JONES DAY

FEBRUARY 2014

U.S. CONGRESS READY TO ENACT DATA SECURITY AND BREACH NOTIFICATION RULES AFTER RECENT CONSUMER DATA BREACHES

In December 2013, a U.S. national retail store announced that credit and debit card data for more than 40 million consumers may have been compromised. On January 10, it further disclosed that cyber criminals had accessed a wide range of personal information belonging to 70 million people through point-of-sale terminals—equipment that annually facilitates more than $3 trillion in U.S. customer transactions throughout various industries.[1] Another major retailer has since made similar disclosures. These are the latest known victims of cyber attacks that have targeted payment systems and consumer data collections and have exposed millions of Americans to the threat of identity theft.

After a series of hearings this past week, Congress appears ready to enact a national data protection and breach notification law.

EXISTING DATA PROTECTION AND BREACH NOTIFICATION LAWS

Currently, in the United States, a company's possession and use of consumer data is regulated by a patchwork of industry-specific federal laws and generally applicable state data protection and/or notification laws. At the federal level, the Gramm-Leach-Bliley Act ("GLBA") and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") are two prominent examples. The GLBA applies to financial institutions and provides for the implementation of standards to limit the purposeful disclosure of and protect against unauthorized access to consumers' "nonpublic personal information."[2] The GLBA also mandates that a financial institution provide to its consumers notice of its policies on sharing nonpublic personal information.[3] HIPAA, on the other hand, sets national standards for the security of electronically protected health information.[4] Additionally, HIPAA requires covered entities—i.e., health care providers, health plans,

and health care clearinghouses—and business associates to give notice to consumers whose unsecured protected health information has been compromised due to a breach.[5]

In addition to industry-specific federal laws, there are numerous state and territorial personal data protection laws. While these laws serve the same general purpose of protecting individuals from identity theft, some vary as to the obligations they impose. For example, once unencrypted personal information is shown to have been compromised, most state laws require that notice be provided to affected individuals or the company that owns the data, depending on who suffered the breach. Some states also require the company that owns the data to notify consumer reporting agencies in certain circumstances.[6] In the same vein, some states require that notice be given to the state's attorney general or other state agency whenever any state resident must be notified of a data breach,[7] and other states require such notice only if a certain number of state residents must be notified.[8] However, the majority of states do not require any notice to the attorney general or other state agency.[9]

Likewise, many states require that notice be provided to affected consumers within the most expedient time and manner possible,[10] but some set specific time limits within which such notice must be provided.[11] Similarly, some state laws are silent as to the required content of the notification,[12] while others specifically require that the notification include such items as a general description of the security breach, the types of consumer data compromised, and steps taken to prevent future breaches of that data.[13]

Finally, a majority of states have not mandated specific security measures for the protection of consumer data. But some states require that an owner or licensor of personal information do one or more of the following: implement reasonable security procedures to protect personal data from unauthorized access,[14] maintain written information security programs,[15] and impose on third parties to which data is disclosed a contractual requirement to implement the aforementioned procedures. [16]

CONGRESS APPEARS READY TO ACT

In view of the recent spate of cyber attacks on retailers and the patchwork of existing laws that greatly complicate a company's data breach response, Congress appears ready to create a national data protection and breach notification law that, in theory, would increase the security of consumers' personal information and simplify the data breach notification process.

Statements made publicly during Congressional hearings this past week evidence a tacit agreement between Democrats and Republicans that a national data protection and breach notification law should not mandate a particular security standard, given that technology is rapidly advancing and that every data breach is factually distinct. That said, Congressional leaders suggested that better technological safeguards are needed, and many pointed to Europe's adoption of "chip-and-PIN" credit cards as an appropriate step forward. For example, Representative Peter Welch (D-VT) noted that "chip-and-PIN technology is what is now being used in Europe and it has better success in preventing fraud."[17] Representative Lee Terry (R-NE) noted that the United States "accounts for 47% of the fraud credit and debit losses worldwide, while only accounting for 30% of the transactions."[18] And Senator Al Franken (D-MN) and Senator Richard Blumenthal (D-CT) reiterated the same, implying that other countries have been more successful at preventing fraud by using chip-and-PIN technology.[19]

