California Data Breach Report

October 2014

Kamala D. Harris, Attorney General
California Department of Justice

California
Data Breach Report

October 2014

Kamala D. Harris, Attorney General
California Department of Justice

Contents

Message from the Attorney General

California is the birthplace of the digital revolution that has transformed nearly every aspect of the world in which we live. Yet even as technological innovation and advances bring us greater convenience, efficiency, and productivity, they are also generating new vulnerabilities. The Internet has created a new frontier for criminal activity in the form of cybercrime, such as data breaches.

The term "data breach" refers to any situation in which an individual or group steals sensitive, protected or confidential data. By compromising sensitive information, such as payment card data, Social Security numbers and health records, data breaches place the privacy, security, and economic wellbeing of businesses and consumers at risk. Increasingly, highly sophisticated criminal organizations and state-sponsored entities — located as far away as Russia, China and Eastern Europe — are responsible for breaches.

With the world's eighth largest economy and more than 38 million consumers, California is uniquely impacted by data breaches. In 2012, 17 percent of the data breaches recorded in the United States took place in California – more than any other state. Even more troubling, the number of reported breaches in California increased by 28 percent in 2013.

Fortunately, the Golden State is on the cutting edge when it comes to protecting consumers and businesses from emerging cyberthreats. In 2003, California was the first state to mandate data breach notifications, requiring businesses and state agencies to alert Californians when their personal information is exposed in a security breach. Since 2012, companies and state agencies subject to that law have been required to report any breach involving more than 500 Californians to the Office of the Attorney General.

This report sheds light on the threat that data breaches pose to California consumers and businesses, including an analysis of the information the Attorney General's office collected on data breaches in California in 2013. It also contains best practices and makes recommendations to companies, law enforcement agencies, and the legislature about how data security can be improved. For example, we recommend that companies take advantage of cutting-edge technology to devalue payment data in the event of a security breach. This would mean that data, even if stolen by criminals, would not be useful for processing new transactions.

Data breaches are a serious threat to Californians' privacy, finances, and even their personal security. As California continues to lead the way in technological innovation, we must also continue to ensure that consumers and businesses are protected from cybercriminals and others who seek to profit from data breaches. My office has made it a priority to investigate data breaches and enforce California's consumer privacy laws, which are the strongest and most sophisticated in the nation. This report is designed to be helpful to consumers, businesses, and government agencies alike.

Sincerely,

Attorney General Kamala D. Harris

Executive Summary

Payment Card Data and Health Information at Risk

In this report, Attorney General Kamala D. Harris presents findings and recommendations based on a review of the 167 breaches reported in 2013 and on the full set of 298 breaches reported since 2012.

The critical role that retailers play in the payment card system came into sharp relief the past year with a series of large retailer breaches involving payment card data. This type of breach often occurs when skilled hackers and thieves seek out and steal payment card data, then sell the information on the black market to transnational criminal organizations that quickly monetize the information, defrauding innocent consumers and harming retailer victims and others in the payment chain. Criminal organizations target not only major corporations but also smaller businesses, such as franchise operations, which are far less able to bear the cost of a breach.

In 2013, the number of reported data breaches increased by 28 percent, and the number of Californians' records affected increased by over 600 percent. This later increase was due largely to two massive retailer breaches, one of which, the Target breach, involved the payment card data of 41 million individuals, including 7.5 million Californians.

Today technological advances offer means to devalue payment card data, making it an unattractive target for hackers and thieves. Chip cards and tokenization are among the most promising tools for protecting retailers and consumers from the theft and abuse of payment card data. This report includes several recommendations intended to encourage the rapid adoption of these security technologies.

The report also includes recommendations on improving the readability and helpfulness of breach notices, particularly of the substitute notices, which involve web site posting and media notification, that are used in retailer breaches of payment card data. A recent study found that breach notices from retailers were viewed less favorably by recipients than notices from other industry sectors.[1]

In the health care sector, breaches affected more records than in other industry sectors, with the exception of retail since the two mega breaches of 2013. Many of the health care breaches reported to us are of a type that could be prevented by the strategic use of encryption. Unlike other industry sectors, where computer intrusions caused the majority of breaches, in health care 70 percent of breaches reported in the past two years were the result of stolen or lost hardware or digital media containing unencrypted personal information.

A recent study by the Ponemon Institute reports that criminal attacks targeting the health care system are growing and that employees' use of unsecured portable devices is also increasing the risk of breach.[2] The need to use encryption is a lesson that must be learned by the health care industry and we recommend that it be applied not only to laptops and portable media, but also to many computers in offices.

Key Findings

- In 2013 Attorney General Kamala D. Harris's office received reports of 167 data breaches affecting more than 500 California residents. This constitutes a 28 percent increase over the 131 breaches reported in 2012.
- The records containing personal information of more than 18.5 million California residents were involved in breaches reported in 2013, constituting an increase of more than 600 percent over the 2.5 million records breached in 2012.
- The 2013 breaches included two very large incidents that skew the data. If those two breaches (Target and LivingSocial) were excluded, the number of records affected would have been 3.5 million, a 35 percent increase over 2012.
- The retail industry reported the most breaches in 2013: 43 (26 percent of total breaches), followed by finance and insurance with 33 (20 percent) and health care with 25 (15 percent).
- Retail breaches affected 15.4 million records of Californians, 84 percent of the total records breached in 2013.
- More than half of the 2013 breaches (53 percent) were caused by computer intrusions (malware and hacking). The remaining breaches resulted from physical loss or theft of laptops or other devices containing unencrypted personal information (26 percent), unintentional errors (18 percent) and intentional misuse by insiders (four percent).
- In 2012-2013, 84 percent of retail industry breaches were the result of malware and hacking, distinguishing the sector from all others, where 36 percent of breaches were of this type.
- In 2012-2013, the majority of breaches in the health care sector (70 percent) were caused by lost or stolen hardware or portable media containing unencrypted data, in contrast to just 19 percent of such breaches in other sectors.
- In 2012-2013, in 29 percent of breaches of Social Security or driver's license numbers, where a mitigation service such as credit monitoring or a security freeze would have been helpful, the breached entity failed to offer such a service.

Key Recommendations

California Retailers should:

- Move promptly to update their point-of-sale terminals so that they are chip-enabled and should install the software needed to operate this technology.
- Implement appropriate encryption solutions to devalue payment card data, including encrypting the data from the point of capture until completion of transaction authorization.
- Implement appropriate tokenization solutions to devalue payment card data, including in online and mobile transactions.
- Respond promptly to their data breaches and should notify affected individuals in the most expedient time possible, without unreasonable delay.
- Improve their substitute notices regarding payment card data breaches.

California Retailers and Financial Institutions should:

- Work together to protect debit cardholders in retailer breaches of unencrypted payment card data.

The California Health Care Sector should:

- Consistently use strong encryption to protect medical information on laptops and on other portable devices and should consider it for desktop computers.

The California State Legislature should:

- Consider legislation to amend the breach notice law to strengthen the substitute notice procedure, clarify the roles and responsibilities of data owners and data maintainers, and require a final breach report to the Attorney General.
- Consider legislation to provide funding to support system upgrades for small California retailers.

Introduction

Data Breaches and Harm

A data breach is harmful to all concerned. Organizations that experience a data breach must pay the costs of responding to it and often pay even more in reputational damage. Not only large corporations but also smaller businesses are targeted by data thieves. A franchise store or a restaurant, for example, can find its financial viability threatened by a breach.

Individuals whose personal information is breached can also suffer financial loss and other significant harms. One harm that can result from a data breach is identity theft, defined as the unauthorized taking and use of personal information for unlawful purposes.[3] The national survey on identity theft conducted annually by Javelin Strategy & Research has shown that the correlation between breaches and identity theft has been increasing for several years. In their most recent study, Javelin found that nearly one in three data breach victims in 2013 also became an identity theft victim in the same year. This is an increase from nearly one in four in 2012.[4]

Another Javelin study, on payment card data security, found that card fraud following a data breach more than quadrupled from 2010 to 2012.[5] According to Javelin, 36 percent of data breach victims suffered card fraud in 2013, up from 28 percent the previous year.[6]

In spite of laws that limit consumers' liability for many fraud-related losses, consumers often do pay to resolve identity theft situations. Such costs may include photocopying, postage, certified mail charges or credit monitoring. The out-of-pocket costs to identity theft victims vary, depending on the type of data involved. The average cost to a consumer who falls victim to the fraudulent use of a credit card account is $63, debit card $170, checking account $222 and Social Security number $289.[7]

Identity theft is not the only harm that a data breach can inflict on victims. Stolen sensitive personal information can be used to damage people's reputations, extort money from them and put them at risk of physical harm. Stolen credentials can open the doors to the theft of personal and corporate information and can also enable cyber attacks, including attacks on critical infrastructure.

