Data Breach Report 2012

Kamala D. Harris, Attorney General
California Department of Justice

Contents

Message from the Attorney General i

Executive Summary iii

Introduction 1

What the California Law Requires 1

California and Other States 3

Report Methodology 5

Breaches Reported in 2012 7

Breaches by Industry Sector 7

Breaches by Data Type 8

Breaches by Type of Failure 8

Breach Size 10

Other Findings 11

Recommendations 13

Appendix 19

Breach Notification Law 19

Information Security Law 25

Notes 27

Message from the Attorney General

California has the strongest consumer privacy laws in the country. When consumers in California entrust their Social Security numbers, credit card details, medical information, and other personal information to companies and government agencies, they rely on those entities to secure their personal information and protect it from access by unauthorized persons. This is good policy for consumers and for businesses. It is good for consumers because it respects their privacy and reduces the likelihood that they will become victims of identity theft or have their personal information used without their consent. It is also good for businesses because it reduces the likelihood that companies will be defrauded by an identity thief, promotes consumer confidence in industry, and, most importantly, builds consumer trust.

In 2003, California became the first state in the country to require data breach notification. Notifying individuals when their personal information has been put at risk by a breach gives them the opportunity to take defensive action. With prompt notice, people can close imperiled accounts, put a fraud alert or security freeze on their credit records, and take other steps to protect themselves from the consequences of the breach.

The breach notice law has also opened a window on privacy and security practices for researchers and policy makers. In 2012, for the first time, companies and government agencies subject to the California law were required to submit copies of their data breach notices to the Attorney General. Our offices reviewed this information. In this report, we describe what we have seen and provide recommendations based on our findings.

Particularly striking is the impact of the failure to encrypt sensitive personal information. It has been ten years since we realized the vulnerability of personal information on stolen laptops, lost data tapes, and misdirected emails. If encryption had been used, over 1.4 million Californians would not have had their information put at risk in 2012. That number represents more than half of the 2.5 million people affected by the 131 breaches covered in this report. It is my strong recommendation that companies and agencies implement encryption as a basic protection and reasonable security measure to help them meet their obligation to safeguard personal information entrusted to them.

As a society, we increasingly rely upon companies and government agencies to manage and secure our most sensitive records and personal information. I hope that this report will prove helpful to these organizations as they review their privacy and security policies.

Sincerely,

Attorney General Kamala D. Harris

Executive Summary

California's landmark law on data breach notification, which requires businesses and state agencies to notify Californians when their personal information is compromised in a security breach, took effect in 2003. Since then, all but four states have enacted similar laws. In addition, the federal government requires breach notification in the health care sector, and other jurisdictions around the world are considering and enacting such laws. The authors of the California law stated that its intent was to give consumers early warning that they were at risk of identity theft, so they could take defensive action.

Criminals are making use of breached information to commit fraud, with nearly one in four recipients of breach notices in the U.S. becoming identity theft victims, more than four times the rate of the general population in 2012.

The law also opened a window on privacy and security practices for companies, researchers, and policy makers. In 2012, for the first time, those subject to the California law were required to provide copies of their notices to the Attorney General when the breach involved more than 500 Californians. We received reports of 131 breaches in 2012, and we have reviewed the information submitted in order to gain an understanding of the types of breaches that are occurring, what vulnerabilities they may reveal, and what actions might be taken to prevent or reduce the likelihood of future breaches. In this report, we describe what we have seen and offer some recommendations based on our findings.

Key Findings

- In 2012, the Attorney General's Office received reports of 131 data breaches, each affecting more than 500 California residents.
- The average (mean) breach incident involved the information of 22,500 individuals. The median breach size was 2,500 affected individuals, with five breaches of 100,000 or more individuals' personal information.
- More than 2.5 million Californians were put at risk by data breaches in 2012.
- More than 1.4 million Californians would not have been put at risk, and 28 percent of the data breaches would not have required notification, if the data had been encrypted.
- The retail industry reported the most data breaches in 2012: 34 (26 percent of the total reported breaches), followed by finance and insurance with 30 (23 percent).
- More than half of the breaches (56 percent) involved Social Security numbers, which pose the greatest risk of the most serious types of identity theft.

- More than half of the breaches (55 percent) were the result of intentional intrusions by outsiders or by unauthorized insiders. The other 45 percent were largely the result of failures to adopt or carry out appropriate security measures.
- The average reading level of the breach notices submitted in 2012 was 14th grade.

Recommendations

1. **Companies should encrypt digital personal information when moving or sending it out of their secure network. The Attorney General's Office will make it an enforcement priority to investigate breaches involving unencrypted personal information, and encourage our allied law enforcement agencies to similarly prioritize these investigations. The Legislature may also want to consider requiring the use of encryption to protect personal information in transit.**

   Despite the incentive created by the breach notification law's exemption for encrypted data, many companies are still failing to use this effective security measure. Far too many people continue to be put at risk when companies do not encrypt data in transit. More than half of the Californians affected by data breaches reported to the Attorney General in 2012 – fully 1.4 million – would not have been put at risk if the data had been encrypted.

2. **Companies and agencies should review and tighten their security controls on personal information, including training employees and contractors.**

   Computer intrusions, by outsiders and malicious insiders, accounted for over half of the breaches reported to the Attorney General in 2012. Cyber security is a continual and escalating battle, but it is one that must be vigorously waged. Not only must safeguards be constantly reviewed and adapted to meet new threats, but employees and contractors must be provided with regular training in organizational policies and procedures.

3. **Companies and agencies should improve the readability of breach notices.**

   The 14th-grade average reading level of the notices is significantly higher than the U.S. average reading level of eighth grade. The purpose of a breach notice is to alert individuals that they are at risk and give them the opportunity to take protective action. This can only be achieved if the recipients understand the notices.

4. **Companies and agencies should offer mitigation products or provide information on security freezes to victims of breaches involving Social Security numbers or driver's license numbers.**

   Breaches that compromise Social Security or driver's license numbers expose victims to the risk of one of the most serious types of identity theft, new account fraud. The

latest research indicates that this type of identity theft is increasing. When a thief uses the information to open new accounts, victims generally do not learn about it for many months, often when the account has been sent to collection. The work of clearing up new account identity theft can take hundreds of hours and cost thousands of dollars. Protective measures that can limit the victim's risk in this type of breach include credit monitoring services and a security freeze. Yet in 29 percent of the breaches of this type, no credit monitoring or other mitigation product was offered to victims.