Although the two political parties agree that consumer information must be better protected, they differ in how this protection should be obtained. Generally, Democrats appear to advocate for a strong national regulation that would impose an obligation upon handlers of consumer data to take reasonable security measures to protect that data and that would grant rulemaking authority to the Federal Trade Commission ("FTC") to promulgate technology-appropriate rules. For example, Senator Franken stated that currently, "there's no federal law setting out clear security standards that merchants and data brokers need to meet. And there's no federal law requiring companies to tell their customers when their data has been stolen."[20] He then concluded that "Congress needs to pass laws that promote data security."[21] Senator Chris Coons (D-DE) opined that there was "a strong

federal role here in ensuring strengthening cybersecurity and privacy."[22] Senator Elizabeth Warren (D-MA) observed that "we may need some pressure from the government to make sure that the toughest standards are used."[23] Senator Dianne Feinstein (D-CA) said that "any bill that's forthcoming from this institution should provide notification of customers that their data may have been breached so they can protect themselves."[24] And Representative Jan Schakowsky (D-IL) advocated for legislation that will ensure that best practices are followed as soon as possible after discovery of the theft of data and suggested a technology-neutral law that allowed the FTC and other agencies the power to update the requisite standards.[25]

The Republicans set a more cautious tone at the hearings. Representative Terry said that "[f]lexibility, quickness and nimbleness are all attributes that absolutely are necessary in cybersecurity, but run contrary to government's abilities.... We must encourage the private sector to keep improving on its consensus-driven standards, which are built to adapt over time [to] changing threats to data security."[26] Representative Mike Pompeo (R-KS) suggested that circumstances may not be ripe for legislation and that Congress should not overreact to media hype.[27] He also suggested that consumers may themselves force change by avoiding companies with weak data security measures in place.[28] And Senator Charles Grassley (R-IA) argued for a flexible approach in which the government partners with private business to strengthen data security.[29] He referred to the voluntary cybersecurity framework being developed by the National Institute of Standards and Technology as a possible model.[30]

CONGRESS IS NOT THE ONLY STAKEHOLDER

Although Congress has a strong interest in protecting consumer data, other significant stakeholders participated in the recent Congressional hearings as well. Retail representatives recognized the need for greater transparency and information-sharing when it comes to combating cyber attacks.[31] Various witnesses also emphasized that updating payment card technology is important, but that more is needed to address the many consumer transactions that are conducted via the internet and through emerging mobile payment methods.[32]

Lisa Madigan, the Attorney General of Illinois, advocated for a strong national law but cautioned that federal law should not preempt state laws.[33] Rather, she argued that any federal law should establish a floor upon which states can provide stronger protections where necessary and, at the very least, should allow for concurrent state enforcement rights.[34] For its part, the FTC voiced support for legislation that would strengthen existing data security standards, require notification in the event of a data breach, and provide to the FTC rulemaking authority under the Administrative Procedure Act and authority to seek civil penalties to enforce the law.[35] FTC representatives also favored giving states concurrent enforcement powers and, like most lawmakers, did not support government regulations requiring the use of any particular technological standard, such as chip-and-PIN technology.[36]

CONGRESS IS QUICKLY ADVANCING LEGISLATION

Not surprisingly, there are four separate legislative proposals that have been offered in the Senate, one of which was also offered in the House of Representatives. All but one are partisan efforts from the Democratic Party.

Senator Pat Leahy (D-VT), together with co-sponsors Senators Chuck Schumer (D-NY), Franken, and Blumenthal, were the first to sponsor a recent bill.[37] Representative Carol Shea-Porter (D-NH) has since offered the same bill in the House of Representatives.[38] The bill requires that entities handling personal information of 10,000 or more U.S. citizens implement stringent security measures, including a system of auditing the effectiveness and vulnerabilities of the security system. Should an entity suffer a breach that compromises the security of stored personal information, the entity must notify affected consumers without unreasonable delay, but no later than 60 days after discovery of the breach. If 5,000 or more persons are affected by the breach, or the database affected by the breach stores such information for 500,000 or more persons, the entity must notify federal law enforcement. Credit reporting agencies also must be notified of the breach if 5,000 or more persons are affected.

Shortly after Senator Leahy introduced his bill, Senator Jay Rockefeller (D-WV), together with Senators Mark Pryor (D-AR), Bill Nelson (D-FL), and Feinstein, co-sponsored their own proposal.[39] Unlike Senator Leahy's proposal, the Rockefeller bill requires that any business entity that handles personal information implement the prescribed security measures, even if that entity handles data for less than 10,000 persons. Additionally, this bill requires consumer notifications within 30 days of the discovery of a breach. While the bill requires notice to consumer reporting agencies if 5,000 or more persons are affected by a breach, notice to law enforcement under this bill is required only if 10,000 or more persons are affected. The proposed legislation also calls for covered entities to provide for up to two years of credit monitoring services to affected individuals.

