Disclosure Requirements Under California's Breach Notification Law

Tom Clark, Counsel
Assembly Judiciary Committee

Prepared for the Hearing of the Assembly Judiciary Committee
November 19, 2008
10:00 am – Noon
California State Capitol Building
Room 4202

Introduction: The Purpose of This Hearing:

On August 5, 2008, United States Attorney General Michael Mukasey announced that federal prosecutors had brought indictments against an international ring of computer hackers who allegedly accessed more than 40 million debit and credit card numbers from at least nine American retailers. Attorney General Mukasey claimed that, "So far as we know, this is the single largest and most complex identity theft case ever charged in this country."[1] Although this breach may have been unusual in its international reach, it is but one of hundreds of recent examples of instances where people's sensitive personal information – including social security numbers and credit and debit card numbers – have fallen into the hands of identity thieves.[2]

Of particular interest to this Committee were the disparate responses taken by the nine retailers that were targeted by the computer hackers. According to an investigation conducted by the *Wall Street Journal*, only four of the nine companies took steps to inform affected customers about the breach. Two of the nine companies claimed that they did not inform customers because they could not "confirm" that a breach had occurred, despite that fact that federal prosecutors had uncovered enough evidence to bring indictments. The remaining three companies would not say whether or not they disclosed the breach to anyone, but the *Journal's* search of SEC filings, company web sites, and press releases turned up no evidence that any disclosures had been made.[3]

---

[1] U.S. Department of Justice, "Remarks Prepared for Delivery by Attorney General Michael B. Mukasey at the Identity Theft Press Conference, August 5, 2008," available at http://www.usdoj.gov.ag/speeches/2008/ag-speech-0808057.html.)

[2] The Privacy Rights Clearinghouse maintains a regularly updated list of major data breaches. Available at http://www.privacyrights.org/ar/ChronDataBreaches.htm

[3] *Wall Street Journal*, August 11, 2008. The companies that disclosed the breach were the TJX Companies, BJ's Wholesale Club, Inc. shoe retailer DSW, Inc., and Dave and Buster's Inc. The companies that failed to disclose because they could not confirm that a breach had occurred were Boston Market Corporation and Forever 21, Inc. The three companies that would not say whether or not they disclosed the breach were Office Max, Inc,, Barnes and Noble, Inc., and Sports Authority, Inc.

That the nine companies apparently perceived their duty to disclose the breach differently raises troubling questions about the applicability of data breach notification laws in California and at least 40 other states.

The purpose of this hearing is threefold: First, the Committee wishes to ascertain how companies that collect the personal information of Californians in the course of doing business understand their obligation to provide notice in the event of a data breach. Second, the Committee wishes to explore recommended "best practices" on providing notice of data breaches, including the recommended practices of the California Office of Privacy Protection.[4] Third, the Committee wishes to consider what changes, if any, may be needed in existing law in order to enhance consumer protection and facilitate effective enforcement of the law.

Existing Law: California's Breach Notification Law

With the enactment of AB 1386 in 2002, (Chapter 915, Stats of 2002), California adopted the nation's first data breach notification law. Since that time, at least 40 other states have followed suit, often tracking the exact language of the California law.[5] California's notification requirements apply to any person, state agency, or business that owns, licenses, or maintains computerized data that contains the unencrypted personal information of a California resident.[6]

Under California law, any person, agency, or business that "owns or licenses" computerized personal information must notify any person whose unencrypted data is accessed by any unauthorized person or entity. The obligation to notify is triggered whenever a breach occurs, or is "reasonably believed" to have occurred.[7] Any business or entity that "maintains" computerized personal information must notify the owner or licensee of the information in the event of a breach.[8] Generally, a business that "owns or licenses" personal information, such as debit and credit card numbers, would include the financial institution that issued the card. A business that "maintains" this personal information would include a retail establishment that accepts debit or credit cards as means of payment and keeps that information on record for some period of time.

