillafranco@kelleydrye.com](mailto:jvillafranco@kelleydrye.com)

**Special Counsel**

Julie G. O'Neill  
[joneill@kelleydrye.com](mailto:joneill@kelleydrye.com)

**Associates**

Ponneh Aliabadi  
[paliabadi@kelleydrye.com](mailto:paliabadi@kelleydrye.com)

Christie Grymes  
[cgrymes@kelleydrye.com](mailto:cgrymes@kelleydrye.com)

Jeffrey A. Kauffman  
[jkauffman@kelleydrye.com](mailto:jkauffman@kelleydrye.com)

Gonzalo Mon  
[gmon@kelleydrye.com](mailto:gmon@kelleydrye.com)

Elisa A. Nemiroff  
[enemiroff@kelleydrye.com](mailto:enemiroff@kelleydrye.com)

Dustin Painter  
[dpainter@kelleydrye.com](mailto:dpainter@kelleydrye.com)

Alysa N. Zeltzer  
[azeltzer@kelleydrye.com](mailto:azeltzer@kelleydrye.com)