The two bills have far more in common, however, than not. Both bills call for the FTC to develop and implement rules and regulations to execute the law. Both measures provide for civil penalties for violations of the security and notification provisions through various enforcement mechanisms, and both also call for criminal liability in the event a person with knowledge of the notification requirements conceals a data breach. The proposals also allow for concurrent enforcement by state attorneys general, although both preempt state data security and breach notification laws. Neither bill, however, allows for a private right of action based on violations of the requirements.

Perhaps motivated by the lack of a private right of action in both of these measures,[40] Senator Blumenthal, with the support of Senator Ed Markey (D-MA), also has sponsored his own measure.[41] The proposal contains many of the same requirements as the aforementioned proposals, but it differs in a few respects. Rather than provide an absolute deadline by which notice is required to be given to consumers, Senator Blumenthal's proposal simply requires such notice to be given "without unreasonable delay." However, in the event that law enforcement must be notified of the breach, such notice shall be given no later than 10 days after discovering the breach, and consumer notification must be delivered no later than 48 hours after law enforcement receives notice. In addition to providing to the state attorneys general concurrent enforcement powers, the bill also provides for a private right of action to enforce the requirements of and to recover damages for any violations of the laws. While the two prior bills cap the civil penalty amount for non-willful or unintentional violations at $1 million and $5 million respectively, Senator Blumenthal's bill provides for up to $20 million in penalties for such violations.

Unlike the other current proposals, and in line with the general consensus that information sharing is the most important weapon against data breaches, Senator Blumenthal's proposal also calls for a to-be-designated federal entity to establish and manage a clearinghouse in which information of data breaches is to be shared. The bill also requires the administrator of the General Services Administration to evaluate the data security programs of a data broker before entering into a government contract totaling more than $500,000 with that entity.

Senators Roy Blunt (R-MO) and Thomas Carper (D-DE) have proposed a bipartisan bill on the matter.[42] Their bill is less comprehensive and stringent than the other three proposals. It requires notice of a data breach to affected consumers only if the breach is likely to cause "substantial harm" to consumers. Substantial harm in this context does not include the need for consumers to change their account information or other harms that do not involve identity theft or account fraud. The bill does not establish a timeframe within which notice must be given but instead leaves that task for the rulemaking process. The bill also requires entities to implement certain security measures to protect data, but again leaves the task of providing specific guidance on effective security measures to the rulemaking process. Rather than granting the FTC exclusive rulemaking authority, however, the bill assigns to a number of industry-specific agencies the task of developing, implementing, and enforcing the rules. The bill does not provide for criminal liability, nor does it delineate any specific civil penalty for violating the requirements. This bill also preempts state law, and it does not give concurrent enforcement powers to state attorneys general or provide for a private right of action to affected individuals.

CONCLUSION

The general consensus among those who testified or otherwise spoke at the Congressional hearings was that more is needed to protect consumer information and to prevent identity theft in the United States. Participants were less agreeable, however, as to specific solutions, and future legislation will better judge the efficacy of these Congressional hearings.

With the widespread availability of sophisticated malware, additional breaches are inevitable. Congress now seems poised to propose new federal legislation that may increase obligations, liabilities, and costs to private industry. Interested parties are encouraged to monitor this rapidly developing area of law.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Shawn Cleveland
Dallas
+1.214.969.3732
Houston
+1.832.239.3794
scleveland@jonesday.com

Walter W. Davis
Atlanta
+1.404.581.8517
wwdavis@jonesday.com

Robert W. Kantner
Dallas
+1.214.969.3737
rwkantner@jonesday.com

Matthew D. Orwig
Dallas
+1.214.969.5267
Houston
+1.832.239.3798
morwig@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Katherine Ritchey
San Francisco
+1.415.875.5728
ksritchey@jonesday.com

Jay Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Steven G. Gersten and Mina Saifi, associates in the Dallas Office, assisted in the preparation of this Commentary.