Criminal Organizations and Data Breaches

As the profitability of cybercrimes has become apparent, criminal organizations have increasingly engineered and executed some of the most devastating data breaches in the United States. Many of these assailants are transnational criminal organizations that operate remotely, avoiding arrest or prosecution due to the obstacles law enforcement may encounter when tracking perpetrators in foreign jurisdictions. Moreover, cybercrimes can be difficult to detect, and even if offenders are prosecuted, they are likely to receive penalties that are lower by comparison to violent crimes and drug trafficking.[8]

Criminal organizations have targeted a wide array of sensitive information, but tend to focus on Social Security numbers and payment card data. While the value on the black market of a stolen Social Security number is greater than the value of a payment card number, the speed with which payment card data can be monetized has put this type of data in the sights of many criminals. In one instance, an Eastern European transnational criminal organization stole 160 million credit card numbers by attacking numerous companies around the world and then sold the credit card numbers on the black market for $10 per American number and $50 per European number.[9]

For more information on the involvement of transnational criminal organizations in cybercrimes and traditional crimes, see the Attorney General's report *California and the Fight Against Transnational Criminal Organizations.*[10]

Update on 2012 Data Breach Report

California's landmark data breach notification law has made it possible for individuals to learn about breaches of their personal information and take action to protect themselves from many of the harmful uses of the information.[11]

The 2003 law, which has served as a model for 47 other states as well as for jurisdictions around the world, was inspired by the environmental justice movement. Like the disclosure of toxic emissions, notification of data breaches provides transparency to the public. It gives individuals early warning that their personal information is at risk of being abused, allowing them to take action to protect themselves. The requirement to notify also serves as an incentive to businesses and other organizations to improve their privacy and security practices.

Since 2012, organizations have been required to submit a sample copy of their breach notices to the Attorney General when a breach involves the personal information of more than 500 Californians. The Privacy Protection and Enforcement Unit reviews the reported breaches, reports on patterns and trends and makes recommendations to help reduce the number of data breaches and the number of people affected, as well as to encourage more effective assistance to those put at risk when breaches do occur.

In our first report on data breaches, we made five specific recommendations, two of which have since been enacted as amendments to the data breach law. We recommended that, as a result of increased criminal focus on stealing online account credentials, this type of personal information should be included in the breach notice law. Based on our recommendation, SB 46 of 2013 was enacted to do just that; the law took effect in January 2014.[12]

We recommended that companies should offer mitigation products or provide information on the security freeze to victims of breaches of Social Security numbers or driver's license numbers. In 2014, AB 1710 was enacted, requiring the source of a breach of such data to offer identity theft prevention and mitigation services at no cost to the affected person for no less than 12 months.[13] It will take effect in January 2015.

Another of our legislative recommendations has not come to pass: requiring encryption to protect personal information in transit. Such a requirement was included in an early version of AB 1710, but was not in the version enacted.

We also recommended that organizations review and tighten security controls protecting personal information, including training of employees and contractors. As part of this recommendation, we noted that the retail and financial services sectors should continue to work on security improvements, including better protections for point-of-sale terminals and the payment card processing network. It is difficult to assess whether organizations are improving their information security. The 28 percent increase in the number of breaches reported to us in 2013 may both reflect security weaknesses and increases in targeted criminal attacks. And the several large retail breaches reported in 2013 (and continuing in 2014) attest to the need for significant security improvements in this sector. AB 1710, which amended the breach law, also amended the data security statute, adding the requirement that maintainers of personal information, not just the owners of such data, must use reasonable and appropriate security safeguards to protect the data.[14]

On the other hand, our recommendation to companies and agencies to improve the readability of their breach notices does not seem to have been heeded. The reading level of notices submitted in 2012 averaged at the college level (grade 14), as did the 2013 notices (grade 13). This is significantly beyond the average reading level of the American population, which is equivalent to eighth grade.[15] The intended benefit of the notices – to give individuals the opportunity to take action to protect themselves from the abuse of their personal information – is undercut if the recipients cannot understand them.

2013 Data Breaches

In 2013, the Attorney General received reports of 167 data breaches, each of which affected more than 500 California residents. This was a 28 percent increase over the 131 breaches reported in 2012. A total of 18.5 million records of California residents were put at risk by the 2013 breaches, up more than 600 percent from 2.6 million in 2012. (We use the term "records," rather than "individuals," because one individual may have records breached in more than one incident or included in more than one dataset in a single incident.)

Breaches were reported by 136 different entities. Six entities reported more than one breach: American Express submitted 21 breaches, Discover Financial Services submitted seven, Massachusetts Mutual life Insurance submitted four, Kaiser submitted two and the California Correctional Health Care Services Department and the California Employment Development Department each submitted two. It should be noted that the breaches reported by American Express and Discover did not occur in their systems. American Express and Discover, as payment card processors, submitted the notices they provided to their cardholders of breaches that had occurred in either merchant or payment processor systems.

In 2013, there were two large-scale breaches experienced by the retail industry: the Living-Social breach of online account credentials, reported in April 2013, and the Target breach of payment card data, reported in December 2013. Each of these two breaches put the personal information of approximately 7.5 million Californians at risk.

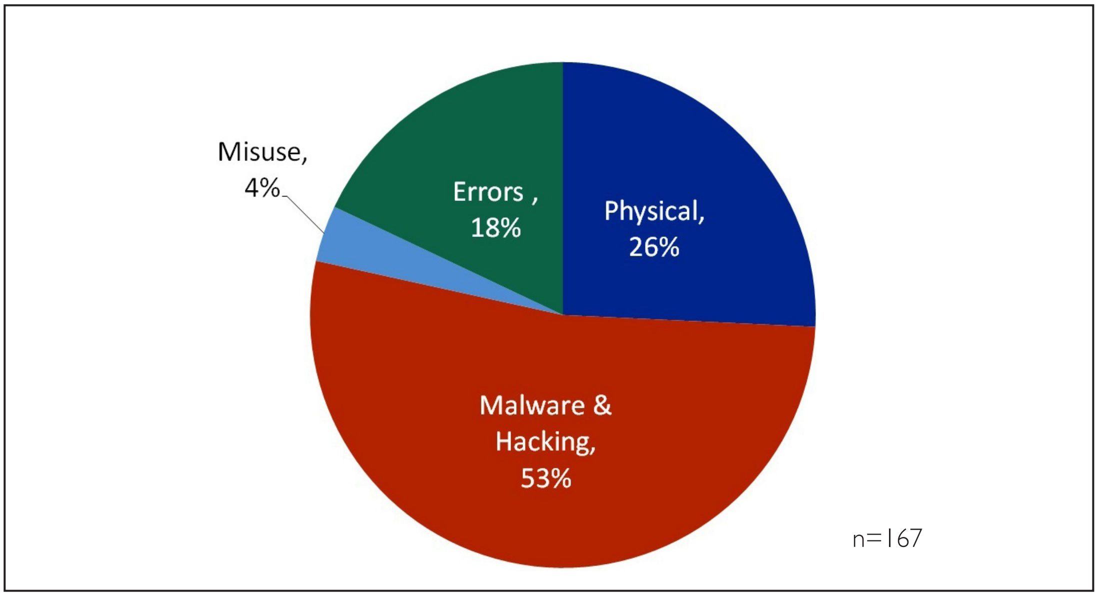
Despite these two outlier incidents, the distribution of breaches by industry and type is fairly consistent over the two years that the Attorney General has received reports of breaches.

Breach Types

As shown in Figure 1, Malware and Hacking breaches made up over half (53 percent) of all reported incidents in 2013, followed by Physical Theft and Loss (26 percent), Errors (18 percent) and Misuse (4 percent).

The distribution of breaches by type in 2012 was similar: Malware and Hacking was the largest category (45 percent), followed by Physical Theft and Loss (27 percent), Errors (18 percent) and Misuse (10 percent).

Figure 1: 2013 Breach by Types



- ## Malware and Hacking

  The Malware and Hacking category covers intentional unauthorized intrusions into computer systems. Malware and Hacking breaches comprised a majority (53 percent) of all breaches reported in 2013.

  Malware and Hacking breaches made up 93 percent of all compromised records (over 17 million records). The LivingSocial and Target breaches accounted for the bulk of those records. In April, the online marketplace LivingSocial reported a cyber attack on their systems that compromised the names, email addresses, some birth dates and passwords of over 50 million customers, including 7.5 million Californians. In December, Target reported a hacking and malware insertion into its network that resulted in the theft of the names and payment card data of 41 million customers, including 7.5 million Californians.

  These two outliers explain the significant gap between average number of affected records in a breach (211,946) and the much lower median (2,600). Nevertheless, the prevalence of Malware and Hacking breaches suggests that attention should be directed towards reducing the risk of this type of breach.

  The Malware and Hacking category showed the greatest increase from 2012. The share of these breaches rose from 45 percent in 2012 to 53 percent in 2013.

- **Physical Theft and Loss**

  Physical breaches include all breaches in which data stored in a physical form was lost, stolen or otherwise removed from the owner's control. These breaches involve the theft or loss of laptop and desktop computers, hard drives, USB drives, data tapes or paper documents.

  Physical breaches were the second most common type of breach, making up 26 percent of reported incidents in 2013. These breaches compromised a total of 1.15 million records, averaging 27,389 per incident, with a median breach size of 3,082 records.

  The share of Physical breaches (26 percent) did not change significantly from 2012 (27 percent). In 2012, however, Physical breaches comprised a far larger share of records affected: 56 percent, compared to just six percent of records breached in 2013.

- **Miscellaneous Errors**

  Breaches resulting from Miscellaneous Errors include anything unintentionally done or left undone that exposes personal information to unintended individuals. Errors can include misdelivery, when personal information is accidentally sent to unintended recipients; insecure disposal, when documents or media containing personal information are disposed of without being shredded or "wiped"; and inadvertent publishing of personal information, making it available to individuals not authorized to access it, such as by posting it on a website.

