

California S.B. 1386
First Published in the CSI July 2003 Alert
Written May 30, 2003
Rebecca Herold, CISSP, CISM, CISA, FLMI

The FTC reports more than 750,000 cases of identity theft occurred in the United States last year; a 2000% increase since the early 1990's. Various consumer advocacy groups estimate banks lost around \$90 million last year from identity theft incidents, and that the number of incidents is going to continue to grow.

According to the FTC's ID Theft Data Clearinghouse, the most common types of identity theft are:

- Using or opening a credit card account fraudulently
- Opening telecommunications or utility accounts fraudulently
- Passing bad checks or opening a new bank account
- Putting loans in another person's name
- Working in another person's name

California now has a new law intended to address the identity theft epidemic that you need to discuss with your lawyers if your organization has California customers. An amendment went into effect on July 1st to the California Civil Code that requires companies to notify their California customers when certain types of privacy and security breaches and incidents occur.

S.B. 1386 was passed a few months following an April 2002 computer intrusion into California's Teale Data Center. The breach into the California state payroll system, of which administrators reportedly were aware for more than two weeks before informing possibly more than 250,000 affected state workers, included potential access to employee Social Security Numbers. According to various news reports, the data center's officials stated they did not believe information was removed, but they were not certain.

Overview of S.B. 1386

Bill S.B. 1386 was signed into law by Governor Gray Davis on September 25, 2002 and filed with the California Secretary of State the next day. The law became operative on July 1, 2003. The full text is at: http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

This personal information privacy law requires any organization (state agency, person or business) conducting business in California and processing personal information for California residents to disclose any information security breach to California residents whose unencrypted personal information was obtained by an unauthorized person. Notifications can be delayed if law enforcement determines it could hinder a criminal investigation. S.B. 1386 will preempt all local regulation of this issue. The primary requirements, as listed within the regulatory text, will require:

“(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident

California S.B. 1386

First Published in the CSI July 2003 Alert

Written May 30, 2003

Rebecca Herold, CISSP, CISM, CISA, FLMI

of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation."

What is "personal information"?

"Personal information" includes a person's first name or first initial and last name in combination with any one of the following when at least one of the pieces of information is not encrypted:

- Social security number
- Driver's license number or California Identification Card number
- Account number, credit or debit card number, in combination with any required security code, access code, or password that allows access to a financial account

Personal information does not include information that is publicly and lawfully available from federal, state, or local government sources.

What constitutes a "breach of the system"?

A "breach of the security of the system" is unauthorized "acquisition" of personal information resulting from a security compromise in the organization's computer systems. It is not considered a breach when the organization's personnel access personal information to perform business activities as long as the information is not subjected to unauthorized disclosure.

How must individuals be given "notice"?

Individuals may be given "notice" using one of the following methods:

- Written notice
- Electronic notice, if the notice consistent with U.S.C. Title 15 Section 7001 requirements for electronic records and electronic signatures.
- Substitute notice when the cost of providing notice would exceed \$250,000, or the number of persons to be notified exceeds 500,000, or the organization does not have sufficient contact information. Substitute notice consists of **all** of the following:
 - E-mail notice (using available email addresses)

California S.B. 1386

First Published in the CSI July 2003 Alert

Written May 30, 2003

Rebecca Herold, CISSP, CISM, CISA, FLMI

- Clearly posting the notice on the organization's Web site (if one exists)
- Notification to major statewide media

How can agencies, businesses and persons be in compliance?

The regulatory text indicates that organizations that maintain notification procedures to appropriate individuals as part of their information security policies and are consistent with the timing requirements of this law are generally in compliance with the notification requirements, assuming the policies are consistently followed.

What are the penalties?

Individuals injured as a result of noncompliance with this law can bring civil action to recover damages. Businesses that violate the law can be enjoined (very broadly, be required to abstain from further business, or do a specific act). An important aspect of potential penalties is that they are cumulative to each other and to any the rights and remedies available under other applicable laws.

Identity Theft Laws in Other States

At least 48 other states have laws specifically covering or addressing identity theft. (I could not find any for Vermont or Colorado, or for the District of Columbia.) What sets the new California S.B. 1386 law apart from all these other laws are the requirements being placed upon businesses to report security and privacy breaches that may lead to identity theft.

The Identity Theft and Assumption Deterrence Act of 1998 made it a federal crime for anyone to knowingly transfer or illegally use another person's identification to commit, or to aid or abet, activities that violate Federal law, or that is a felony under any applicable State or local law.

Business Impact of S.B. 1386 and Other Identity Theft Laws

I always have an abundance of questions whenever these new laws are launched. With regard to S.B. 1386 and similar laws, will we be able to start obtaining more accurate security incident statistics as a result? You would think so, if covered organizations comply with the law. Organizations need to be aware of incidents in order to contact customers and applicable individuals. We should see if this is the case next year in the yearly CSI/FBI report...at least with regard to statistics regarding California residents.

