THE "DATA SECURITY ACT OF 2010" WOULD ESTABLISH NEW FEDERAL DATA BREACH NOTIFICATION AND DATA SECURITY REQUIREMENTS, AND WOULD BROADLY PREEMPT STATE LAW

Overview

Senators Tom Carper (D-Del.) and Bob Bennett (R-Utah) introduced a new Senate Bill on July 21, 2010, entitled the "Data Security Act of 2010" (the "Data Act" or the "Act"), which would adopt new federal data breach notification and data security requirements and broadly preempt the numerous existing state laws in these areas. The Data Act (which was originally introduced in 2007 but failed to pass) is the sixth major bill introduced in this Congress to address these issues that are of increasing concern at the state, federal, and international levels of government. If enacted, the Data Act, which is largely modeled after the Gramm-Leach-Bliley Act ("GLBA"), which applies to financial institutions, would expand breach notification and data security requirements to all U.S. businesses, while at the same time removing the existing patchwork of often-inconsistent regulations in these areas currently applied at the state and federal levels.

Entities Covered by the Data Act

Covered entities subject to the requirements of the Data Act are broadly defined to include, among others, financial institutions regulated under the GLBA[1] and any individual, partnership, corporation, trust, estate, cooperative, association, or entity that maintains or communicates "sensitive account information" or "sensitive personal information" ("Covered Entity" or "Covered Entities"). Covered Entities do not include any agency or other unit of the federal, state, or local government or any subdivision thereof, although, as noted below, a separate section of the Data Act requires governmental entities to adopt regulations governing their own operations and procedures in these areas.

Information Covered by the Data Act

Sensitive account information and sensitive personal information are covered by the Data Act ("Covered Data"). "Sensitive account information" is defined as a financial account number relating to a consumer,[2] including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account. ''Sensitive personal information'' is defined as the first

[1] Financial institutions that are regulated under the GLBA are those institutions subject to the jurisdiction of the following agencies: the Securities and Exchange Commission ("SEC"); Federal Trade Commission ("FTC"); Commodity Futures Trading Commission ("CFTC"); Board of Governors of the Federal Reserve System ("Federal Reserve"); Office of Thrift Supervision ("OTS"); Federal Deposit Insurance Corporation ("FDIC"); Office of the Comptroller of the Currency ("OCC"); and the National Credit Union Administration ("NCUA").

[2] A "consumer" is defined as an individual and can include employees, thus being a broader definition of consumer than that under the GLBA.

and last name, address, or telephone number of a consumer, in combination with any of the following relating to such consumer: (i) Social Security account number; (ii) driver's license number or equivalent State identification number; or (iii) taxpayer identification number. Sensitive personal information excludes publicly available information that is lawfully made available to the general public from government records or from widely distributed media (phonebook, Internet, etc.).

Key Provisions of the Data Act

Determination of a Data Breach

The principal requirements under the Data Act are triggered by a "breach of data security," which is defined as the unauthorized acquisition of Covered Data. However, a breach of data security does not include the unauthorized acquisition of Covered Data that is "maintained or communicated in a manner that is not usable to commit identity theft or to make fraudulent transactions on financial accounts." Some of the ways information can be made to be "unusable" for the purposes of the Data Act are if it is encrypted, redacted, altered, edited, or in coded form (none of these terms are defined by the Data Act; also note that the breach notification guidance adopted under the GLBA does not include such exceptions).

Investigation of a Data Breach and Notification

Once a Covered Entity determines that a breach of data security has or may have occurred, it must conduct an investigation to: (i) assess the nature and scope of the breach; (ii) identify any Covered Data that may have been involved in the breach; and (iii) determine if such information is reasonably likely to be misused in a manner causing "substantial harm or inconvenience"[3] to the consumers to whom the information relates.[4]

If a Covered Entity determines that Covered Data is involved in a breach of data security and is reasonably likely to be misused in a manner causing substantial harm or inconvenience to the consumers to whom the information relates, then notifications must be made by the Covered Entity or its agent in the following order: (i) the Covered Entity's primary regulator as defined in

[3] "Substantial harm or inconvenience" is defined as (i) "material financial loss to, or civil or criminal penalties imposed on, a consumer, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer; or (ii) the need for a consumer to expend significant time and effort to correct erroneous information relating to the consumer, including information maintained by a consumer reporting agency, financial institution, or government entity, in order to avoid material financial loss, increased costs, or civil or criminal penalties, due to the unauthorized use of sensitive account information or sensitive personal information relating to such consumer." Excluded from this important definition is "(i) changing a financial account number or closing a financial account; or (ii) harm or inconvenience that does not result from identity theft or account fraud."