5. **Legislation should be considered to amend the breach notification law to require notification of breaches of online credentials, such as user name and password.**

   As consumers and businesses have moved online, identity thieves have followed. Passwords and user names are the latest target of hackers, as evidenced by recent incidents at Yahoo, the *New York Times*, and Twitter. Because people often do not use unique passwords for each of their online accounts, a thief who has stolen one set of credentials can get access to many accounts. With timely notice, individuals can protect themselves by changing their passwords.

Introduction

California's landmark law on data breach notification took effect in 2003. Since then, all but four states have enacted similar laws,[1] the federal government requires breach notification in the health care sector, and other jurisdictions around the world are considering and enacting such laws. The authors of the California law stated that its intent was to give consumers early warning that they were at risk of identity theft, so they could take defensive action.[2]

Data breaches do lead to fraud. An annual nationwide survey has shown an increasingly strong correlation between data breaches and identity theft. Individuals who received a data breach notification in 2012 had an identity theft incidence rate of 22.5 percent, more than four times the 5.3 percent rate for all adults.[3]

The law's impact, however, has been broader than protection against identity theft. It highlighted the cost of bad information management practices and appropriately placed the cost on the company, not the consumer. While the law does not mandate specific data privacy or security practices, the cost of breach notification, in hard dollars and in reputation damage, has tended to focus the attention of top management and shareholders on data privacy and security practices.[4]

The law has also opened a window on privacy and security practices for researchers and policy makers. The data breaches reported to the California Attorney General have allowed us to look through this window. In this report, we describe what we have seen and make recommendations based on our findings.

When it was enacted in 2002, the California data breach notification law was focused on the type of information sought by thieves for financial identity theft: Social Security number, driver's license number, and financial account number. In 2007, with growing awareness of medical identity theft, medical and health insurance information were added as notice-triggering personal information. In 2011, the law was further amended to require entities to provide copies of their notices to the Attorney General when the breach involves more than 500 Californians; notice content requirements were also added.

What the California Law Requires

California Civil Code section 1798.29 applies to state government agencies and section 1798.82 applies to businesses. These statutes are included in the Appendix to this report.

The statutes require any person or business that conducts business in California, and any state agency, that owns or licenses "computerized data" including personal information to notify any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a breach of security.

The type of personal information that triggers the requirement to notify individuals is unencrypted, computerized information, consisting of an individual's name, plus one of the following: Social Security number; driver's license or California Identification Card number; financial account number, including credit or debit card number (along with any PIN or other access code where required for access to the account); medical information (any information regarding an individual's medical history, condition, or treatment); and health insurance information (policy or subscriber number or other identifier used by a health insurer, or information about an individual's application, claims history or appeals).

Notice must be given to individuals "in the most expedient time possible and without unreasonable delay." Notice to individuals may be delayed if a law enforcement agency determines that notification would impede a criminal investigation or in order to take measures necessary to determine the scope of the breach and restore reasonable integrity to the system. An entity that maintains the data but does not own it must notify the data owner immediately following discovery of a breach.

Notice may be provided to individuals in writing, electronically (but only as consistent with the provisions of the Electronic Signatures Act), or by substitute notice. Substitute notice may be used if 1) the cost of providing individual notice is more than $250,000; 2) more than 500,000 people would have to be notified; or 3) the organization does not have sufficient contact information for those affected. Substitute notice means using all of the following methods: available email addresses, conspicuous web site posting, notification of major statewide media, and notification of the California Office of Privacy Protection or, for state agencies, the California Office of Information Security.

The notice to individuals must be written in plain language. It must include the name and contact information of the notifying entity, the types of personal information involved, contact information for the credit reporting agencies in the case of a breach of Social Security or driver's license numbers, and also, if known at the time of notification, the date of the breach, and a general description of the incident. Additional information that may be provided in the notice includes what the entity has done to protect individuals and advice on what individuals can do to protect themselves.

Since January 2012, organizations required to notify individuals of breaches affecting more than 500 Californians must submit a sample copy of the notice to the Attorney General.

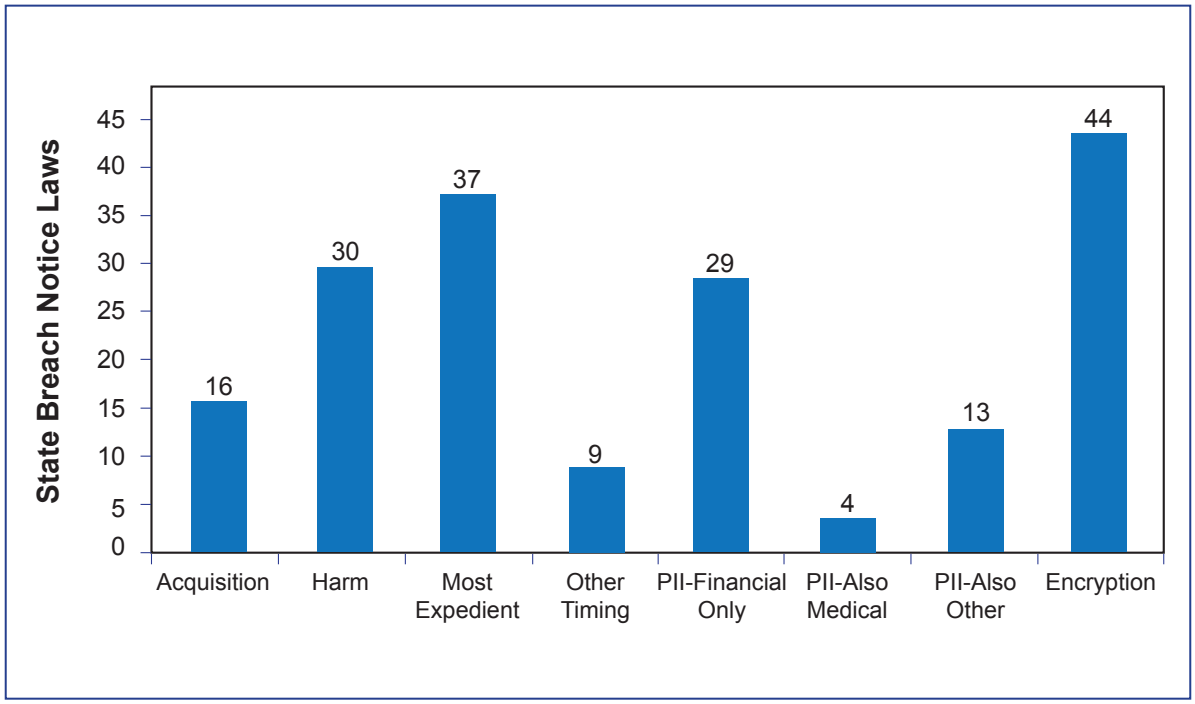
In addition to a "safe harbor" for encrypted data, the law provides for three "exceptions." 1) A covered entity under the Health Insurance Portability and Accountability Act (HIPAA) is deemed to have complied with the notice content requirements of the California law if it has complied completely with the breach notification requirements of the Health Informa-

tion Technology for Economic and Clinical Health Act.[5] 2) An entity may use its own notification procedures as part of its information security policy, if the procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy. 3) In addition, the "good faith employee exception" provides that the unauthorized acquisition of personal information by an employee or agent of an entity acting in good faith is not a breach, provided that the information is not used or further disclosed.

