Paul Hastings
ATTORNEYS

August 2005

StayCurrent
A Client Alert from Paul Hastings

Data Protection Legislation Moves Forward in the Senate: Increased Congressional Activity Expected this Fall

by Behnam Dayanim and Vance Schuemann*

The rash of highly public incidents involving breaches of personal information held by banks, universities, information services and others seems to have made inevitable the passage of federal legislation requiring the protection of personal data and notice of unauthorized access. Personal information relating to more than 50 million people potentially has been compromised, much of which may not have come to public attention were it not for the State of California's once-controversial data breach notification law (known as "S.B. 1386"). Several states – including New York and Washington – already have enacted legislation modeled, to varying degrees, on California's statute. Not surprisingly, congressional efforts seem to be following a similar path.

Keep Your Eye On The Bill(s) . . .

There presently are at least 8 "data breach" bills pending in Congress, with a ninth promised for sometime in September. The one to have made the most headway at present is S. 1408, the Identity Theft Protection Act, which cleared the Senate Committee on Commerce, Science and Transportation just before Congress's August recess. The bill enjoys broad bipartisan sponsorship, including both the present and immediate past chairs of the Commerce Committee – Sens. Ted Stevens (R-AK) and John McCain (R-AZ) – and the committee's ranking Democrat, Daniel Inouye of Hawaii, among others.

The bill still faces a tough road ahead, however, for both jurisdictional and substantive reasons. Sen. Richard Shelby (R-AL), chair of the Senate Banking Committee, publicly has voiced his determination that his committee exercise jurisdiction in this area and has introduced his own legislation as a "place-holder" for that purpose. Similarly, Sens. Arlen Specter (R-PA) and Pat Leahy (D-VT), chair and ranking member, respectively, of the Senate Judiciary Committee, have introduced legislation on the subject.

In the House, jurisdictional struggles between dueling committees also appear to be developing, with an effort underway in the House Financial Services Committee to combine two competing bills, and a separate bill expected to be introduced by the leadership of the House Energy & Commerce Committee.

Key Features of The Legislation

The various bills differ somewhat in their particulars, but the principal measures share certain key elements:

- They all impose some form of data protection requirement for personal information, although some confine that obligation to electronic data, and others apply it to data whatever the form.
- They all require notice in the event of security breaches, although the standard for when the notice requirement is triggered varies significantly.
- They all impose some sort of "mitigation" requirement to limit the harm caused by breaches, although the nature of the required mitigation varies.
- They all include some form of preemption of state and local law, although, again, the breadth of that preemption differs.

Looking At One Of The Bills

S. 1408, the Senate Commerce Committee vehicle, in part because it is the only bill to have emerged through the committee process to date, offers a useful prism through which to examine the nature and impact of these bills' provisions and their key points of difference.

Scope

S. 1408 would apply to any non-governmental person or entity that "acquires, maintains or utilizes sensitive personal information," in whatever form and for whatever purpose. "Sensitive personal information" includes the combination of a name, address or telephone number with either a social security number, financial account information, driver's license information or other information that the Federal Trade Commission ("FTC") may designate. Information lawfully obtained from a public record is not included. This definition largely tracks that of the California law and is substantially similar to that in most of the other principal

legislation. (Interestingly, one bill – the measure introduced by Sens. Specter and Leahy – attempts to encompass some additional types of data, including biometric and electronic identifiers.)

As is true of most of the other bills as well, businesses in compliance with the data security and notification requirements issued pursuant to the Gramm-Leach-Bliley Act, which covers regulated financial institutions, are exempt from the bill's requirements.

Data Security Program

Covered entities are required to establish and to implement a written security program to protect sensitive personal information that incorporates administrative, technical and physical components. This is a universal feature of all of the primary bills in this area, although some confine their scope solely to electronic data.

S. 1408 preserves the federal government's neutral approach to technologies, expressly forbidding the FTC from issuing any regulations "that require or impose a specific technology, product, technological standards, or solution."

Notification of Data Security Breach

The Commerce Committee bill requires notice to a consumer of any "unauthorized access to and acquisition of" that consumer's sensitive personal information "in the most expedient manner practicable, but not later than 45 days after" discovery of the breach, if the holder determines that the breach of security creates a reasonable risk of identity theft.