[4] The Data Act provides guidance for determining the likelihood of misuse of sensitive account information by requiring that Covered Entities consider whether any "neural network or security program has detected, or is likely to detect or prevent, fraudulent transactions resulting from the breach of security." A risk of harm type analysis is also included in the majority of the state data breach notification laws as a determining factor as to whether notification is required under those laws, although the specific formulation of such harm thresholds often differs somewhat from state to state.

Section 5 of the Data Act;[5] (ii) the appropriate law enforcement authorities;[6] (iii) the owner or obligor of a financial account to which sensitive account information is related, if the breach involves sensitive account information; (iv) each national consumer reporting agency if the breach involves the sensitive personal information of 5,000 or more consumers; and (v) all consumers to whom the Covered Data relates. Following a breach, the Covered Entity must also take reasonable measures to restore the security and confidentiality of the Covered Data involved in the breach.

The Data Act would allow a consumer to be notified through either a writing, telephone call, email, or by substitute notification if those methods were not feasible due to lack of sufficient contact for the consumers or excessive cost to the Covered Entity. The contents of the notice must include: (i) a description of the Covered Data involved in the breach; (ii) a general description of the actions taken by the Covered Entity to restore the security and confidentiality of the Covered Data involved in the breach; and (iii) the summary of rights of victims of identity theft prepared by the FTC under the Fair Credit Reporting Act, if the breach involves sensitive personal information.

A financial institution shall be deemed to be in compliance with the investigation and notification requirements of the Data Act if it: (i) maintains policies and procedures to investigate and provide notice to consumers of data breaches that are designed to comply with the investigation and notification requirements established by regulation or guidance under Section 501(b) of the GLBA; and (ii) provides for notification to the required entities and consumers.[7]

Security Procedures

Covered Entities are required to implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of Covered Data of a Covered Entity from the unauthorized use of such information that is reasonably likely to result in substantial harm or inconvenience to the consumer to whom such information relates. These policies and procedures shall be appropriate to: (i) the size and complexity of a Covered Entity; (ii) the nature and scope of the activities of such entity; and (iii) the sensitivity of the consumer information to be protected.

The Data Act would deem a financial institution to be in compliance with its security policies and procedures requirements if the financial institution maintains policies and procedures to protect the confidentiality and security of Covered Data that are designed to comply with the requirements of Section 501(b) of the GLBA and any corresponding regulations or guidance applicable to such financial institution.

---

[5] These agencies and authorities would include the SEC, FTC, CFTC, Federal Reserve, OTS, FDIC, OCC, NCUA, the Director of Federal Housing Enterprise Oversight and the state insurance authorities (the "Regulators").

[6] Much like many state data breach notification laws, the Data Act allows a Covered Entity to delay notification to consumers if law enforcement requests such a delay in writing.

[7] This provision for deemed compliance also applies to affiliates of bank holding companies.

Regulations

The Data Act requires the Regulators to work together to prescribe "consistent and comparable" regulations to implement the requirements of the Data Act, such as those pertaining to security procedures, the methods for providing consumer notice of a data breach, contents of the notice, timing of the notice, and the requirement that service providers inform Covered Entities of breaches, as well as coordinate with the Covered Entities to ensure that only one of them provides the required notification in case of a breach.

Preemption of State Law

The Data Act would preempt all state laws that concern breach notification and investigation, as well as laws and regulations regarding the security and safeguarding of consumer information. Specifically, the Data Act would preempt any law of any state with respect to the responsibilities of any person to "(1) protect the security of information relating to consumers that is maintained or communicated by, or on behalf of, such person; (2) safeguard information relating to consumers from potential misuse; (3) investigate or provide notice of the unauthorized access to information relating to consumers, or the potential misuse of such information for fraudulent, illegal, or other purposes; or (4) mitigate any loss or harm resulting from the unauthorized access or misuse of information relating to consumers."