California and Other States

The 46 state breach notification laws are similar, because they are based on the California law. The most significant difference is in the notification trigger. Most states (65 percent) have a "harm" trigger for notification, generally allowing a determination of no reasonable likelihood of harm or misuse of the data to relieve an entity of the obligation to notify. California and 15 others have an acquisition trigger, with requiring notification when data is acquired by an unauthorized person. Most states (80 percent) require notification "in the most expedient time possible, without unreasonable delay." Four others set an outside deadline of 45 days from discovery and one a seven-day deadline. Four states either have no time frame or require notice as soon as practicable. Most states (63 percent) define

Figure 1: State Breach Notification Laws Compared



personally identifiable information for purposes of the law as financially related information only (name plus Social Security number, driver's license number, or financial account number). All but two states have a "safe harbor" from notification for encrypted data. Sixteen states, including California, require notifying the Attorney General or another government agency, and four apply the law not just to "computerized data," but also to data in paper and other formats.[6]

Report Methodology

This report was prepared by the Attorney General's Privacy Enforcement and Protection Unit in order to gain an understanding of the types of incidents that are occurring, what vulnerabilities they may reveal, and what recommendations might be made or actions taken to prevent or reduce the likelihood of future breaches.

The breaches discussed in this report were submitted to the Attorney General in 2012. Some of the incidents reported in 2012 occurred earlier and some incidents that occurred in 2012 were not reported until 2013 and are, therefore, not included in this analysis. In some cases, more than one notice was submitted for the same incident. This was the case when there were groups that were affected differently by the breach and required different information in the notice, or when further investigation revealed new information or new affected groups.

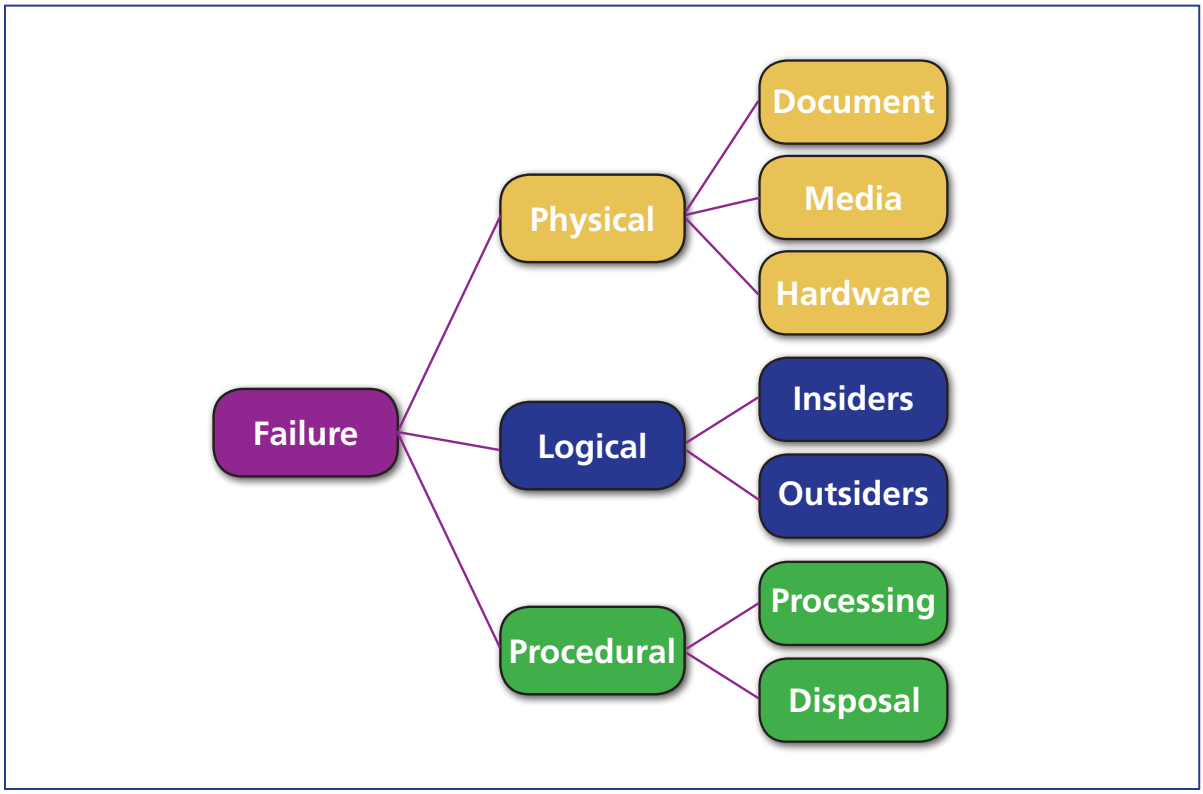
The breaches covered in this report do not represent the entire universe of data breaches requiring notification to California residents. The law requires reporting to the Attorney General only on breaches of electronic data affecting more than 500 individuals. The omission of smaller breaches and non-electronic breaches may qualify our findings and recommendations.

We classified the entities reporting breaches by industry sector, according to the U.S. Census Bureau's North American Industry Classification System.[7] The sectors represented are retail, finance and insurance, education, health care, government, professional services, and other. Professional services includes scientific and technical services. The other category includes accommodation and food services, agriculture, utilities, manufacturing, wholesale trade, transportation, real estate, and waste management, each of which subcategories accounts for just one to three incidents.

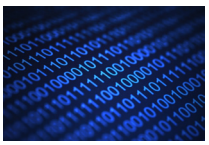
We reclassified 23 incidents reported by companies in the finance and insurance sector as retail incidents. These were breaches of payment card account numbers that occurred not in the financial institution's system but in merchants' systems and in which the payment card issuers notified consumers. We believe that viewing these as retail incidents provides a more accurate picture of the types of breaches that occurred.