  As in 2012, Errors accounted for 18 percent of all reported breaches in 2013. The 2013 Error breaches resulted in the compromise of 136,833 records. These breaches involved an average of 4,877 records with a median size of 1,317 – much smaller than the two previous types of breach. In 2012, this type of breach affected approximately the same number of records (130,371), but the average size was greater at 7,660, with a median of 2,992.

  The consequences of a single accidental email or mistaken posting should not be underestimated. Of the 30 Error breaches reported in 2013, 17 were instances of unintentional publishing, resulting in exposing 104,355 records. The 12 breaches resulting from misdelivery compromised 31,732 records. Although these two errors occurred with similar frequency, publishing errors exposed far more personal information.

- **Misuse**

  Breaches caused by Misuse occur when an insider makes unauthorized use of privileges or resources. These breaches accounted for a small percentage of total breaches reported and a small share of records breached. Instances of Misuse caused six breaches in

2013 (four percent), and compromised 1,681 records (0.1 percent of total records). The average breach size was 1,947, and the median was 1,036 records, accounting for the least number of records of any breach type.

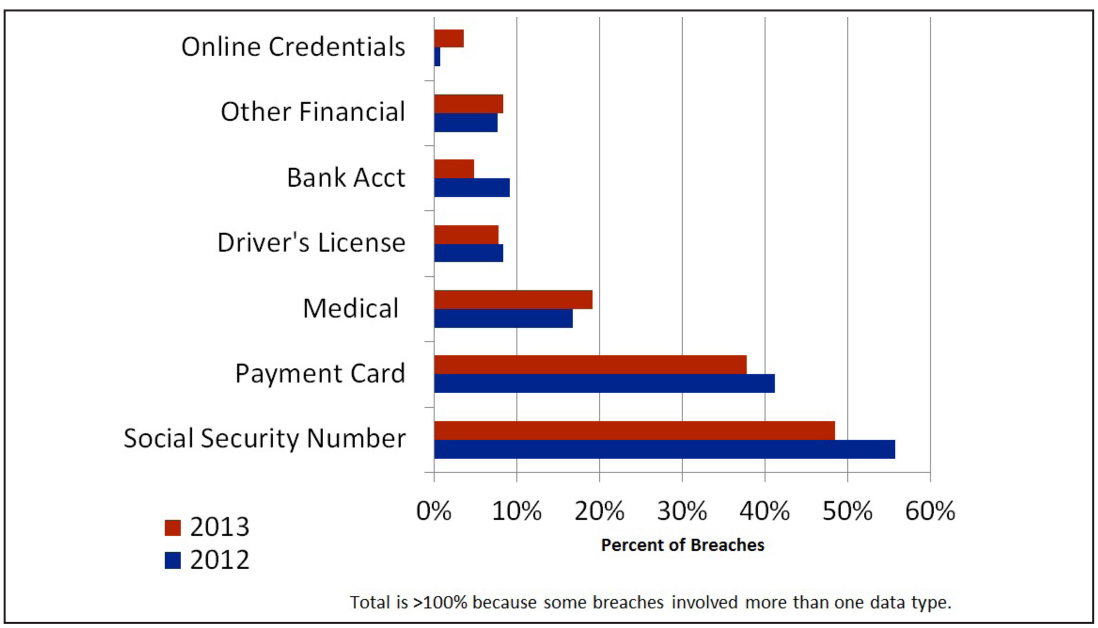
Misuse breaches fell by 50 percent in 2013. In 2012 there were 13 such breaches reported, for 10 percent of the total.

Data Types

As shown in Figure 2, nearly half of data breaches reported in 2013 involved Social Security numbers, making this the most frequently compromised data type in 2013. This is a slight decline from 2012, when Social Security numbers were involved in 56 percent of breaches. The next most frequently breached data type was payment card data (38 percent), followed by medical information (19 percent), driver's license numbers (eight percent), bank account numbers (five percent) and other financial information (eight percent). There were six notifications of a breach of online account credentials, even though the law did not require such notification until 2014. In four of them other notice-triggering information was also breached.

The distribution in 2012 was similar: Social Security numbers figuring in 56 percent of reported breaches, then payment card data (41 percent), medical information (17 percent), driver's license numbers (eight percent), bank account numbers (nine percent), other financial information (eight percent) and online credentials (one percent).

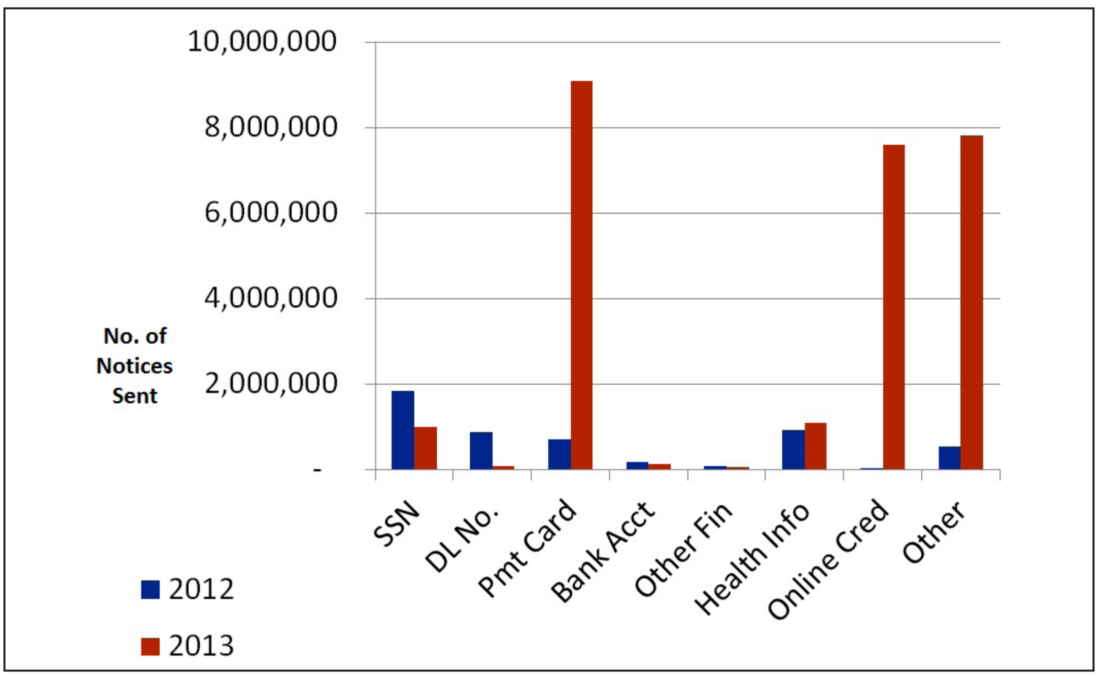
Figure 2: Type of Data Breached



It should not be surprising that Social Security numbers and payment card data are so often compromised, given their value to criminals. The value to a criminal of a stolen Social Security number is greater than the value of payment card data. The mean fraud amount for stolen Social Security numbers is $2,330, compared to $2,026 for a debit card and $1,251 for a credit card.[16]

Figure 3 showing the type of data breached by the number of records or the number of notices sent reveals a different picture, where payment card data and online account credentials dominated. Over nine million notices in 2013 alerted Californians to breaches of their payment card data (49 percent of the 18.5 million notices sent), and nearly eight million notices warned of a breach of online account credentials (42 percent of total notices).

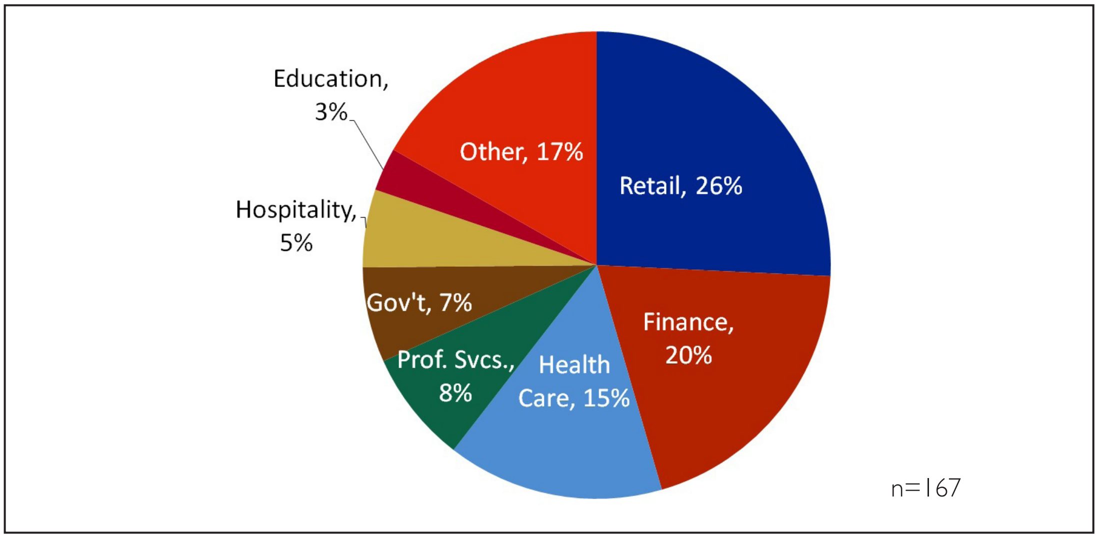
Figure 3: Share of Records Breached by Data Type