---

[4] California. Office of Privacy Protection. *Recommended Practices on Notice of Security Breach Involving Personal Information*, Rev. May of 2008.

[5] According to data compiled by the National Conference of State Legislatures, as of November 4, 2008, 44 states had adopted data breach notifications laws. See http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

[6] Civil Code Section 1798.29 applies to state agencies that own, license, or maintain computerized personal information. Civil Code Section 1798.82 applies to persons or businesses that own, license, or maintain computerized personal information.

[7] Civil Code Sections 1798.29(a) and 1798.82(a).

[8] Civil Code Sections 1798.29(b) and 1798.82(b).

The purpose of California's breach notification law is to provide consumers with useful information in a timely manner, so that they may take necessary steps in order to protect themselves from identity theft. [9] For example, they can cancel the compromised credit or debit card accounts, place a "fraud alert" or "security freeze" on their credit report, obtain a free credit report from one of the major credit reporting agencies, and more closely monitor their debit and credit card statements. Although existing law requires that notices be sent to affected persons in the most effective and expeditious manner as is reasonable, existing law says very little about the required contents of such notices. Recent efforts to amend existing law so as to ensure that notices be written in clear language and provide useful information to the consumer have led to vetoes by the Governor.[10]

Recommended Practices of the California Office of Privacy Protection

The California Office of Privacy Protection recommends "best practices" for businesses and other organizations so that they might manage personal information "in ways that promote and protect individual privacy interests."[11] As part of this charge, the OPP publishes a pamphlet on recommended practices for compliance with data breach notification laws. These practices are not mandatory, but merely offered as guidelines to assist businesses and organizations "in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care."[12]

The OPP outlines several recommended practices, broken down into three parts: (1) Protection and Prevention; (2) Preparation for Notification; and (3) Notification. (See attached.) In addition to recommending specific actions, the OPP more generally recommends that businesses develop written policies and procedures, designate one individual to be in charge of implementing these policies and procedures, and to regularly train employees on their roles and responsibilities under these policies and procedures.

One of the purposes of this hearing is to ascertain the extent to which businesses that own, license, or maintain the personal information of California residents have adopted any or all of these recommended practices.

Unanswered Questions in Light of Recent Data Breaches

In light of the large number of recent data breaches, it is appropriate for the Committee to inquire into how businesses understand their obligations under California law. As noted

---

[9] Senate Floor Analysis of AB 1386, August 27, 2002, available at www.leginfo.ca.gov

[10] In the last two years, the following bills have attempted to amend the breach notification law, in part, by specifying the content of the breach notice: AB 779 (Jones, 2007), AB 1656 (Jones, 2008), and SB 364 (Simitian, 2008). All of these bill were passed by both houses of the Legislature and enrolled, but were vetoed by the Governor.

[11] Office of Privacy Protection, *supra* n. 4, at 6.

[12] Id at 8.

above, in the case of the international hacking ring that brought federal indictments, it appears likely that only four of the nine affected businesses notified customers. To be sure, at least one of these companies (BJ's Wholesale Club) does not operate in California, and the breach of Boston Market affected only a single outlet in Florida. Nonetheless, among the other retailers, all of which have multiple outlets in California, it is reasonable to assume that some portion of the 40 million stolen debit and credit numbers belonged to residents of California and, therefore, should have triggered the notification requirement. As such, the Committee may wish to consider some of the following questions:

- When is a business required to provide notification? In the breach that brought the recent federal indictments, two of the companies reported that they did not disclose the breach because they could not "confirm" the breach. However, California law requires that notice be provided whenever a breach occurs or is "reasonably believed" to have occurred. Presumably, a "reasonably believed" standard would not require a "confirmation" that a breach had occurred. The Committee may wish to inquire as to how businesses that collect the personal information would make this determination.

- What amount of evidence is needed to create a "reasonable" belief that a breach has occurred? Would a federal indictment alleging that hackers had targeted that business constitute per se a reasonable belief that a breach had occurred?