The result of this preemption would be that many state laws concerning the protection and disposal of sensitive personal information would no longer be in effect, including the data breach laws in effect in 46 states, the District of Columbia, and the U.S. Territories, as well as data security laws such as the one recently effective in Massachusetts, which have more detailed requirements regarding security than are contained in the Data Act.

Application to Federal Agencies

Each federal agency is required to implement similar standards and requirements with respect to the safeguarding of, and the breach notification regarding, Covered Data that is maintained or is being communicated by, or on behalf of, that agency.

Effective Dates

The regulations required to be adopted by the Regulators as described above must be issued no later than six (6) months after the Data Act is enacted, and they must take effect no later than six (6) months after the regulations are issued in final form. However, the effective date for the provisions of the Data Act concerning security procedures, data breach investigation and notification, and preemption of state laws would be delayed, so that they would take effect on the later of one year from the date of enactment of the Data Act or the effective date of the final regulations.

Enforcement / No Private Right of Action

Section 5 of the Data Act specifies the Regulators that will enforce the regulations under the Data Act. These provisions closely track the jurisdiction and enforcement provisions of the GLBA, with state insurance authorities enforcing the regulations with respect to any person engaged in the provision of insurance, and with the FTC enforcing the regulations for any Covered Entity that is not subject to the jurisdiction of any agency or authority described in the other provisions of the Data Act. The FTC's jurisdiction is expanded by the Data Act to cover air carriers and foreign air carriers, as well as persons and entities covered by the Packers and Stockyards Act.

The Data Act specifically states that there is no private right of action provided for under the Act, including a class action with respect to any act or practice regulated by the Act. The Data Act further states that no civil or criminal action relating to any act or practice governed under the Act or its regulations may be commenced or maintained in any state court or under state law, including a pendent state claim to an action under federal law.

Related Federal Legislation

While the Data Act is the latest bill introduced in Congress to call for a federal standard for data breach notification and/or data security requirements that would apply to a wide range of companies, it is not the only proposed legislation attempting to address these issues. Notably:

- The "Data Accountability and Trust Act" (H.R. 2221), introduced by Rep. Rush (D-Ill.), passed by the House in December 2009, and referred to a Senate subcommittee, would, among other things: (i) require all businesses engaged in interstate commerce to implement data security programs consistent with new FTC rules and to notify individuals if their electronic unencrypted personal information is breached; (ii) preempt all state data security and data breach notification laws; and (iii) implement a harm threshold under which a business that determines after a breach "that there is no reasonable risk of identity theft, fraud, or other unlawful conduct" is not required to provide notice of the breach (if the breached personal data is encrypted, a presumption would be raised that there is insufficient risk present to trigger the notification requirement; this presumption can be rebutted with evidence that encryption has been or is reasonably likely to be compromised). The FTC would be charged under the bill with examining whether the use of other technologies besides encryption should also give rise to the presumption of no risk.

- The "Data Breach Notification Act" (S. 139), introduced by Sen. Dianne Feinstein (D-CA) in January 2010, would require any business engaged in interstate commerce that uses, accesses, or collects sensitive personally identifiable information ("PII"), following the discovery of a security breach, to notify: (i) any U.S. resident whose information may have been accessed; (ii) the owner or licensee of any PII that the business does not own or license; and (iii) law enforcement in certain situations. It also authorizes federal and state enforcement actions and civil penalties. Notification is not required if a risk

assessment concludes that there is no significant risk that the security breach has resulted in, or will result in, harm to the individual whose sensitive PII was subject to the security breach. The bill would preempt all other state and federal laws regarding breach notification, except for state laws that mandate additional content in the notice regarding victim protection. This bill has been placed on the Senate's calendar for consideration.

- Sen. Leahy (D-Vt.) introduced the "Personal Data Privacy and Security Act" in July 2009 (S. 1490), which would, among other things: (i) require business entities engaged in interstate commerce involving personal information (other than GLBA- and HIPAA-regulated entities) to conduct a risk assessment and design and implement a comprehensive data privacy and security program; (ii) create an Office of Federal Identity Protection within the FTC; and (iii) require businesses to notify within 14 days any U.S. resident of a breach that compromises the individual's personal information, unless a risk assessment concludes that there is no significant risk of harm to the affected individuals (with encryption creating a presumption of no significant risk). For data breaches where the entity concludes that there is no risk of harm, the Secret Service must be notified and has ten (10) days to overrule the entity's decision not to notify. A business is exempt from the data breach notification provisions if the breach involves only credit card-related information, and the business utilizes a security program that detects and blocks fraudulent financial transactions and provides for notice to individuals if fraud occurs. This exemption does not apply if the breach involves the person's full credit card number and full first and last names. The U.S. Attorney General would have primary enforcement authority for the data breach notification provisions, with state Attorneys General having authority in the absence of federal proceedings. The law would preempt any other provision of federal law and all state laws relating to breach notification (except state laws requiring that the notification contain additional information about victim protection assistance). This bill has also been placed on the calendar for the consideration of the full Senate.