ENDNOTES

1 Cheyenne Hopkins, "Senators Call for Update of Data-Theft Rules After Target Breach," *Bloomberg Businessweek* (Feb. 4, 2014), http://www.businessweek.com/news/2014-02-03/senators-call-for-updated-protections-to-combat-data-breaches (citing David Robertson, publisher of the Nilson Report, for the proposition that "[m]ore than $3 trillion in U.S. customer transactions take place each year through the point-of-sale systems infiltrated by the hackers").

2 15 U.S.C. §§ 6801(b), 6802(a) (2012).

3 15 U.S.C. § 6803(a) (2012).

4 *Health Information Privacy,* U.S. Dep't of Health & Human Svcs., http://www.hhs.gov/ocr/privacy/ (last visited Feb. 12, 2014).

5 45 C.F.R Pt. 160 and 164.

6 *See*, e.g., Mo. Rev. Stat. § 407.1500(2)(8) (2013) (requiring notice be given to consumer reporting agencies in the event that 1,000 or more persons are notified of a data breach).

7 *See,* e.g., N.Y. Gen. Bus. Law § 899-aa(8)(a) (Consol. 2013).

8 *See*, e.g., Va. Code § 18.2-186.6(E) (2013) (requiring notice be given to the state attorney general in the event 1,000 or more persons must be notified of a breach); S.C. Code § 39-1-90(K) (2013) (requiring notice be sent to the Consumer Protection Division of the Department of Consumer Affairs in the event 1,000 or more persons must be notified of a breach).

9 *See*, e.g., Ohio Rev. Code Ann. § 1347.12 (LexisNexis 2013).

10 *See*, e.g., Ill. Comp. Stat. Ann. 530/10(a) (LexisNexis 2013).

11 *See*, e.g., Wis. Stat. § 134.98(3)(a) (2013) (requiring notice be given within 45 days of the entity learning of the data breach).

12 *See*, e.g., Del. Code Ann. tit. 6, §§ 12B-101 – 12B-104 (2013).

13 *See*, e.g., Mich. Comp. Laws Serv. § 445.72(6) (2013).

14 *See*, e.g., Tex. Bus. & Com. Code Ann. § 521.052 (West 2013).

15 *See* 201 Mass. Code Regs. 17.00 – 17.05 (2013).

16 *See*, e.g., Cal. Civ. Code § 1798.81.5(c) (Deering 2013).

17 "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Rep. Peter Welch).

18 "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Rep. Lee Terry).

19 "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Judiciary Comm.," 113th Cong. (2014) (statements of Sen. Al Franken and Sen. Richard Blumenthal).

20 "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Judiciary Comm.," 113th Cong. (2014) (statement of Sen. Al Franken).

21 *Id.*

22 "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Judiciary Comm.," 113th Cong. (2014) (statement of Sen. Chris Coons).

23 "Sen. Mark. Warner Holds a Hearing on Safeguarding Consumers' Financial Data: Hearing Before the Subcomm. on Nat'l Security and Int'l Trade and Finance of the S. Comm. on Banking, Housing and Urban Affairs," 113th Cong. (2014) (statement of Sen. Elizabeth Warren).

24 "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Judiciary Comm.," 113th Cong. (2014) (statement of Sen. Diane Feinstein).

25 "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Rep. Jan Schakowsky).

26 "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Rep. Lee Terry).

27 "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Rep. Mike Pompeo).

28 *Id.*

29 "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Judiciary Comm.," 113th Cong. (2014) (statement of Sen. Charles Grassley).

30 *Id.*; *see also* "Improving Critical Infrastructure Cybersecurity, Executive Order 13636, Preliminary Cybersecurity Framework," Nat'l Inst. of Standards and Tech., http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf (last visited Feb. 12, 2014).

31 *See*, e.g., "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014).

32 *Id.*

33 *See*, e.g., "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Lisa Madigan, Att'y Gen. of Illinois).

34 *Id.*

35 *See*, e.g., "Rep. Lee Terry Holds a Hearing on Protecting Consumer Info: Hearing Before the Subcomm. of Commerce, Mfg. and Trade of the H. Comm. on Energy and Commerce," 113th Cong. (2014) (statement of Edith Ramirez, Chairwoman of the FTC).

36 *Id.*

37 Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014).

38 Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2014).

39 Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014).

40 *See* "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime: Hearing Before the S. Judiciary Comm.," 113th Cong. (2014) (statement of Sen. Richard Blumenthal) ("[My bill] also provides for … in my view, very importantly, a private right of action….").

41 Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014).

42 Data Security Act of 2014, S. 1927, 113th Cong. (2014).