- To whom should a business send notice? Existing law requires a business that "owns or licenses" personal data to notify the affected person. A business that "maintains" the data must notify the owner or licensee of the data. A rationale for this distinction is that the retailer who "maintains" a debit or credit card number may not always have the holder's name and address. Therefore, it is incumbent upon the retailer to notify the financial institution that issued the card and presumably has access to this information. However, the Committee may wish to consider whether this is always the most effective means of notification. For example, in cases where the retailer also maintains the name and address of the cardholder, should the retailer notify the customer directly? For example, not all states make the same distinction that California does. Under Florida law, for example, any business that "maintains" computerized personal information must disclose the breach directly to the customer, not merely to the owner or licensee of the data.[13]

- Is the distinction between "owing and licensing" data versus "maintaining" data sufficiently clear to permit businesses to fully understand their notification obligation and to *whom* they must give notice?

- Should businesses be required to notify specified law enforcement agencies? Existing law requires businesses to provide notice of a breach in the most

[13] See Fla. Stat. Section 817.5681.

expedient time possible and without unreasonable delay. Although the statute does not specify an exact time frame, the California Office of Privacy Protection recommends that this be done within 10 business days after learning about the breach. Existing law, however, provides that the notification obligation may be delayed if it will impede a criminal investigation. Yet, nothing in the statute *expressly* requires the business to notify law enforcement agencies in the first place, although the OPP includes such notification as part of its recommended practices and such a requirement may be implicit in the statute. The Committee may wish to consider whether the existing law should be amended to clearly require notification of law enforcement agencies. Not only would this ensure that a criminal investigation will not be impeded, but just as importantly it would prompt law enforcement to initiate such an investigation and allow law enforcement to better track data breaches that affect California residents. In addition, the Committee may wish to consider *which* law enforcement agencies must be notified.

- In order to better serve the original purpose of the breach notification statute, should the notice contain specified information? An important rationale behind AB 1386 was that timely notice would allow the affected person to take certain precautionary steps to decrease the likelihood that his or her information would be used to commit identity theft. However, some of these steps – such as placing a security freeze on one's credit report – are costly, time-consuming, and block access to credit reports for both legitimate and illegitimate purposes. Therefore, the consumer should be fully apprised of all of the circumstances surrounding the breach in order to better weigh his or her options. Thus, the Committee may wish to consider what kinds of information should be included in breach notices, whether they are sent by the owner of licensee of the compromised data.

- Have Businesses in California Adopted the Recommended Practices of the Office of Privacy Protection? Although the OPP recommendations are, by definition, not mandatory, it is not clear how many companies have adopted the OPP guidelines. For example, how many businesses have a "written policy" on the proper procedures to follow in the event of a data breach or suspected data breach? Do they promote awareness of these policies through ongoing employee training and communications? Do they designate one individual as responsible for implementing data breach notification policies? Have they identified the appropriate law enforcement agency to notify in the event of a data breach?

Conclusion:

There is, as of yet, no case law defining what constitutes compliance with California's breach notification statute. For example, would a company that elected not to send notices because it could not "confirm" that a breach had occurred be in violation of California law? On the one hand, the trigger for the notice requirement should not be so low as to alarm consumers when there is limited risk of identity theft or credit or debit

card fraud. Nor should consumers be so inundated breach notices that they simply begin to ignore them. On the other hand, requiring a company to "confirm" that a breach has occurred might be an unreasonably high standard that leaves consumers unaware of a considerable risk of identity theft or other adverse consequences.

Most importantly, as noted by the Privacy Rights Clearinghouse, "companies must have both an *understanding and a plan* about what to do if personal data in its possession is compromised."[14] The purpose of this hearing to ascertain whether companies that possess personal data have an understanding of their obligations under existing law and have adopted written policies and procedures for meeting those obligations.

[14] Privacy Rights Clearinghouse, "Is Your Client Prepared To Comply with Data Security Breach Notification Laws?" November 11, 2007.[Emphasis added.] Available at http://www.privacyrights.org/notification_laws.htm.