Will such laws help justify information security and privacy budgets? This was a common thought when GLB went into effect, and then again when HIPAA became active. However, comments from vendors and practitioners indicate that most companies are still trying to dissect existing information security and privacy budgets to cover these issues because they still have not obtained additional funding. It appears most organizations are taking the stance that, until some other organization has been given a large fine, received a jail sentence, or damaging press, they are not going to invest more money in compliance efforts. This seems to be a risk CIOs, CEOs and COOs are often willing to take.

California S.B. 1386
First Published in the CSI July 2003 Alert
Written May 30, 2003
Rebecca Herold, CISSP, CISM, CISA, FLMI

What about the impact to businesses following incidents? Will organizations always notify applicable individuals following incidents, or only occasionally depending upon the likelihood of the incident being communicated outside their organization? Will companies lose customers they have notified? Or, will customers like the fact that their companies are demonstrating such concern for their privacy and well-being and become more loyal? It probably all depends upon the procedures companies follow after an incident and the way in which communications are made with individuals. Much also depends upon the severity and potential personal impact to the individuals. If they have to subsequently spend weeks and months canceling credit cards and getting new ones issued, changing bank accounts, and repairing credit reports they are likely not to be enraptured, no matter if the organization contacted them quickly enough to mitigate the damage more than if they had not been contacted at all.

Will customers expect organizations to start encrypting all personal information by default? Few people understand or know about encryption, so probably not large numbers...yet. Will there be an increase in the number of encryption solutions implemented within organizations that have California residents? Will this motivate organizations to start using encryption for all personal information so they will not need to notify customers and applicable individuals? Possibly; companies may determine that it is easier, and more desirable from a publicity and procedural point of view, to just go ahead and implement encryption for all personal information instead of trying to figure out how to contact all California residents for security incidents involving disclosure of customer information. The cost of implementing an encryption solution is arguably a large up front investment with comparatively small ongoing maintenance and support costs compared to the ongoing costs of monitoring security incidents, contacting customers and applicable individuals, and addressing potential revenue impact. Perhaps IDS systems implementations will increase dramatically so organizations will not have to implement encryption solutions and also decrease the risk of unauthorized access to personal information. Or, possibly a small percentage of companies will not do any type of security incident monitoring, choosing instead the ignorance is bliss plan.

Will other states start to follow suit and pass similar laws? Possibly; it seems there are always states waiting to introduce new laws based upon the success of similar laws in other states. For instance, look at the large number of proposed anti-spam laws that have proliferated in the past few months.

Will new similar Federal laws be passed? Probably not anytime soon considering the conflicts with the National Strategy to Secure Cyberspace and the protections built in for companies who disclose computer attack information to the government.

How many civil lawsuits will we see in the year following the enactment of the law? Ah, to have a reliable crystal ball! I predict the number will be few during the first 6 to 12

California S.B. 1386

First Published in the CSI July 2003 Alert

Written May 30, 2003

Rebecca Herold, CISSP, CISM, CISA, FLMI

months, but then pick up considerably in number following the inaugural period...along with one or two successful customer or employee litigations.

Will companies start contacting law enforcement more often to avoid or delay contacting their customers? Possibly, but it is unlikely.

The real gray area is what triggers disclosure of security breaches. Each organization needs to decide what constitutes a breach, even in cases where no fraud or identity theft results. Your organization should consider:

- Do you have documented, internally published and well-communicated information security policies?
- Do the information security policies include customer and individual notification requirements?
- Do you have procedures in place to support these policies, in addition to meeting the requirements of S.B. 1386?
- Have you communicated the definition of personal information to your personnel?
- Who is considered to be the owner of the personal information?
- Do you know where all your computerized customer and personal information is located?
- At what points does personal information enter and leave your network?
- Is the act of unauthorized viewing of personal information considered to be acquiring information?
- How will your organization handle necessary customer and individual contacts following security incidents?
- How will your organization handle the accompanying publicity?
- How can you tell if the personal information you are processing is for California residents?

Now the next question is, will this law be effective in stemming the increase in identity theft incidents?

Rebecca Herold, CISSP, CISM, CISA, FLMI is an independent information security, privacy and compliance consultant, author and instructor. She can be reached at rebeccaherold@rebeccaherold.com or 515-491-1564. Rebecca has a B.S. in Math & Computer Science, an M.A. in Computer Science & Education, created "The Privacy Papers," co-authored "The Practical Guide to HIPAA Privacy and Security Compliance," and authored "Managing an Information Security and Privacy Awareness and Training Program" all published by Auerbach.