Banking & Financial Services Alert

Published by Bradley Arant Boult Cummings LLP

Data Security Breaches – State Notification Rules in Transition

By Elena A. Lovoy

Privacy issues remain a constant and complicated concern for most financial services companies. A recent Wall Street Journal article focused on the increasing use of privacy impact assessments to identify issues and minimize liability before the launch of new products or services. High profile data security breaches also seem to be a staple in the daily headlines. 2011 is on track to be the worst year in a decade for security breaches.

The risk of a data security breach at your business or at a third party vendor is always present even with the best risk management program and state of the art security procedures in place. A comprehensive privacy compliance program should include a security breach incident response plan that, among other things, addresses the delivery of notifications to customers impacted by the breach and imposes specific breach response requirements on vendors that maintain or store customer data for your business.

State laws requiring businesses to notify their customers of data security breaches have been on the books for several years. As security breach notifications have become common, the content of the notifications have also become generic. To provide more substantive information to consumers impacted by security breaches, some states are beginning to impose additional requirements for the content of these notifications. California and Illinois have recently followed this trend.

California

On August 31, 2011, Governor Brown signed into law a bill amending section 1798.82 of the California Civil Code to require businesses to include certain specific information in data security breach notifications provided to California residents. California law currently requires any person or business, including financial institutions, conducting business in the state that owns or licenses computerized data to notify residents when there has been a breach of the security of unencrypted personal information. The law does not specify the type of information that should be included in the notification. This will change effective January 1, 2012.

New Content Requirements

Under the new requirements, any security breach notification to California residents must be written in plain language. The notification must also, at a minimum, include the following disclosures:

(1) The name and contact information of the reporting person or business;
(2) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
(3) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred;
(4) The date of the notice;
(5) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

November 29, 2011

Author

Elena A. Lovoy
205.521.8746
elovoy@babc.com

Related Attorneys

Paige M. Boshell
205.521.8639
pboshell@babc.com

Paul Compton
205.521.8381
pcompton@babc.com

Lesley Smith DeRamus
205.521.8642
lderamus@babc.com

Dave Dresher
205.521.8605
ddresher@babc.com

Charles S. Sanger
615.252.2331
csanger@babc.com

Laurence D. Vinson, Jr.
205.521.8607
lvinson@babc.com

Paul Ware
205.521.8624
pware@babc.com

Ken Wyatt
205.521.8604
kwyatt@babc.com

(6) A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
(7) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security, driver's license or California identification card number.

At the discretion of the person or business, the notification may also include the following:

(1) Information about what the business has done to protect individuals whose information has been breached.
(2) Advice regarding the protective measures available to the person whose information has been breached.

Companies conducting business in California will need to ensure that their breach notification forms incorporate these required disclosures. These new disclosure requirements will also add a layer of complexity to multistate notification programs. Some companies may opt to include the California disclosures in all notifications.

Notification to Attorney General's Office

The new law will also require businesses to electronically submit a sample copy of their security breach notification to the California Attorney General's Office. This filing is required when a notification is being sent to more than 500 California residents as a result of a single breach of a security system. The sample copy should not include any personally identifiable information. Although the Attorney General's Office will become a repository of these notification forms, there is no requirement under the new law for the Attorney General's Office to take any action upon submission of a notification.

Illinois

On August 22, 2011, Governor Quinn approved a bill amending the Illinois Personal Information Protection Act ("PIPA") to prescribe certain disclosures that must be included in any notice of breach sent to Illinois residents. These new requirements will be effective January 1, 2012.

The requirements under PIPA apply to any "data collector," including financial institutions. There is no exemption under PIPA for institutions otherwise subject to any federal privacy law. PIPA currently requires any business that owns or licenses nonpublic personal information concerning an Illinois resident to notify the resident when there has been a breach of the security of the system data. Although PIPA requires the notification to be made in the most expedient time possible and without unreasonable delay after discovery of the breach, PIPA did not prescribe any content requirements for such notifications. The recent amendments have added new content requirements for this notification.