Industry Sectors

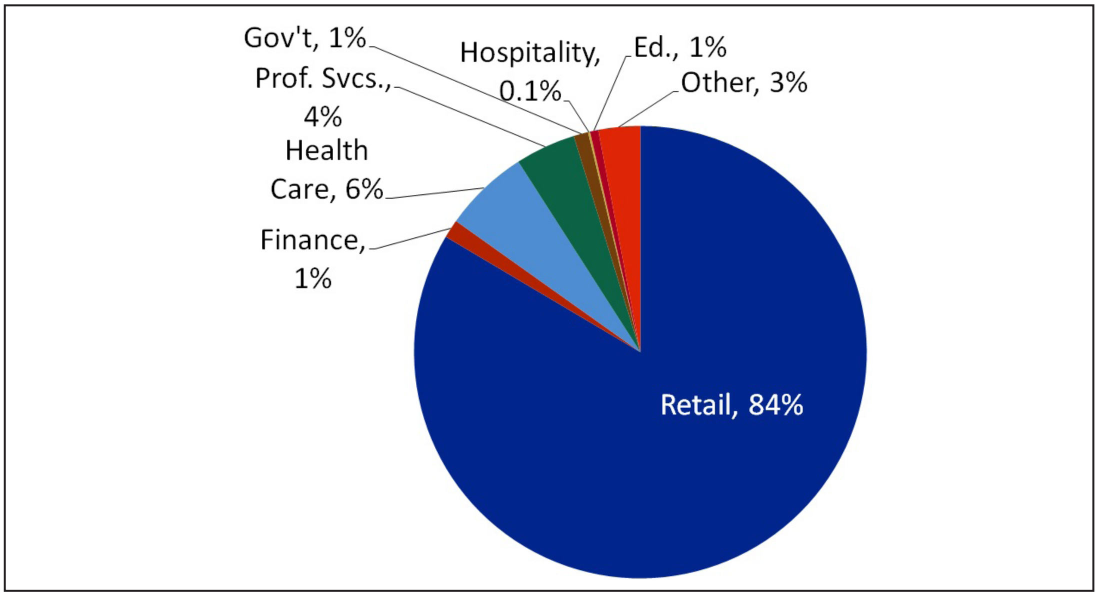
In 2013, the retail sector reported the largest number of breaches: 43, representing 26 percent of total breaches, as shown in Figure 4. This was followed closely by the finance and insurance sector with 33 breaches (20 percent) and health care with 25 breaches (15 percent). Professional services, government, hospitality and education each accounted for less than 10 percent, with all other sectors combined making up 17 percent.

Figure 4: 2013 Breaches by Industry Sector



As shown in Figure 5, retail industry breaches involved the most records, 15.4 million, which is 84 percent of total records breached in 2013. Health care breaches affected 1.1 million records (six percent), professional services 795,000 (four percent), finance 245,000 (one percent), followed by government 194,000, education 109,000 and hospitality 26,000 (all at less than one percent).

Figure 5: 2013 Records Breached by Industry Sector



2012-2013 Breaches Combined

The profile of breaches by industry and type is fairly consistent over the two years that incidents have been reported to the Attorney General. In both years, the retail sector accounted for the most breaches (26 percent), followed by the finance sector (22 percent in 2012, 20 percent in 2013) and then health care (15 percent). None of the remaining sectors were responsible for more than seven percent of the breaches. In both years computer intrusion (malware and hacking) was the predominant type, making up about half of the breaches each year (45 percent in 2012, 53 percent in 2013). The next most common type of breach was physical theft or loss of hardware or documents containing unencrypted personal information (27 percent in 2012, 26 percent in 2013), followed by unintended errors made by authorized persons (18 percent) and intentional misuse of data access privileges by insiders (20 percent in 2012, four percent in 2013).

Combining the data for this period, we can begin to get a picture of differences among industry sectors. Our analysis particularly focuses on breaches within the retail and health care sectors, because these industries experienced respective malware and hacking breaches and physical breaches that were disproportionate in comparison to other sectors. Moreover, these industries accounted for the majority of breached personal records. Finally, the two massive retailer breaches in 2013 deserve special attention in our analysis.

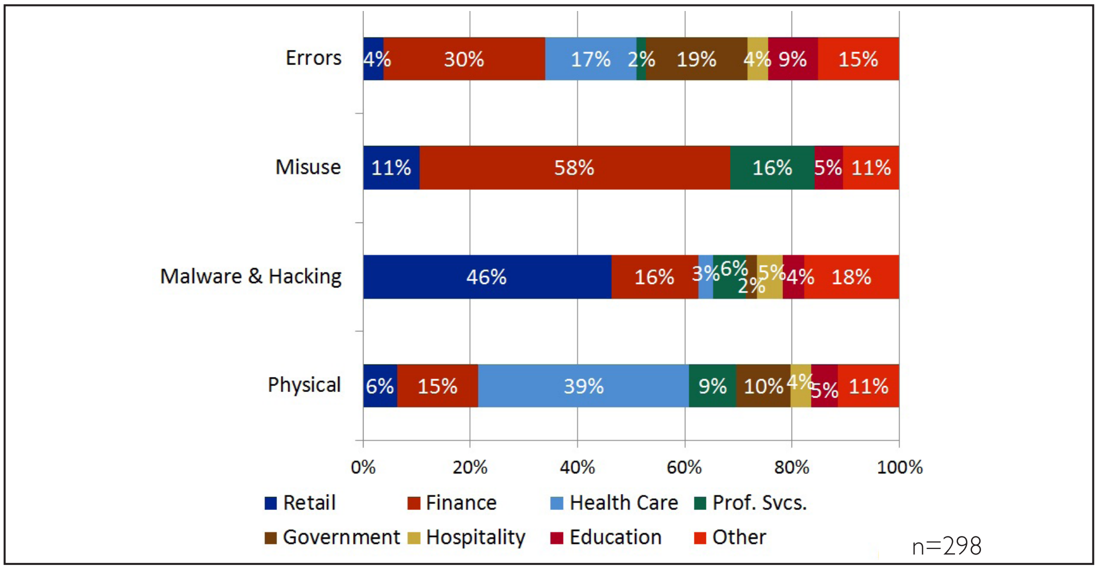
Figures 6 and 7 show the types of breach within industry sectors for 2012 and 2013. In Figure 6, we see that malware and hacking is the predominant type of breach for the two-year period, and that the retail sector, which is responsible for one quarter of the breaches, accounts for nearly half (46 percent) of the malware and hacking breaches.

Physical theft or loss was the second most common type of breach, with 79 incidents making up 27 percent of total breaches. The largest share of the physical breaches occurred in the health care sector, where 31 incidents comprise 39 percent of such breaches.

Errors were responsible for 53 breaches, for 18 percent of the total. The finance sector accounted for the largest share of this type of breach at 30 percent, followed by government at 19 percent and health care at 17 percent.

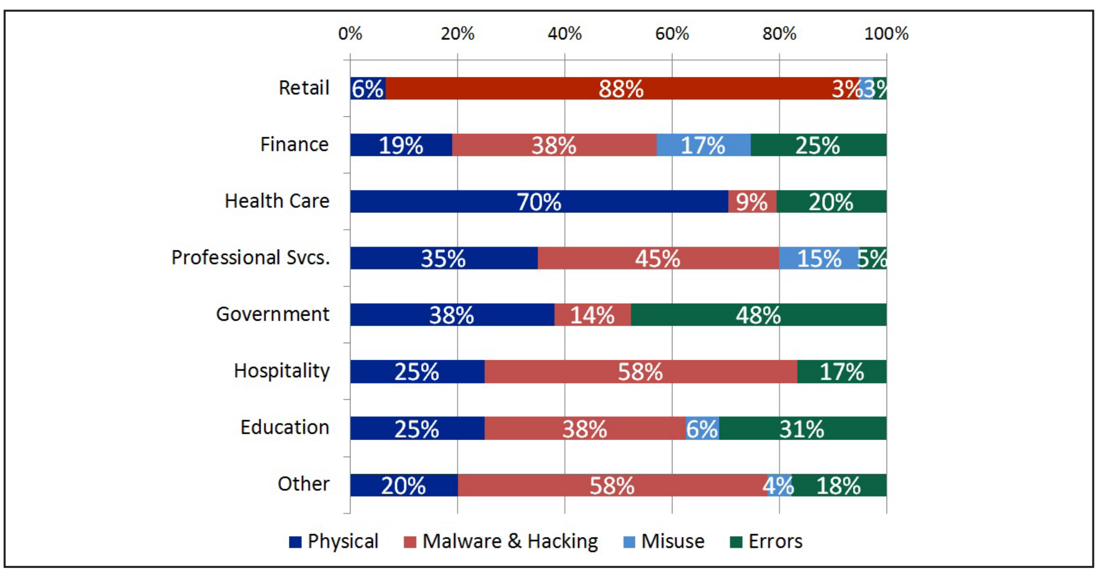
Misuse of access or privilege by insiders led to 19 breaches, six percent of total breaches. Eleven of these (58 percent) were experienced by the finance sector.