In analyzing the data breaches reported in 2012, we used an approach developed by C. Matthew Curtin and Lee T. Ayres.[8] Their "taxonomy of data loss" categorizes the types of failure that result in the loss of control over personal information, enabling the identification of the controls needed to manage the information. All failures are divided into three general categories: physical, logical, and procedural. These are further broken down into more specific levels. See Figure 2.

Figure 2: Curtin & Ayres Taxonomy of Data Loss



Physical failures involve the loss of control over a physical asset containing personal information. This type of failure is comprised of documents, portable data storage media such as flash drives or tapes, and computer hardware that were lost or stolen. *Logical failures* involve intentional access to information without access to the physical asset, either unauthorized access by an insider or the exploitation of vulnerability by an outside hacker. *Procedural failures* result from data custodians mishandling personal information, exposing it to unauthorized parties. These failures include the unintentional exposure of information on a website, exposure in mailings, misdirected mailings and email, and improper disposal or abandonment of information or media.



Breaches Reported in 2012

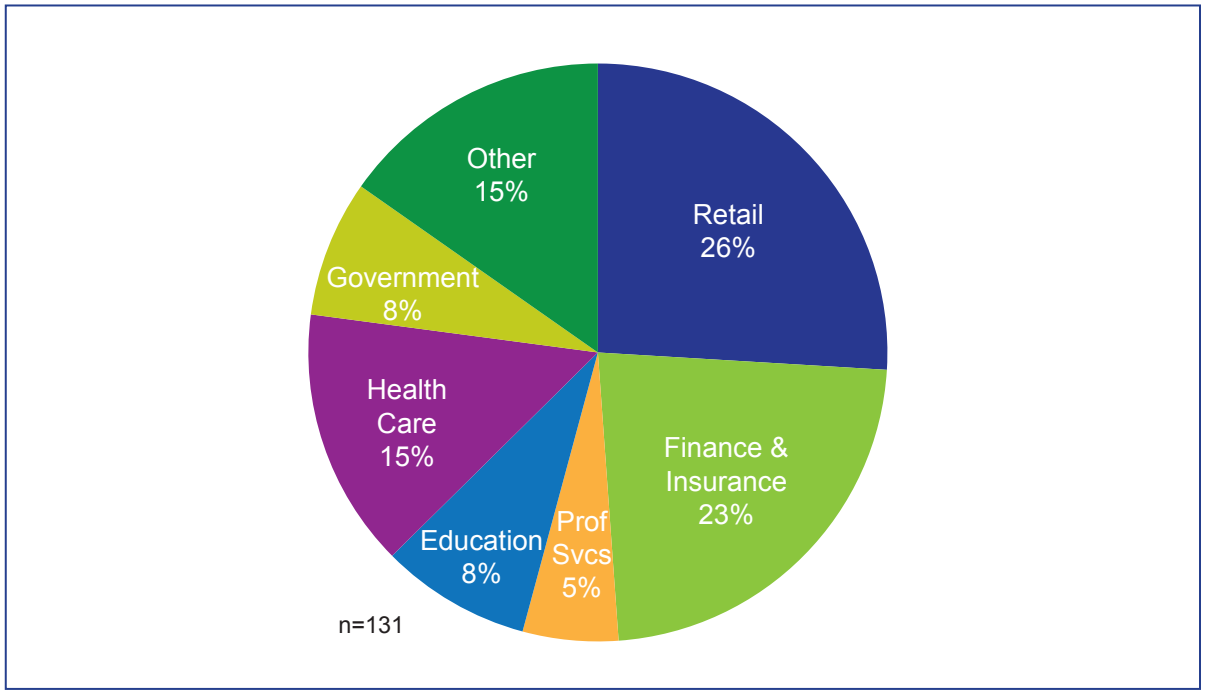
In 2012, the Attorney General's Office received reports of 131 data breaches that each affected more than 500 California residents.[9] The total number of Californians whose personal information was breached was over 2.5 million.

The reports were submitted by 103 different entities. Nine entities reported more than one breach. Three of the entities reporting multiple breaches were payment card issuers who notified their customers of breaches of card account numbers that had occurred either at a merchant or at a payment processor (American Express, 19; Discover Financial Services, three; and Yolo Federal Credit Union, two).

Breaches by Industry Sector

The retail industry reported the largest number of breaches in 2012: 34, representing 26 percent of the total. This was followed closely by finance and insurance with 30 breaches, (23 percent). Health care reported 19 incidents (15 percent), education 11 and government 10 (eight percent each), professional services seven (five percent), and all other sectors combined 20 (15 percent).