- "Reasonable risk of identity theft" would mean that the "preponderance of the evidence available to the covered entity that has experienced a breach of security establishes that identity theft for 1 or more individuals from the breach of security is foreseeable."

- For any security breach involving more than 1,000 consumers, notice to the FTC or other appropriate federal regulator and to all consumer reporting agencies would be required before notice to the affected consumers. The FTC would be required to post the report on its website.

- For any security breach involving fewer than 1,000 consumers that does not create a reasonable risk of identity theft, report to the FTC or other regulator nevertheless would be required. The agency would not be permitted to disclose news of the breach.

It is perhaps in this respect that the various bills differ most significantly. For example, the Personal Data Privacy and Security Act, introduced by Sens. Specter, Leahy and Feingold, would require notice to any U.S. resident (not only "consumers"), whenever sensitive personal information was subject to the breach. No "risk" analysis is permitted.

Consumer Credit Security Freeze

S. 1408 would require consumer credit reporting agencies to honor a consumer request for a "security freeze" on the consumer's credit report. The freeze would prohibit the reporting agency from disclosing any information on the report to a third party without express authorization from the consumer.

Other bills require free file monitoring for consumers who receive notice of a breach, free credit reports more often than is already required under federal law and similar measures.

Restrictions on Social Security Numbers

S. 1408 would generally prohibit a business, school or other entity from requesting, with limited exceptions, an individual's person's social security number unless there is no other identifier that could be used. It also would prohibit the use of social security numbers on any form of identification, including state driver's licenses.

Other Senate measures have suggested similar restrictions, but no legislation in the House introduced to date has addressed this issue.

Preemption

A key feature of most of the pending bills is the degree to which they would preempt state and local legislation. Businesses concerned over the passage of the California law have grown progressively more alarmed in recent months as state after state becomes poised to enact similar legislation. The specter of compliance with a welter of inconsistent state mandates has fostered a grudging acceptance of – and even preference for – federal intervention.

S. 1408 would preempt any state or local law that requires a covered entity to maintain an information security program or to provide notice to consumers in the event of breach, or that imposes liability for failure to comply with either of those requirements. It also preempts any state or local requirement on a consumer reporting agency to comply with a consumer request for a security freeze and any limitation on the sale, use or disclosure of social security numbers.

Enforcement

S. 1408, like virtually all of the other bills, does not provide for a private right of action under its provisions. Courts typically are reluctant to infer private rights of action in statutes that do not expressly permit them. However, to avoid any uncertainty, S. 1408 includes an express prohibition to that effect. It also would allow state attorneys general to institute suit only in federal court and only if premised on S. 1408. The relevant federal financial regulators would possess exclusive authority over financial institutions subject to GLB, while the FTC would hold enforcement authority for other entities. Other bills are similar, although with some variation particularly with

respect to state attorney-general enforcement.

S. 1408 also provides that failure to notify or report a breach when required would subject the covered entity to fines of up to $11,000 per individual consumer whose information was affected by the security breach, with a cap of $11 million per breach. Here, the individual bills vary widely, but all attempt to provide "teeth" to their provisions.

Devil In The Details . . .

The broad outlines of any eventual federal legislation are fairly clear, but, as is usually the case with legislation on any subject, the struggles will take place over the details. Whether Congress is able to surmount those hurdles and produce legislation this fall is uncertain, but the increasing public pressure on this issue and the steady drumbeat of disclosures triggered by California's (and now other states') laws make eventual action seemingly inevitable.

Paul Hastings' Privacy and Information Security Practice advises clients on all aspects of privacy and information security law and regulation, conducts privacy assessments, formulates and helps establish privacy and security compliance programs, and represents clients facing privacy enforcement investigations or litigation. We also represent clients in working with Congress and the Federal regulatory agencies in the formulation and implementation of public policy in this dynamic and important area.

** Behnam Dayanim is a partner and Vance Schuemann is a government affairs policy advisor in Paul Hastings' Washington, DC, office.*

For more information on the subject of this Alert or on any other privacy or information-security related topic, please contact:

John J. Altorelli (212) 318-6607
johnaltorelli@paulhastings.com

Behnam Dayanim (202) 551-1737
bdayanim@paulhastings.com

Michael Lindsey (213) 683-6262
michaellindsey@paulhastings.com

Robert L. Sherman (212) 318-6037
robertsherman@paulhastings.com