Figure 6: 2012 and 2013 Breach Type by Industry Sector



In Figure 7, we see that the dominant type of breach in the retail sector was Malware and Hacking, representing 88 percent of total retail breaches. The same type also dominated in the hospitality industry (58 percent of sector breaches), and to a lesser degree in the professional services sector (45 percent), finance (39 percent) and education (38 percent). Only in the health care sector was Malware and Hacking not the leading cause of breaches.

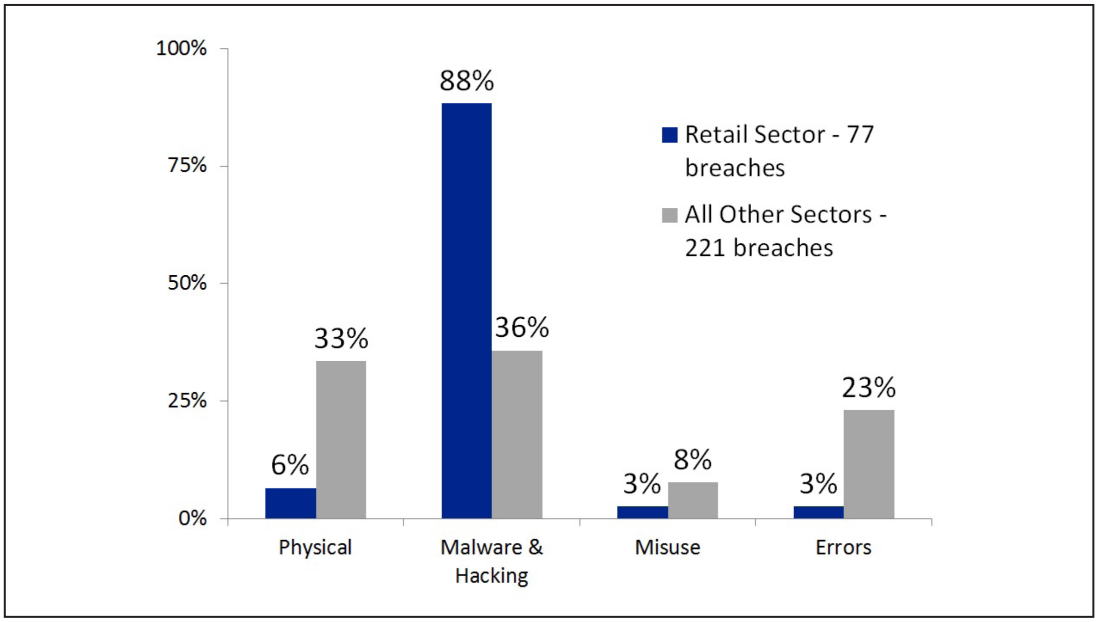
Figure 7: 2012 and 2013 Industry Sectors by Breach Type



Retail Sector Breaches

The 77 retail industry breaches comprised 26 percent of all the breaches reported during the two-year period. As shown in Figure 8, nearly all of the retail breaches (68 breaches or 88 percent) were the result of malware and hacking. While this type of breach represents the largest share of all non-retail incidents (36 percent), it is much less dominant in other industry sectors.

Figure 8: Retail Sector vs. All Other Sectors by Type of Breach



Retail sector breaches affected 15.6 million records of Californians, 74 percent of the total number affected in all breaches reported in 2012 and 2013. This is significantly the result of the two very large incidents at Target and LivingSocial in 2013, which together involve over 15 million records of Californians. Without those two breaches, the retail sector would have ranked fourth in the number of records breached.

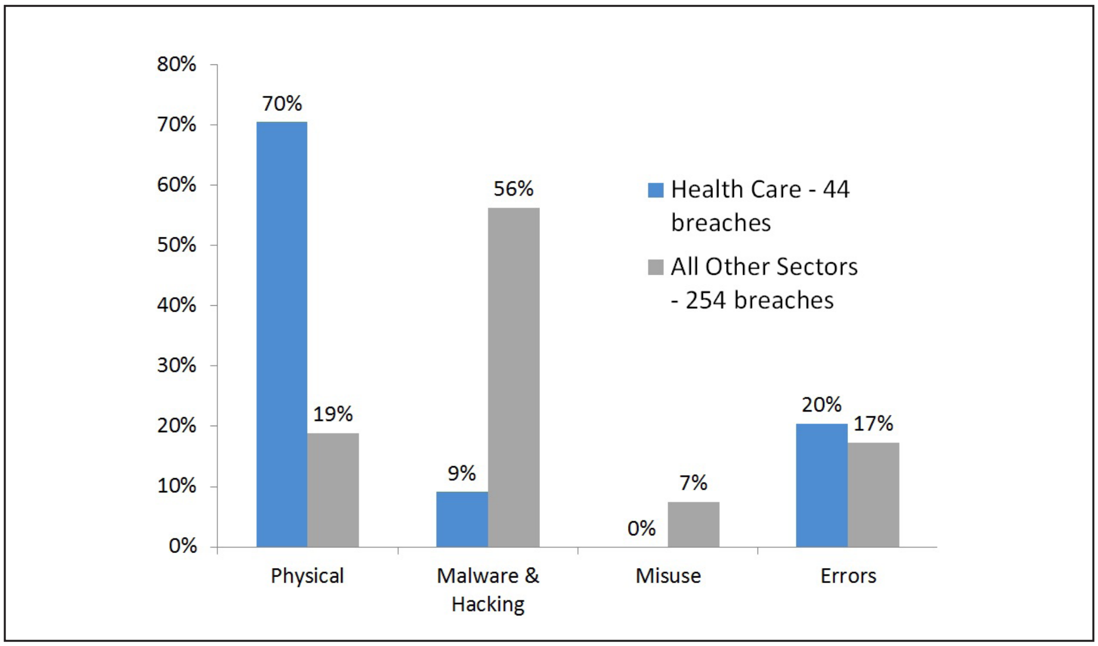
Unsurprisingly, nearly all – 90 percent – of retail breaches involved payment card data. This is the type of data involved in nearly all retailer breaches, and because breaches of payment card data have the strongest correlation with fraud, retail breaches are the most likely to actually result in fraud.

Ten percent of retail breaches involved Social Security numbers and 17 percent other types of data.

Health Care Sector Breaches

The 44 health care breaches made up 15 percent of the breaches during the two-year period. As shown in Figure 9, health care reported the smallest share (nine percent) of malware and hacking breaches, the most prevalent breach type. The majority of health care breaches resulted from physical theft or loss, which accounts for 70 percent of all the health care breaches. Physical breaches involving unencrypted digital data accounted for 70 percent of health care breaches, compared to 19 percent of breaches in other sectors.

Figure 9: Health Care Sector vs. All Other Sectors by Type of Breach



Of health care's 31 physical breaches, 24 resulted from stolen hardware, five from lost media and two from stolen documents. The stolen hardware was comprised of 16 laptops and eight desktops. Two thirds of the hardware items (eight desktops and eight laptops) were stolen from an office or workplace, with the remaining eight laptops stolen from an employee's car or home. The lost digital media were four USB drives and one disc. The documents were records stolen from a storeroom in one instance and from an employee's car in the other.

Over half of health care breaches (55 percent) involved Social Security numbers, but the most common type of data breached was health information, which represented 75 percent of health care breaches.

Health care breaches were second to retail in the number of records affected. The 1.5 million records involved in health care breaches accounted for two percent of all records breached. If the Target and LivingSocial breaches were removed from the data set, health care breaches would rank first in the number of records affected.

Additional Findings

Law Enforcement Notification: Reporting entities indicated that they had notified law enforcement in 184 of the 298 total breaches (62 percent). Federal law enforcement agencies were notified in 78 cases, local agencies in 95 and both federal and local agencies in six cases. Five entities did not specify which level of law enforcement was contacted.

In 58 breaches (19 percent), reporting entities did not notify law enforcement. The breach law does not require notifying law enforcement and in some situations such notification is not necessary, such as in cases of internal employee errors. In 57 breaches, reporting entities did not indicate whether or not they had notified law enforcement.

Mitigation Services: It has become increasingly common for entities experiencing a data breach to offer victims a mitigation service, such as credit monitoring or a security freeze. In 140 breaches (47 percent), the breached entity offered affected individuals free subscriptions to credit monitoring or similar "identity theft protection" services. Such services can be helpful in cases where Social Security numbers or driver's License numbers are compromised, as they give early notice to individuals when criminals use their information to open new accounts in their name.

While 157 breaches involved Social Security numbers or driver's license numbers, a mitigation service was offered in just 112 of them (71 percent). In 45 of such breaches (29 percent), no service was offered. There was no meaningful change from 2012, when no mitigation service was offered in 29 percent of breaches where it would have been helpful, to 2013, when no such product was offered in 28 percent of appropriate breaches.

Breaches of Paper Records: While the breach notification law is triggered when "computerized data" is compromised, 24 of the breaches reported (eight percent) involved paper records. Ten breaches involved lost or stolen documents, 10 resulted from internal misdelivery and four from external misdelivery.

Readability of Notices: Using the Flesch-Kinkaid Grade-Level index[17] to assess readability, we analyzed 70 randomly selected notices and found no significant improvement in readability over the two years. The average reading grade was college level in both years: 14 in 2012 and 13 in 2013.

Encryption: Eighty-three of the breaches (28 percent) involved unencrypted digital data on lost or stolen hardware and media (70) or in misdirected emails (13). Social Security numbers were included in more than three quarters of those breaches (64). Those 83 incidents affected a total of 2.6 million Californians.