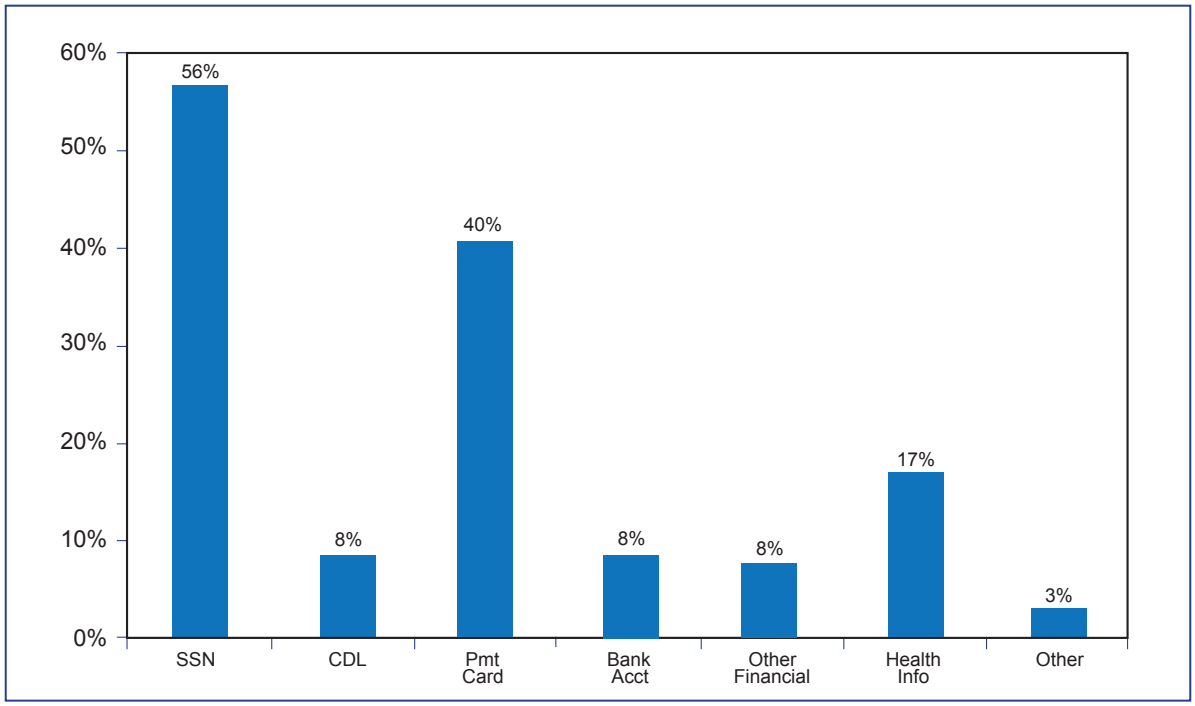
Figure 3: Breaches by Industry Sector



Breaches by Data Type

The type of data most frequently involved in breaches was Social Security numbers, which figured in 74 of the breaches reported (56 percent). The next most commonly breached information was payment card information in 53 breaches (40 percent), followed by health or medical information in 22 breaches (17 percent). Driver's license numbers were involved in 11 breaches, bank account numbers in 11, and other financial account numbers in 10 (eight percent each).

Figure 4: Breaches by Type of Data Involved



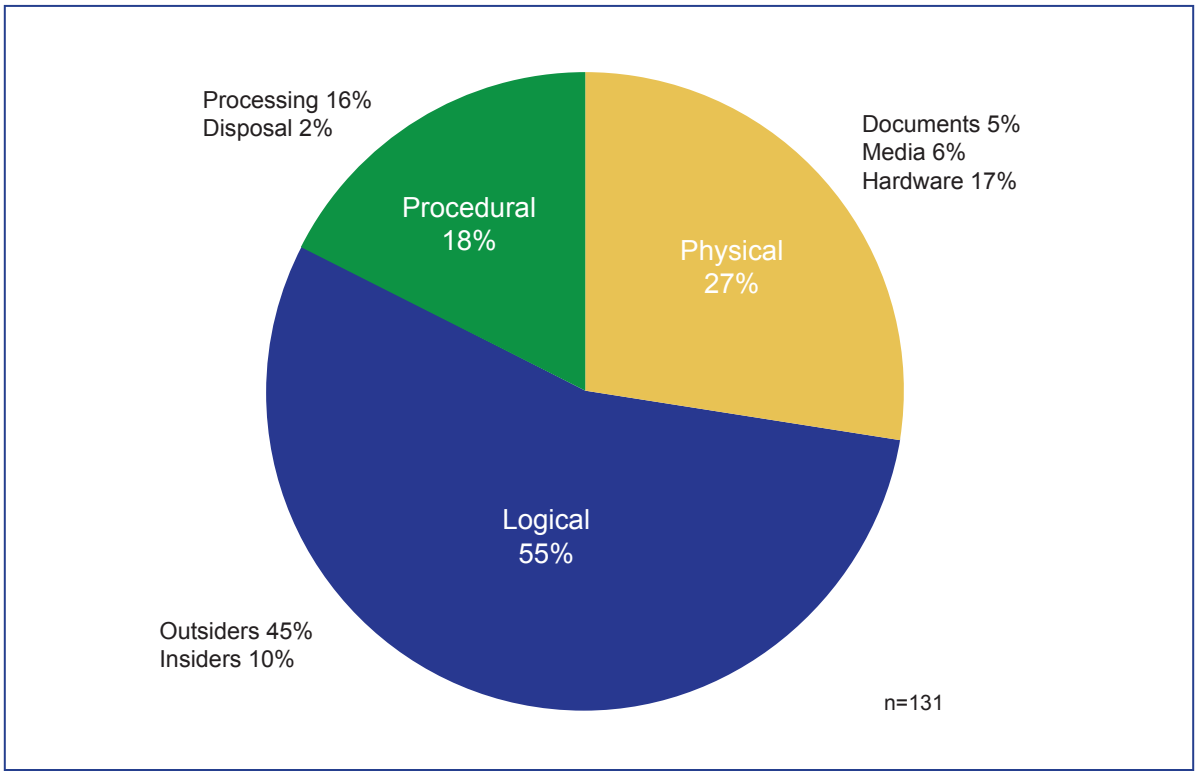
Note: The total is more than 100% because some breaches involved more than one type of data. CDL is California driver's license or state ID card

Breaches by Type of Failure

See Figure 5 for the breakdown of breaches by physical, logical, and procedural failures. More than half of the breaches in 2012 (72 breaches, 55 percent) were the result of logical failures; that is, they were the result of intentional access to data by outsiders or by unauthorized insiders. Outsider intrusions accounted for 59 of the total incidents (45 percent). Twenty-three of these were compromises at a merchant, such as with the installation of a skimming device in a point-of-sale terminal. Two of the five largest breaches

affecting more than 100,000 individuals were caused by outside hackers. Valve Corporation, an online game software company, reported an intrusion affecting 509,000 individuals in February 2012, and Global Payments Inc., a processor of electronic payment transactions, reported an intrusion affecting 139,034 individuals in July 2012. Ten percent of the breaches (13) were caused by insiders – employees, contractors, vendors, customers – who intentionally accessed systems and data without authority.

Figure 5: Breaches by Type of Failure



Note: Rounding may affect totals.

Physical failures accounted for 36 of the breaches (27 percent of the total), with 22 instances of lost or stolen hardware (17 percent), eight of lost or stolen media (six percent), and six of lost or stolen documents (five percent). Two of the five largest incidents were in this category. The California Department of Social Services reported a lost computer storage device containing information on 845,000 parents, children, and caregivers in March 2012, and Emory Healthcare, Inc., reported missing data discs containing financial and medical information on 318,000 patients in May 2012.

Procedural failures were 23 of the incidents (18 percent of the total): 21 caused by processing errors, such as misdirected mail or email, and unintentional web posting. Two were caused by improper disposal of data. One of the five largest breaches was of this type, reported by First Data Corporation in May 2012, as information on 108,500 merchants that was inadvertently transmitted to outside firms.