New Content Requirements

Under the new requirements, the notification to an Illinois resident must include, but need not be limited to, the following:

(1) The toll-free telephone numbers and addresses for consumer reporting agencies.
(2) The toll-free telephone number, address and website address for the Federal Trade Commission.
(3) A statement that the individual can obtain information from these sources about fraud alerts and security freezes.

The notification may not include information concerning the number of Illinois residents affected by the breach.

Businesses with customers in Illinois will need to ensure that their notification forms include the required disclosures. Businesses that experience a multistate breach impacting customers in California and Illinois may wish to incorporate the disclosures required in both states into a single notification form.

Vendor Cooperation

Although the new Illinois requirements do not provide for notification to the Attorney General's Office, Illinois joins a handful of states mandating cooperation between the owner or licensee of data and third party vendors in connection with breaches of personal information in the vendor's care. Since many breaches occur at vendors, businesses must continue to monitor the privacy and data security compliance programs at their vendors. This includes requiring vendors to cooperate in breach investigations to ensure that notifications to affected customers can be sent out as timely as possible.

PIPA requires any vendor that maintains or stores, but does not own or license, computerized data that includes personal information to notify the owner or licensee of the information of any breach of the security of the data. This notification must be provided immediately following discovery of the breach, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The new requirements mandate that the vendor also cooperate with the owner or licensee in matters relating to the breach. This cooperation must include, but need not be limited to, the following:

(1) Informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and
(2) Informing the owner or licensee of any steps the vendor has taken or plans to take relating to the breach.

A vendor will not be required to disclose confidential business information or trade secrets as part of its cooperation with the owner or licensee. Furthermore, a vendor will not be required to notify any Illinois resident who may have been impacted by the breach. This obligation remains with the owner or licensee of the personal information.

A robust privacy and data security compliance program should include a formal security breach incident response plan that will assist a company in meeting its notification obligations in those states in which the company has a customer footprint. The recent changes in California and Illinois may lead other states to amend their security breach notification laws to impose similar or more onerous requirements. For businesses with customers in one or both of these states, the new security breach notification obligations only further complicate the privacy compliance landscape.

There are a number of bills currently pending in the U.S. Congress addressing privacy and data security issues. A number of these bills would, among other things, preempt the patchwork of multistate breach notification laws and prescribe uniform content requirements for breach notification letters. It is unclear whether the House and Senate can resolve all of these various proposals into a single piece of legislation that can move forward in light of other competing issues, such as the overall economy and the impending election season. Although there seems to be interest in carving out a national security breach notification standard from these various proposals, time will tell whether Congress will tackle this narrow issue.

This alert is a brief summary of recent developments addressing the content of security breach notifications. Other federal and state privacy developments are not addressed in this alert.

If you have any questions regarding security breach notifications or other privacy compliance issues, please contact Elena A. Lovoy, Paige M. Boshell, or one of the other attorneys in the Banking and Financial Services Practice Group at Bradley Arant Boult Cummings LLP.

BRADLEY ARANT BOULT CUMMINGS LLP OFFICE LOCATIONS:

ALABAMA
One Federal Place
1819 Fifth Avenue North
Birmingham, AL 35203-2119
205.521.8000

200 Clinton Avenue West, Suite 900
Huntsville, AL 35801-4900
256.517.5100

Alabama Center for Commerce
401 Adams Avenue, Suite 780
Montgomery, AL 36104
334.956.7700

MISSISSIPPI
188 E. Capitol Street, Suite 400
Jackson, MS 39201
601.948.8000

NORTH CAROLINA
100 North Tryon Street, Suite 2690
Charlotte, NC 28202
704.332.8842

TENNESSEE
1600 Division Street, Suite 700
Nashville, TN 37203
615.244.2582

WASHINGTON, DC
1615 L Street, N.W.
Suite 1350
Washington, DC 20036
202.393.7150