Substitute Notice: Of the 298 breach notices submitted, just six (two percent) were substitute notices delivered through web posting, news media and sometimes email, rather than individual notices mailed to individuals. Three of the substitute notices were from retailers, one from a restaurant, one from a spa and one from an online gaming company. Five of these breaches involved payment card data and the sixth, at the gaming company, involved online account credentials. For half of these breaches, the substitute notice method would have been justified by the number of affected parties (more than 500,000) and for all of them, the method could have been justified by a lack of sufficient contact information to provide individual written notices.

Recommendations

Our analysis of the 298 breaches reported to the Attorney General in the past two years reveals certain patterns that suggest opportunities for improvement, and we believe that there are lessons to be learned.[18] We offer these recommendations to companies and agencies in an effort to help reduce the number of data breaches and the number of people affected, as well as to encourage more effective assistance to those put at risk when breaches do occur.

Recommendations on Retail Sector Breaches and Payment Card Data Protection

The critical role that retailers play in the payment card system came to public attention in the past year with a series of large retailer breaches involving payment card data. Payment card data breaches often occur when skilled hackers and thieves seek out and steal payment card data, then sell the information on the black market to transnational criminal organizations that quickly monetize the information, defrauding innocent consumers and harming retailer victims and others in the payment chain. In 2013, the number of reported data breaches increased by 28 percent, and the number of Californians' records affected increased by over 600 percent. This later increase was due largely to two massive retailer breaches, one of which, the Target breach, involved the payment card data of 41 million individuals, including 7.5 million Californians.

While not all breaches result in fraud, breaches of payment card data – the type involved in nearly all retailer breaches – are the most likely to result in fraud. One study found that 36 percent of card breach victims experienced the fraudulent use of their existing card accounts in 2013, compared to 5 percent for other consumers.[19] Victims of this type of breach can have funds put on hold, miss payments linked to the compromised card and even have their bank accounts drained. For these victims, not having access to a payment card or bank account can create serious difficulties. For retailers, exposure to liability, reputational harm and lost business can cause devastating consequences.

The serious effects of payment card breaches highlight the need for retailers to take affirmative steps in their data security programs to devalue payment card data and to improve the timeliness and quality of their responses to a breach.

Devaluing Payment Card Data

The data that criminals are after is the Primary Account Number (PAN), the number printed on the front of a payment card and encoded in the card's magnetic stripe, along with the Card Verification Value (CVV). The PAN identifies the financial institution that issued the payment card and the associated customer account. Traditionally, payment card security has focused on securing the PAN as it moves through the payment cycle.

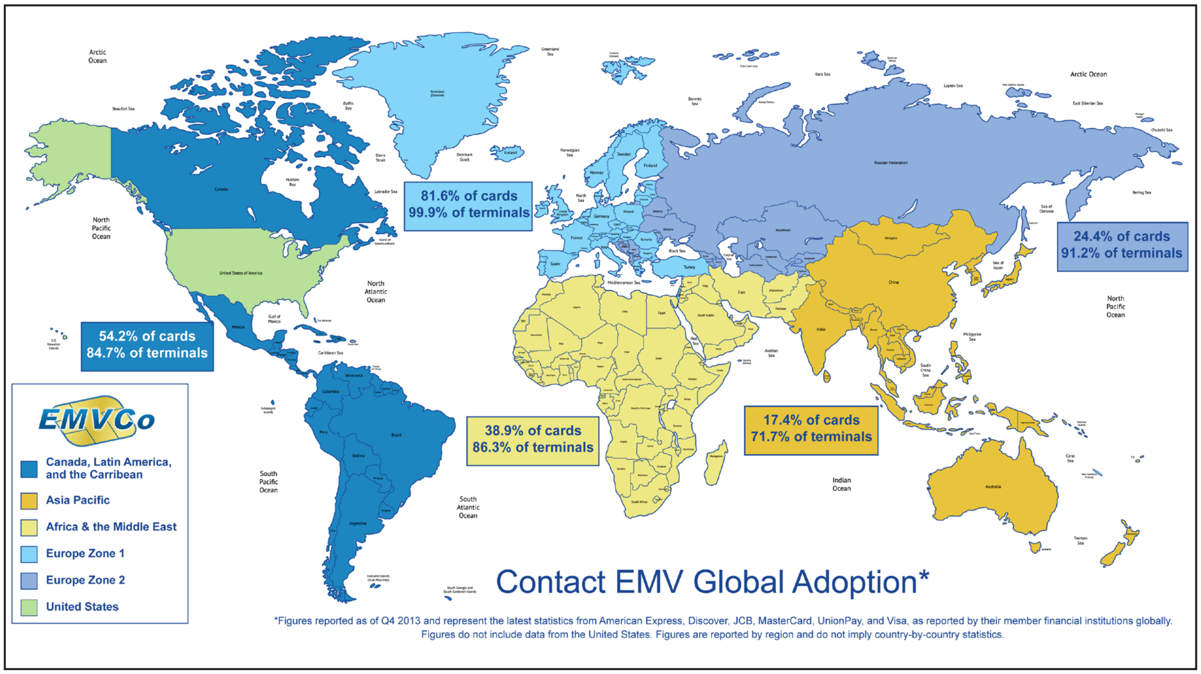
The Payment Card Industry Data Security Standard (PCI-DSS) is a set of industry requirements that the card networks (Visa, MasterCard, American Express, Discover) contractually obligate businesses that handle cardholder information to follow. PCI-DSS provides general technical guidance, but not always specific requirements. It requires rendering PANs unreadable when stored, but does not specify how this is to be accomplished. Encryption is one measure suggested by PCI-DSS and strong encryption is required for data in transmission across open, public networks.

Today technological advances offer ways to devalue payment card data, making it an unattractive target for hackers and thieves looking for data they can quickly convert to cash, while avoiding some of the vulnerabilities of encrypting data that must pass through the many different systems of the payment card ecosystem. Chip cards and tokenization are among the most promising tools for protecting retailers and consumers from the theft and abuse of payment card data.

Recommendation 1: California retailers should move promptly to update their point-of-sale terminals so that they are chip-enabled and should install the software needed to operate this technology.

A global standard for payment cards based on chip technology was established in 1994 and since then, more than 80 countries have moved to use chip cards, including countries in Europe and Asia, as well as Canada, Mexico and Brazil. Often referred to as EMV, after the companies that originally established the standard,[20] a chip-embedded card provides more security for cardholder data than the payment cards with magnetic stripes that are in use in the U.S. today. Countries that have adopted chip cards experienced a dramatic decrease in fraud in face-to-face card transactions. For example, following the move to chip cards in the UK in 2004, counterfeit card fraud losses there fell by 34 percent.[21]

Figure 10: Chip Card Technology Around the World



Reproduced with Permission from EMVCO

The U.S. has already begun migrating to payment cards with chip technology, but currently, most Americans still use payment cards with 1970s magnetic stripe technology. Payment cards with imbedded computer chips offer significant security improvements over existing magnetic stripe payment cards for face-to-face card present (CP) transactions. Magnetic stripe technology is static, merely storing the account number, and lacks the capability of verifying the authenticity of the card itself. The chip card, interacting with the retailer terminal to authenticate the card, has the ability to send a one-time message that changes for every transaction. The result is that payment card data is a less attractive target for thieves to use for making counterfeit cards. With the addition of a cardholder-verification procedure, based on a PIN or a signature, the technology can also authenticate the cardholder, protecting against the fraudulent use of lost or stolen cards.[22]

Retailers play a major role in the success of chip card implementation in the United States. A recent industry forecast estimated that more than 575 million chip-enabled payment cards will have been issued by the end of 2015, representing more than half of all cards.[23] As major financial institutions have started issuing chip cards, retailers have begun upgrading their terminals with the hardware and software required to operate the chip technology. The massive breaches at Target and other large retailers in 2013 and early 2014 have accelerated merchant acceptance and willingness to upgrade to chip card technology. They have good reason to do so, as retailers who do not upgrade will soon face additional exposure to liability for fraud, such as in the case of a data breach. As of October 2015, the payment card networks (American Express, Discover, MasterCard and Visa) will impose a liability shift on retailers, so that if a chip card is used at a terminal that is not chip-enabled, the retailer will be liable if the resulting transaction is determined to have been counterfeit fraud.

Chip cards do not provide protection against online card fraud or other card not present (CNP) fraud. Although CNP transactions are on the rise, the vast majority of consumer card transactions today – 90 percent or more – still occur face to face. Therefore, chip technology has enormous potential to make most consumer card transactions more secure.

Recommendation 2: California Retailers should implement appropriate encryption solutions to devalue payment card data, including encrypting the data from the point of capture until completion of transaction authorization.

While upgrading to chip technology will prevent counterfeit fraud and PIN or signature verification adds protection against the fraudulent use of lost or stolen cards, chip technology is not a silver bullet that will stop all payment card fraud. Retailers must also protect card data during transactions and in storage. Encryption and tokenization are two technologies that can address different vulnerabilities in the payment process.[24]

Encryption can be used by retailers to avoid exposing the PAN from the first moment it is captured at the point-of-sale terminal or at the point of initiation of the transaction, until the authorization of the transaction authorization is completed. During the encryption process, the PAN is transformed from plain-text format into a non-readable form by a mathematical algorithm. Once encrypted, that PAN can only be decrypted into its readable format by using a cryptographic key generated by the algorithm. Of course, if a thief steals the key as well as the data, then the data is readable. Key management can be challenging, particularly in a payment card network where the data must be decrypted and re-encrypted as it passes through multiple systems.