Breach Size

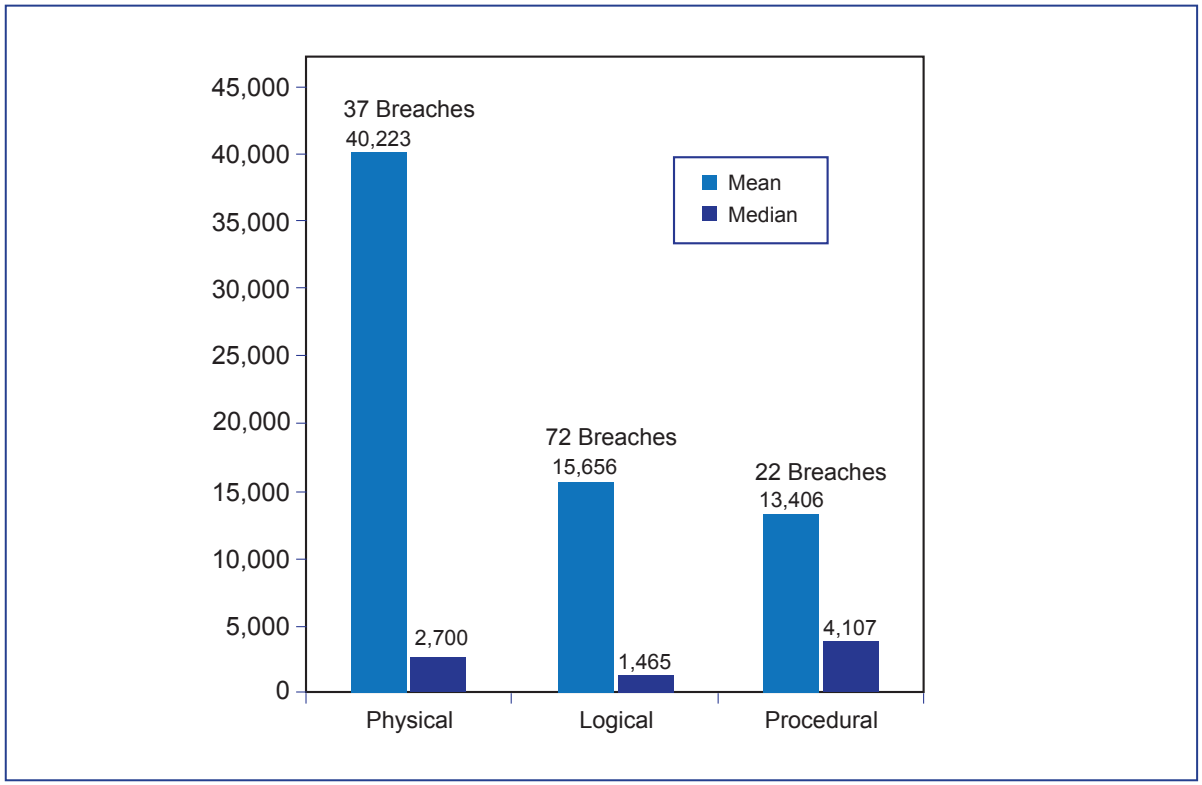
The 131 breaches reported in 2012 affected over 2.5 million Californians.[10] The average (mean) incident involved the personal information of 22,500 individuals. The median breach size was 2,500 affected individuals, with five breaches of 100,000 or more individuals' information.

Breaches resulting from physical failures constituted 27 percent of total breaches in 2012, but they accounted for 58 percent of the victims. The 37 breaches resulting from loss or theft of documents, media, or hardware affected over 1.4 million individuals. This type of breach affected the largest number of individuals on average, at 40,223 per incident. The category includes two of the largest breaches and the median size is 2,700 affected individuals.

The 72 breaches from unauthorized intrusions affected a total of over one million individuals, with an average of 15,656 and a median size of 1,465. This category contained two of the larger breaches. Outsider intrusions affected more people than unauthorized insider intrusions, averaging 18,173 for outsiders and 3,234 for insiders.

The 22 breaches resulting from procedural failures affected over 241,000 people. This type of breach included one of the top five and averaged 13,406 per incident, with a median of 4,107. The two subtypes were similar in size, processing errors averaging 13,548 and inappropriate disposal 12,275.

Figure 6: Breaches by Size



Other Findings

Reporting to the Attorney General: Breaches were reported to the Attorney General an average of 12 days from notification of the affected individuals. Thirty-five percent (46) were reported before or on the same day as individual notification, and 63 percent (82) within 10 days.

Notification of Law Enforcement: In 79 of the breaches (60 percent), reporting entities indicated that they had notified law enforcement. They notified local law enforcement in 45 incidents and federal authorities in 34. In 29 breaches (22 percent), law enforcement was not notified. In the remaining 23 breaches, reporting entities did not indicate whether or not they had notified law enforcement.

Mitigation Products: Offering data breach victims a mitigation product such as credit monitoring has become fairly common. In 65 breaches (50 percent), the breached entity

offered the affected individuals the opportunity to subscribe to credit monitoring or a similar "identity theft protection" product. Credit monitoring services are intended to give individuals early notice when someone applies for new credit accounts in their name, so that they can take prompt corrective action. Such a service can be beneficial in the case of breaches of Social Security or driver's license numbers, which can be used by a thief (along with other easily acquired personal information) to open new accounts. While 75 breaches involved Social Security numbers or driver's license numbers, in 22 breaches no mitigation product was offered. On the other hand, such products were offered in 12 breaches involving just payment card numbers, which do not facilitate the opening of new accounts.

Breaches of Paper Records: While the breach notification law specifies "computerized data" as the type that triggers notice when breached, 10 of the breaches reported (8 percent) involved paper records. Seven of them were misdirected, lost or stolen mail and three were records stolen from a car or office.

Readability of Notices: An analysis of 70 randomly selected notices revealed an average reading grade level of 14 using the Flesch-Kinkaid Grade-Level formula.[11]

Encryption: Thirty-six of the breaches (27 percent), affecting a total of over 1.4 million Californians, involved lost or stolen digital data or misdirected emails in which the personal information was unencrypted.

Recommendations

While 131 data breaches may not be a large sample, certain patterns suggest opportunities for improvements that could result in fewer data breaches affecting fewer people and more effective assistance to those put at risk when breaches do occur.

1. Make it an enforcement priority to investigate breaches involving unencrypted personal information. The Legislature may also want to consider requiring the use of encryption to protect personal information in transit.

Ten years after the California breach notification law took effect, we are still seeing the unencrypted personal information of tens of thousands of individuals carried on laptops and left in cars, shipped on tapes and mailed on thumb drives, and stored on desktop computers in offices. Employees use email to send Social Security numbers and other personal information that is not encrypted, and when the email goes astray, so does the information. This is true even with the law's "safe harbor" that exempts encrypted personal information from the notification requirement.

