Data Security Law in 2011: Responding to a Breach and Security Considerations for Engaging Vendors

By: Reed Freeman, Partner, Morrison & Foerster, LLP

Inevitably, every company must address a potential or actual security breach incident.

Practical Aspects of Responding to a Breach Incident

To date, 46 states, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, have enacted data security breach notification laws. These laws are not uniform and vary significantly in terms of their scope, notice triggers, notice contents, and other requirements. For example, the California law (upon which many state breach laws appear to have been modeled) generally requires any person conducting business in California that owns or licenses computerized data that includes "personal information" to notify the individuals to whom that data relates about any breach in which "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

Inevitably, every company must address a potential or actual security breach incident. Accordingly, a crucial element of a company's overall data security program is a process to detect and investigate possible incidents, secure data systems if an incident has, in fact, occurred, and take steps to respond in an appropriate manner as quickly as possible.

Even before an incident occurs, a company must have in place an effective mechanism for it to receive notice of potential incidents in a timely fashion. This should consist of both internal and external reporting systems (e.g., a toll-free hotline or security e-mail address) to receive notice promptly from its employees, service providers, customers, and/or third parties. This is only the first step, though. Having a reporting mechanism is not enough unless reports of potential incidents are actually and promptly provided to the response team and/or other decision makers.

Once an incident has been reported, an incident response plan can guide a company in responding in a timely manner to a data security incident by providing a framework for its response, including, importantly, assembling a team comprised of relevant personnel and creating and issuing any legally required notifications. The importance of a plan cannot be overstated. When a company has a well thought-out plan with appropriately delegated roles, the response to the incident will be more coordinated, more timely, and, ultimately, more effective. Moreover, updating a plan, if necessary, after experiencing an incident further strengthens a company's ability to fulfill its responsibilities under the various security breach laws and otherwise respond to the breach in a suitable manner.

In its initial response to any particular incident, a company should take four basic steps (to the extent each is applicable):

- It should investigate a suspected data security incident to determine the relevant facts and circumstances. Specifically, to determine the scope of the breach and its appropriate response, a company must ask, "who, what, where, when, why, and how?"
- In addition, a company should take steps to stop the breach if it is ongoing and/or to recover the compromised data. For example, if a laptop was accidentally left in a taxi, a company should take reasonable steps to recover it. If a company discovers that a web server has been infected with malicious code that provides third parties with unauthorized access to its data, it should take steps to remove the code and prevent further unauthorized access.

- A company should determine the form and type of data potentially compromised. For instance, it should ascertain whether an incident involved paper or electronic records, the type of data involved (e.g., employee and/or customer data), and the specific categories of personal data compromised (e.g., name, Social Security number, credit card number).
- If an incident involves the types of personal data covered under state security breach laws (e.g., name plus Social Security number, driver's license number, financial account number, or medical or health information), the company must determine the potential number of individuals to whom the information related and where they reside. If, in fact, an applicable state's law would require notice to an affected individual, the company must, of course, also attempt to determine the identities of the affected individuals.

These basic steps are also core elements of a response program. Beyond these steps, the specific circumstances of an incident will dictate any additional steps that may be legally required, including, for example, any required notification to a state authority or nationwide consumer reporting agency. Moreover, the laws themselves do not dictate the only necessary or desirable responses to a data security incident. For example, depending on the facts of a particular incident, a company may need to consider employee-related issues (e.g., training or discipline), public relation issues, contractual issues (e.g., if a service provider is responsible for the breach), and whether it may face liability to the issuers of any payment cards involved in the breach.

After its investigation, the company must determine whether any state security breach law applies – that is, whether the incident would be considered a "breach of security" within the meaning of the potentially applicable laws. If so, it must further determine, among other things, if it has a duty to provide notice to:

- the individuals whose personal data was compromised (and, if so, what the notice must say and when it must be provided);
- state authorities;
- consumer reporting agencies; and/or
- another company on whose behalf the company may have been maintaining the compromised data.

In certain instances, a company's contractual obligations may dictate one or more responses to an incident, including, for example, the obligation frequently imposed on service providers (outside of the state laws) to promptly notify their principals of data security incidents.

Considerations for Vendor Relationships

Companies have been plagued by data security breaches that have occurred at their vendors. In light of this very real threat, a company should take steps to ensure that its data will be adequately secured by vendors. In particular, it should select vendors that have appropriate security in place for the data they will process, contractually require them to maintain sufficient data safeguards, and periodically assess whether the vendors are actually safeguarding the company's data consistent with their contractual obligations. Because there is no one-size-fits-all solution to vendor relationships and contracts, a company should take a risk-based approach to the steps outlined above. A prudent approach is one based on the sensitivity and quantity of the data that the vendor will process, as well as on the risks associated with how the vendor will handle the company's data (e.g., if it will operate a web server or process credit card transactions).

> When a company has a well thought-out plan with appropriately delegated roles, the response to the incident will be more coordinated, more timely, and, ultimately, more effective.

The following basic provisions make sense for most vendor contracts:

- A requirement that the vendor maintain a written security program that covers the company's data;
- A limitation that the vendor use the company's data solely for the purpose of providing the services;
- A prohibition on the disclosure of the company's data to third parties (including vendor affiliates);
- Requirements to promptly notify the company of any potential security incidents involving company data and to cooperate with the company in addressing the incident;
- A requirement that the vendor comply with applicable data security laws;
- A requirement that the vendor return or appropriately destroy company data at the end of the contract;
- Company audit rights; and
- An indemnification (or other risk allocation provision) related to vendor security and compliance with these requirements.

Data Leakage and Referring Headers

A referring header is a type of HTTP header that identifies, among other things, the URL of the Internet resource which links to it. Web servers frequently log all traffic to a website and record the referring header sent by the web browser for each request to visit that site, so the referring header allows a company to identify the web page that referred a visitor (i.e., the source of the link to the web page, often the URL of the previous web page visited by the user). Not surprisingly, a referring header can contain personal or sensitive information, and, as a result, it presents a new and unique potential security risk to companies that collect such information.

The potential risks have recently been publicized and are even being litigated. In October 2010, The Wall Street Journal reported that many popular Facebook applications (apps) allegedly passed users' Facebook IDs to online advertisers in referring headers. One app maker has been hit with a class action relating to this. The class is potentially huge, as the game has more than 50 million consumers. The complaint alleges that the defendants violated federal and state laws related to unlawful interception and access of data. It also claims unfair competition, breach of contract, and breach of privacy for allegedly violating Facebook's privacy policy and App Developer Agreements.

In light of this very real threat, a company should take steps to ensure that its data will be adequately secured by vendors.

To learn more about data breach resolution, visit **www.experian.com/databreach**, or contact Experian® at **databreachinfo@experian.com** or **1 866 751 1323**.