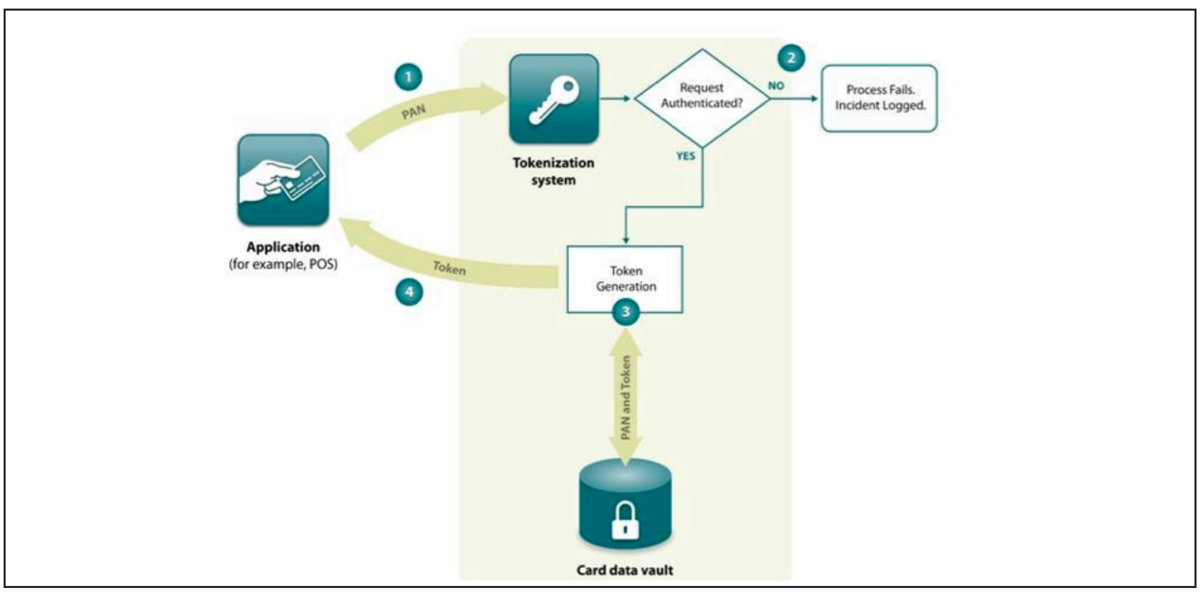
Recommendation 3: California retailers should implement appropriate tokenization solutions to devalue payment card data, including in online and mobile transactions.

Tokenization can eliminate the need to use real card data in storage and in post-authorization business processes. Tokenization is also a technology that can be used strategically to secure payment card data in CNP transactions. Like encryption, tokenization renders data unreadable and unusable by unauthorized persons and in many implementations, it offers operational advantages over encryption.

With tokenization, the PAN is replaced by a surrogate value, called a token, that is used like a reference number and that has no exploitable meaning or value. De-tokenization is the reverse process of redeeming a token for its associated PAN value. The security of a token depends on the infeasibility of determining the original PAN from the token and on the restricted usability of the token.[25]

Tokenization differs from encryption in that tokens are generated randomly rather than through a mathematically reversible algorithm. On a basic level, encryption results in a secret code that is very hard to break and tokenization results in a reference number (the token) that can be exchanged for a PAN.

Figure 11: Basic Tokenization Process



This diagram shows a basic tokenization process:

1) A consumer presents a payment card, along with authentication information (a signature or PIN) to a retailer point-of-sale terminal, which passes the PAN to a tokenization system.

2) The tokenization system sends the authentication information to the issuing bank, which verifies it. If the authentication fails (e.g., wrong PIN for the PAN), the incident is logged for monitoring.

3) If the authentication is successful, the tokenization system generates a token associated to the PAN and records both the PAN and the token in the card data vault.

4) The tokenization system returns the token generated to the requesting application (retailer), which can then store the token instead of the PAN.

In practice, the token value is used throughout the payment system, removing the PAN from a retailer's internal networks and isolating it to a central, highly secured server called the card data vault. The ability to retrieve the PAN from the card data vault in exchange for an associated token is restricted, dramatically decreasing the PAN's exposure throughout the processing system. Once a token is generated, it can be used as a replacement for the original PAN value during a transaction post-authorization. Accordingly, a retailer can store tokens in the retailer's payment environment instead of sensitive PANs. If there is a breach, the thieves only have access to tokens, which are valueless. Besides offering a powerful layer of security, tokenization solutions can simplify retailers' compliance with the PCI-DSS by limiting the amount of cardholder data stored in the retailer's payment environment.

Tokenization can be effective in CNP transactions. As face-to-face transactions become more secure with the use of chip cards, online, mobile and other CNP transactions are likely to become more vulnerable to fraud. Other countries that migrated to chip card technology saw fraud decrease in face-to-face transactions, but increase in CNP transactions. In the UK, while card-present fraud declined, CNP fraud increased from 30 percent of all card fraud to 62 percent in the six years following implementation of chip technology.[26] Tokenization can combat fraud in both face-to-face and CNP transactions. Further, many tokenization service providers offer unique tokenization solutions particularly appropriate to e-commerce environments.

Tokenization standards are being defined by the American National Standards Institute, the Payment Card Industry Security Standards Council and EMVCo.[27] Meanwhile retailers can find guidance on implementing tokenization from the Council, including on using tokenization to complement compliance with the PCI Data Security Standard.[28] In late July 2014, a coalition of retail industry groups expressed support for the creation of an open tokenization standard that can be supported by all networks, brands and payment types.[29]

Improving Retailer Response to Breaches of Payment Card Data

The first step in securing payment card data is installing robust security technology to devalue the data. Retailers must have a firm grasp on their overall security environment, including logging system access to detect possible attacks and breaches and being prepared to respond when one occurs. Even smaller retail businesses can be the target of data thieves and can experience data breaches as the result of sloppy employee practices. Our recent publication, *Cybersecurity in the Golden State*, is directed to smaller businesses.[30] It provides basic information on threats facing small businesses and practical steps to minimize vulnerability through a stronger security posture.

> **Recommendation 4:** California retailers should respond promptly to their data breaches and should notify affected individuals in the most expedient time possible, without unreasonable delay.

Like any business that collects personally identifiable information, retailers should have a plan in place for detecting and responding to a breach of their system that could permit unencrypted payment card data or other personal information to be acquired by an unauthorized person. A tested plan and a trained response team are essential to secure the system and provide notification "in the most expedient time possible and without unreasonable delay," as required by law. Because attackers move fast to monetize stolen card data, timely notification is particularly important in a payment card data breach.

The Attorney General's office takes timely notice very seriously. In one recent case involving the timing of a notification, the Attorney General arrived at a stipulated final judgment with Kaiser Foundation Health Plan, Inc. The Attorney General alleged that after an unencrypted USB drive containing over 20,000 Kaiser employee records was discovered at a thrift store, Kaiser should not have delayed notification for three months, but should have begun notifying employees earlier as their information was confirmed. Kaiser paid $150,000 in penalties and attorneys' fees, and agreed to provide notification of any future breach on a rolling basis and implement additional training regarding the sensitive nature of employee records.

Cybersecurity in the Golden State and other resources available on the Attorney General's web site provide recommendations on developing and implementing a breach response plan.[31]

Recommendation 5: California retailers should improve their substitute notices regarding payment card data breaches.

When a payment card data breach occurs in a retailer's system, the retailer must notify affected cardholders. Because most retailers do not have mailing addresses for their customers who pay by credit or debit card, they must use the substitute notice method. The method requires conspicuously posting a notice on the business's website, notifying major statewide media and providing notice by email where the business has an email address. Substitute notice is a permitted when a breach affects more than 500,000 persons, individual notices would cost more than $250,000 or the breached entity does not have sufficient contact information to send individual notices.

In a recent study, half or less of the recipients of breach notices from retailers reported being satisfied with the level of detail provided in the notices, while notices from other industry sectors were viewed more favorably in this regard.[32]

In addition to notifying promptly, retailers and other users of the substitute notice method can make their notice more effective by making it more likely that it will be noticed and by providing helpful information on what those affected can do to protect themselves. Better notices can also help to repair the customer relationship damaged by the breach. Measures for improving substitute notices could include the following:

1) Make the link to your notice conspicuous by putting it on the homepage of your website in a prominent place on the page (for example, at the top), labeling it clearly (for example, "Information on Security Incident") and making the link a font size and color that contrast with the background.

2) Leave the link and the notice page up for at least 30 days.

3) Put the notice up on your website as in the most expedient time possible after discovery of the breach and then update the information as you learn more about the breach. As soon as known, provide the time frame and the specific locations when card use exposed consumers to risk.

4) Tell affected consumers what they can do to protect themselves from the fraudulent use of the breached information. In breaches of Social Security numbers, credit-monitoring services can be helpful and a security freeze is even more effective. Credit monitoring does not, however, provide protection against the fraudulent use

of a payment card number. In such a case, a better suggestion is that consumers use online, email or text alerts from their bank to monitor activity on card accounts. For holders of debit cards, the safest step to take to protect their bank account is to cancel the card. (See Recommendation 6.)