Twenty-eight percent of the data breaches reported in 2012 were the result of lost or stolen media or hardware or misdirected email containing unencrypted personal information. There were 22 instances of lost or stolen computer hardware and eight of lost or stolen digital media in the breaches. There were also seven breaches caused by misdirected emails containing unencrypted information.

Fully 89 percent of these breaches involved Social Security numbers, which enable new account and account takeover fraud, the types of identity theft that are the most costly to resolve. If the data had been encrypted, very likely all of those incidents would not have required notification and would not have exposed over 1.4 million victims to the risk of harm.

Breaches of these types also tended to be larger than other types, that is, they affected more people on average. Breaches caused by a failure to protect physical information assets affected 40,223 people on average, nearly three times the 15,656 affected in an average intrusion.

These breaches are essentially the result of deficient data management policies or practices, in particular, a failure to encrypt sensitive data when it is in transit on portable devices or in emails. In spite of the carrot of the breach notification law's encryption exemption, organizations are subjecting too many Californians to a risk that is eminently avoidable.

The Attorney General's Office will make it an enforcement priority to investigate breaches involving unencrypted personal information, and encourages our allied law enforcement agencies to similarly prioritize these investigations.

We also recommend enacting a law to require the use of encryption to protect personal information on portable devices and media and in email. An appropriate encryption standard might be FIPS 197, the National Institute of Standards and Technology's standard approved for U.S. Government organizations to protect higher risk information.

2. Companies and agencies should review and tighten security controls protecting personal information, including training of employees and contractors.

More than half of the breaches reported in 2012 (72, representing 55 percent) were the result of intentional access to data by outsiders or by unauthorized insiders. This suggests a need to review and strengthen security controls applied to personal information. We recognize that cyber security is a continual and escalating battle, but it is one that must be vigorously waged. Companies and agencies have legal and moral obligations to protect personal information with reasonable and appropriate safeguards. California law requires businesses to use reasonable and appropriate security procedures and practices to protect personal information.[12] Doing so is also a competitive imperative for companies whose business model depends on the use of customer information and on the trust of those who tender it. We also note that the best protection is to limit the collection and retention of personal information.

The retail sector accounted for 44 percent of the intrusions, followed by finance and insurance at 26 percent. Both industries should continue to work on security improvements, including better protections for point-of-sale terminals and the payment card processing network.

In light of the risks posed by the theft of online credentials (see Recommendation 5), companies should take measures to protect against such intrusions. Protective measures include multi-factor authentication to protect sensitive systems and strong encryption to protect user IDs and passwords in storage. In addition, using system-enforced strong passwords is valuable for user education, as well as a good security practice.

A key component of an information privacy and security program is regular training on an organization's policies and procedures for the employees, contractors, and other agents who handle personal information. Many of the 17 percent of breaches that resulted from

procedural failures were likely the result of ignorance of or noncompliance with organizational policies regarding email, data destruction, and web site posting.

Even a smaller business – such as the office of a doctor, dentist, or accountant – may be the custodian of the very sensitive personal information of thousands of past and present clients and employees. Protecting that information is part of their professional and legal responsibilities. We encourage them to review their security practices, including investigating ways to use encryption effectively, and to consult their professional organizations and security experts for best practice guidance.

3. Companies and agencies should improve the readability of breach notices.

The purpose of a breach notice is to alert individuals that their personal information is at risk, giving them the opportunity to take protective action. This purpose can only be accomplished if the recipients understand the notices. In addition, the law requires that the notices be written in plain language.

We found an average reading level of 14th grade in the sample of notices we reviewed. This is significantly higher than the average reading level in the U.S. The National Assessment of Adult Literacy found in 2003 that 43 percent of the U.S. population is at or below basic literacy levels, with the average reading level equivalent to eighth grade.[13]

Communications professionals can help in making the notice more accessible, using techniques such as shorter sentences, familiar words and phrases, the active voice, and layout that supports clarity such as headers for key points and smaller text blocks.

4. Companies and agencies should offer mitigation products or provide information on the security freeze to victims of breaches of Social Security numbers or driver's license numbers.

Criminals use Social Security numbers and driver's license numbers to perpetrate one of the most serious types of identity theft: new account fraud. New account fraud, in which the victim's personal information is used to open new credit card or other accounts, increased by 50 percent in 2012, representing 23 percent of identity theft.[14] While there are fewer victims of this type of fraud than of the more common existing account fraud, the impact on victims is greater.

When a breach compromises a credit card number, victims can protect themselves from charges made by a thief simply by closing the affected account, which generally takes just a phone call and perhaps a letter of dispute. In addition, federal law limits a consumer's liability for unauthorized credit card transactions to $50 and most banks today have a zero-liability policy.[15]

The situation is much different for a breach of a Social Security number. A thief can use the number, along with the victim's name and other easily obtainable information, to do a number of things, including opening new accounts, taking out loans, receiving medical services, even providing the information when arrested or prosecuted for a crime. Because the thief usually provides a different address, the victim does not receive bills and may not learn of the problem for many months, perhaps when he or she is denied credit or is contacted by a debt collector. Victims of new account identity theft may spend hundreds of hours and thousands of dollars clearing up their records and their lives.

There are protective measures available that can limit, or in some cases prevent, the harm of fraudulently opened new accounts. One such measure is a credit monitoring or "identity theft protection" service. Credit monitoring provides alerts, usually by email, whenever an application for new credit is submitted to a consumer credit reporting agency. Such an early warning allows a consumer to take immediate action to dispute or even prevent a new account from being opened. Some services may provide credit monitoring with out-of-band alerts, such as by cell phone, in closer to real time, enabling the prevention of the account opening. Many protection services supplement credit monitoring with monitoring of web sites for personal information, and may provide insurance that covers some victim costs when identity theft does occur.

Another protective measure, which can prevent the fraudulent opening of most new accounts, is a security freeze. This measure is available by law in California and many other states and is offered by the credit reporting agencies in all states. When a consumer has placed a security freeze on his or her credit records, a creditor considering opening a new account receives a response from the credit reporting agencies that the file is frozen. In the absence of a credit rating, most creditors will not open a new account. (A consumer who places a freeze is provided with a mechanism for unlocking the records when desiring to apply for new credit.)[16]

Seventy-five of the breaches reported in 2012 involved Social Security numbers or driver's license numbers. In 22 of those breaches, no credit monitoring or other mitigation product was offered to victims. Because of the severity of the impact of this type of breach and because protective measures are available, we recommend that companies and agencies notifying of a Social Security number or driver's license number breach offer protective

measures to victims. This could mean providing credit monitoring or a broader identity theft protection service for a period of time. In selecting an identity theft services provider, we suggest consulting the best practices and reviews that the Consumer Federation of America developed with the help of identity theft service providers and consumer advocates.[17]

A good alternative, which is less costly, is the security freeze. We encourage providing victims with the option of a security freeze even if another mitigation product is offered. The freeze is the strongest protection available against the most prevalent types of new account identity theft.