- Congressman Boucher (D-Va.) released a discussion draft of proposed legislation in May 2010 that would establish broad new privacy protections for individuals and would affect a wide variety of businesses that collect, use, or disclose certain information about individuals, both online and offline. (See our Willkie Client Memo dated May 20, 2010, which provides a detailed summary and analysis of this discussion draft.) Congressman Boucher received a number of comments on his discussion draft and is in the process of considering those comments before releasing a bill.

- Rep. Bobby Rush (D-Ill.) released on July 20, 2010 a privacy bill called "Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act" or "Best Practices Act." The Rush bill contains certain provisions that seem to address issues raised by privacy groups and industry in comments on the Boucher bill. For example, the Rush bill includes a private right of action provision that was supported by privacy groups. The Rush bill also provides that businesses complying with a self-regulatory "Choice Program" approved by the FTC would have a safe harbor from private right of action. Addressing industry

concerns, the Rush bill also excludes from its definition of covered information any information collected from or about an employee by an employer, prospective employer, or former employer that relates to the employee-employer relationship. On July 22, 2010, a panel of the House Committee on Energy and Commerce held a hearing to examine both the Rush bill and the Boucher bill. Consumer groups and privacy advocates were divided on the bills, with the Center for Digital Democracy speaking out in favor of the legislation, while U.S. PIRG argued that the bills don't go far enough, stating that they "largely sanction the existing and worsening regime of ongoing collection, analysis and use of off- and online data, through the industry-preferred regime of notice and choice." Businesses such as Intel and other industry groups such as the Interactive Advertising Bureau[8] indicated their concern with the flexibility of the Rush bill and its effect on commerce. Rep. Kathy Castor (D-Fla.) was also concerned with the bills' effect on the economy, stating that businesses must be allowed to "grow and flourish." The FTC also submitted testimony stating that it supports proposals for data security and accuracy requirements, but that it believes the legislation needs to be amended to include simplified disclosure requirements by companies, and to create one streamlined consent mechanism to avoid consumer confusion. The FTC testimony also stated that it does not support allowing all companies to share consumer data with its affiliates without prior consent. In addition, Rep. Ed Whitfield (R-Ky.), the top Republican on the committee, was concerned about the considerable size of the proposed legislation, stating that "it would be difficult for Congress to be involved in every nuance of privacy." He also said he was troubled about the amount of latitude that the bills would give to the FTC. Rep. Cliff Stearns (R- Fla.) voiced his apprehension about the civil penalties in the Rush bill and thought it contained an overbroad definition of covered information. Finally, Rep. Rush stated that he was not attempting to hurry the bill through Congress even though the hearing was only a few days after his bill was introduced, but that it was "time for the discussion to end and the work to begin."

* * *

At this point it is unclear which of the above proposed legislation, if any, will gain enough momentum to be enacted by Congress. However, as certain members of Congress appear to be determined to reform the nation's privacy and data security laws, businesses should closely monitor these bills. They should also watch developments abroad, as the European Union and many other countries are also currently considering new laws that would adopt or expand breach notification and data security requirements that apply to entities doing business in their jurisdictions.

For a more detailed description of each of the above privacy bills, and of the other key developments in the data privacy and data security area at the federal, state, agency, judicial, and

[8] Its board members include representatives of Google, Facebook, Microsoft, AOL, Comcast, Amazon.com, Fox Interactive, and CBS Interactive.

industry levels, please email Francis M. Buono at fbuono@willkie.com to be added to Willkie's distribution list for receipt of our quarterly omnibus update on these issues.

* * * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Francis M. Buono (202-303-1104, fbuono@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com), McLean B. Sieverding (202-303-1163, msieverding@willkie.com), or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

July 28, 2010