5. Consider legislation to amend the breach notification law to require notification of breaches of online credentials, such as user name and password.

As consumers and businesses have moved online, identity thieves have followed. Along with dumpster diving and stealing wallets to get personal information, thieves are resorting to sophisticated attacks involving the use of stolen online credentials. In recent years intrusions at Sony, Yahoo, the *New York Times*, and Twitter have targeted passwords and other account credentials of more than one million people.[18] Criminals use the stolen credentials to get access to the accounts, and because most consumers do not use unique passwords for all their accounts, a takeover of one can result in access to all, including banking and other supposedly secure accounts.

The Attorney General's eCrime Unit reports that in one breach targeting California law enforcement, a web site operator did not notify officers that their user names and passwords had been compromised, since there is no legal requirement to make such a notification. California's breach notice law does not require notifying individuals where an email address or user ID in combination with a password or security question and answer is compromised.

Criminals and even foreign governments are focusing efforts on web sites with inadequate security to harvest email addresses, user names, and passwords. Stolen credentials can open the doors not only to the theft of personal and corporate information, but also to cyber attacks on critical infrastructure and national assets.

Just as the breach notice law was amended to include medical information when medical identity theft was recognized, so now is the time to update it to address changing criminal practices by adding online credentials (user ID or email address, in combination with pass-

word or security question and answer) to the type of personal information requiring notification if breached. Such a law would enable breach victims to be notified and take action to protect themselves and also the other assets to which they have authorized access.

Appendix

Breach Notification Law

California Civil Code Section 1798.29

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 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.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) 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. The notification shall also include the date of the notice.

(D) Whether the 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.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(g) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(i) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Internet Web site page, if the agency maintains one.

(C) Notification to major statewide media and the Office of Information Security within the California Technology Agency.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

California Civil Code Section 1798.82

(a) Any person or business that conducts business in California, and 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 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 person or business that maintains computerized data that includes personal information that the person or business 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.

(d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language.

(2) The security breach notification shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) 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. The notification shall also include the date of the notice.

(D) 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.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Medical information.

(5) Health insurance information.

(i) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(j) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media and the Office of Privacy Protection within the State and Consumer Services Agency.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of

personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Information Security Law

California Civil Code Section 1798.81.5

(a) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information. For the purpose of this section, the phrase "owns or licenses" is intended to include, but is not limited to, personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates.

(b) A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(A) Social security number.

(B) Driver's license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(D) Medical information.

(2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

(3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code.

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.

(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

Notes

[1] Only Alabama, Kentucky, New Mexico and South Dakota do not have breach notification laws, as of September 1, 2012.

[2] See legislative committee analyses of SB 1386 (Peace) and AB 700 (Simitian) of 2002, at *www.leginfo.ca.gov*.

[3] Javelin Strategy & Research, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters" (February 2013), available at *www.javelinstrategy.com*. Javelin found an incidence of identity fraud among data breach victims of 11.8 percent in 2010, 18.9 percent in 2011, and 22.5 percent in 2012.

[4] The cost per compromised record in 2011 was estimated at $194, according to the Ponemon institute's "2011 U.S. Cost of Data Breach Study" (March 2012), available at *www.ponemon.org/library*.

[5] HIPAA, the federal Health Insurance Portability and Accountability Act (42 U.S.C. § 1320d et seq.); the HITECH Act, the federal Health Information Technology for Economic and Clinical Health Act, (Public Law 111-5), which amended HIPAA.

[6] For a table comparing state breach laws, see Mintz Levin, "State Data Security Breach Notification Laws," (2012), available at *www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf*.

[7] The 2012 NAICS, available at *www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012*.

[8] C. Matthew Curtin, CISSP, and Lee T. Ayres, CISSP, "Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry," 4 ISJLP 525–922 (2008), 569-601.

[9] The sample breach notices submitted by entities reporting breaches are posted on the Attorney General's web site at *www.oag.ca.gov/ecrime/databreach/list*.

[10] The number affected was provided to the Attorney General for 114 breaches (87 percent of the total).

[11] The Flesch-Kinkaid Grade-Level score was determined by using Microsoft Office Word 2007's built-in readability calculating function. In an article on using Word's readability calculator in the Michigan Bar Journal (January 2009), Norman Stockmeyer, former president of Scribes, the American Society of Legal Writers, acknowledged the limitations of such programs: "While not 100 percent reliable, readability tests are as reliable as other common psychological tests, such as reading tests. They work well because they use simple word-length and sentence-length factors, which are among the primary causes of reading difficulty."

[12] See Civil Code sec. 1798.81.5, included in Appendix to this report.

[13] The National Assessment of Adult Literacy is administered by the National Center for Education Statistics in the Department of Education, *nces.ed.gov/naal/.*

[14] Javelin Strategy & Research, op cit. The incidence of new account identity theft increased from 0.82 percent of adults in 2011 to 1.22 percent in 2012. This type of identity theft constituted 23 percent of the crime in 2012, but nearly half of the total annual cost ($10 billion of $21 billion).

[15] The Fair Credit Billing Act, 15 U.S.C. § 1601 et seq., for credit cards, and the Electronic Funds Transfer Act, 15 USC 1693 et seq., for debit cards.

[16] For more information on the security freeze in California, see How to Freeze your Credit Files, available on the Attorney General's web site at *www.oag.ca.gov/idtheft/information-sheets*.

[17] Consumer Federation of America, "Best Practices for Identity Theft Services," and "Best Practices for Identity Theft Services: How Are Services Measuring Up?," available at *www.idtheftinfo.org*.

[18] Sony breach:
http://online.wsj.com/article/SB10001424052748704810504576307322759299038.html;
Yahoo! breach:
http://abcnews.go.com/blogs/technology/2012/07/yahoo-password-breach-includes-gmail-hotmail-and-aol-users/;
New York Times breach:
http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0;
Twitter breach:
http://www.informationweek.com/security/application-security/twitter-pursues-two-factor-authenticatio/240147787.

California Department of Justice
Privacy Enforcement and Protection Unit

www.oag.ca.gov/privacy