Recommendation 6: California retailers and financial institutions should work together to protect debit cardholders in retailer breaches of unencrypted payment card data.

Another concern regarding payment card data breaches is the impact on consumer victims whose debit card accounts were breached. While the impact of any payment card data breach on consumer victims is generally less severe than that of a breach of Social Security numbers, such victims are burdened by monitoring their accounts, disputing fraudulent transactions and dealing with cancelled and replaced cards linked to automatic payments. Monitoring an account for suspicious transactions can be effective for credit card accounts, where federal law limits consumer liability and provides the right to dispute and not pay for unauthorized transactions while the dispute is under investigation by the card issuer.[33]

The situation is not the same with debit cards accounts, which operate differently and are subject to a different federal law.[34] Debit cardholders can find their bank accounts drained for a period of time. While a consumer is usually not liable for unauthorized debit card transactions, because the card is connected to the consumer's bank account, he or she may not have access to the stolen money until after the bank has completed an investigation. The amount for which a consumer is ultimately liable depends on how soon the consumer reports fraudulent transactions to the issuing bank.

While online account monitoring can provide an early warning of a fraudulent transaction on a debit account, the prompt cancellation of a breached debit card is the best way to protect consumers from the risk of having their back account drained, even if only temporarily. We recommend that retailers acknowledge the particular impact of a breach on debit cardholders and alert consumers to it in their breach notice, letting them know that cancelling the card is the safest thing to do.

We recognize that a retailer breach of payment card data can impose burdens on issuing banks and others in the payment card ecosystem. We encourage the parties to collaborate in seeking a fair and reasonable resolution, with the ultimate objective of protecting their mutual customers from harm.

Recommendations for the Health Care Sector

Recommendation 7: The health care sector should consistently use strong encryption to protect medical information on laptops and on other portable devices, and should consider it for desktop computers.

Most people consider their health information to be extremely sensitive data that should be accorded the most stringent protective measures. More than half the health care breaches in our set included Social Security numbers, which can be abused in many ways and against some of which consumers, including patients, have no effective defense strategies.

Medical identity theft, the fraudulent use of an individual's personal information in a health care setting to obtain medical services or goods, is a pernicious form of the crime that appears to be on the rise.[35] As explained in our publication *Medical Identity Theft: Recommendations for the Age of Electronic Medical Records*, victims of medical identity theft lack many of the rights and resources available to victims of financial identity theft and health care organizations do not all have the policies and procedures in place to prevent and respond to the problem.[36]

Health care breaches also affect many people, on average more than breaches in other industry sectors, with the exception of retail since the major outlier breaches of 2013. Many of the health care breaches reported to the Attorney General are of a type that could be prevented by the strategic use of strong encryption. Unlike other industry sectors, where Malware and Hacking breaches dominated, in health care 66 percent of the breaches reported in the past two years were the result of stolen or lost hardware or digital media. Nearly half of the health care breaches were desktops and laptops that were stolen not from employees' homes or cars, but from the workplace.

Breaches of this type are preventable. An affordable solution is widely available – full disk strong encryption, to the standard set by the National Institute of Standards and Technology. This is a lesson that must be learned by the health care industry and applied not only to laptops and portable media as we recommended in last year's report, but also to computers in offices. The desktop computer in an office can be encrypted when shut down at night and decrypted in the morning. If someone should break in after hours and steal the computer, the data on it would not be accessible. Even small practices that lack full-time information security and IT staff can do this. They owe it to their patients to do it now.

Recommendations for All Industry Sectors

The following recommendations are directed to all businesses, government agencies and other organizations that collect, maintain or use personal information.

Recommendation 8: Organizations should conduct risk assessments at least annually and update privacy and security practices based on the findings.

Rapidly developing technologies, new business practices and evolving cybercrime mean that organizations must regularly review and update their privacy and security policies and practices. Privacy risk assessments, conducted at least annually, enable an organization to identify external threats and internal vulnerabilities that put personal information at risk and permit the determination of additional controls needed.

One critical component of an effective data protection program must be the training of employees and also of service providers who handle personal information for their clients. Nearly one fifth of the data breaches reported resulted from employees or service providers unintentionally doing the wrong thing: mailing documents with Social Security numbers exposed, publicly posting sensitive information online, sending mail or email to the wrong place. Other preventable breaches are the result of leaving unencrypted laptops in cars or sending unencrypted thumb drives with sensitive information through the mail.

Wherever possible, this type of vulnerability should be controlled with technology, such as full disk encryption on portable computers or with procedural changes, such as not printing Social Security numbers on documents sent through the mail. Regardless of technological controls, employees can strengthen or weaken an organization's privacy posture, and individual employee actions are the key to making strong privacy practices a reality. Regular training in the right way to handle personal information is just the beginning of building a company culture that the respects the privacy of those who entrust it with their information.

Recommendation 9: Organizations should use strong encryption to protect personal information in transit.

Echoing a finding in the 2012 report, we continue to see breaches that could be prevented by the strategic use of strong encryption, particularly for data that is being sent by email or in transit on laptops or portable media. While encrypting data at rest can often pose usability challenges, this is not the case for data being moved outside the network on a device or in an email. To be effective, full disk encryption of all portable devices and media is preferable to protecting only those known to be used for sensitive information or to allowing users to choose what data to encrypt on the devices.

We recommend amending current California 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 for Technology's standard approved for U.S. Government organizations to protect higher risk information.

Recommendation 10: Organizations should improve the readability of their breach notices.

Breach notices continue to be written at the college level, well above the average reading level for adults.[37] The intent of the breach notice law is to alert individuals that their information is at risk, so they can take steps to protect themselves. Notices that can be easily understood are obviously essential to accomplishing this purpose.

While concerns about litigation risks may cause companies to draft notices in legalistic language that is less than accessible, we encourage companies to work with communications professionals to improve the clarity of their notices. Good writing can make the notices more readable, using techniques such as shorter sentences, familiar words and phrases, the active voice and a layout that supports clarity.

Legislative Recommendations

These recommendations are offered to California Legislature.

Recommendation 11: Consider legislation to amend the breach notice law to strengthen the substitute notice procedure, clarify the roles and responsibilitities of data owners and data maintainers and require a final breach report to the Attorney General.

Substitute Notice Procedure

Substitute notices tend to be less effective in reaching those affected by a data breach than the standard mailed notices. The breach notice law allows the use of a substitute notice in certain situations: when the cost of providing notice would exceed $250,000 or the number to be notified exceeds 500,000 or the entity required to notify does not have sufficient contact information for individual notices.

The substitute notice procedure requires three things: 1) conspicuously posting the notice on the entity's website, 2) notifying major statewide media and 3) providing notice by email where the business has an email address.

The substitute notice method should be improved by requiring a breached entity to make the notice more conspicuous on its website and to leave it up for a specified period of time.

Roles and Responsibilities of Data Owners and Data Maintainers

Under the current law, owners and maintainers of breached data have differing responsibilities. The law requires owners or licensees of data in a system that has been breached to notify the victims (data subjects) in the most expedient time possible and without unreasonable delay. A maintainer of data is required to notify the data owner immediately upon discovery of a breach of the data maintainer's system. The law does not define "owner" or "maintainer," but the difference in the notification obligations implies that it is the data owner who is responsible for notifying data subjects, although the cost and logistics of making the notification is often contractually imposed by the owner on a maintainer, such as a service provider. In some cases, notification may be delayed as parties debate about who should be considered the data owner and who the maintainer. Clarifying the roles by defining the two terms in the law would lead to more timely notification in such circumstances.

Final Breach Report to the Attorney General

The breach notice law currently requires breached entities subject to the law to submit to the Attorney General's office a sample copy of the notice provided to affected individuals. We review the notices, post them on our website and usually request additional information at the time of submission. If companies were required to provide a final investigative report upon completion of their internal investigation, including corrective actions taken, we would be able to gain a deeper understanding of the nature of the vulnerabilities that can result in a breach and could provide better recommendations for protecting California residents.

Recommendation 12: Consider legislation to provide funding to support system upgrades for small California retailers.

As banks continue to issue chip cards, retailers should invest in the upgraded point-of-sale terminals and software needed to enable the machines to read the chip. Without these upgrades, consumers will remain vulnerable even when they are using chip cards. While larger retailers are on track to upgrade in advance of the October 2015 liability shift, many smaller retailers are not. The cost of upgrading has deterred them from moving rapidly. When the liability shift occurs, retailers that have not implemented the new technology will face liability that could destroy a small business. These smaller businesses need financial assistance and support to upgrade their systems so they can protect their customers, their reputations and their livelihood.

Appendix

Report Methodology

The Attorney General's office analyzes the data breaches reported to us in order to gain an understanding of the types of incidents that are occurring and the vulnerabilities and threats they may reveal. We seek to identify patterns and trends and to recommend data protection strategies and practices that can reduce the risk of breaches and mitigate their harmful impact.

To facilitate our analysis, we describe and classify breaches in a number of ways, primarily by industry sector and by breach type. For industry sectors, we classify the organization that experienced the breach according to the U.S. Census Bureau's North American Industry Classification System.[38]

For breach type, in this report, we adopted some of the terminology of the VERIS (Vocabulary for Event Recording and Incident Sharing) Framework developed by Verizon in 2010.[39] We adopted the VERIS model in order to facilitate the comparison of our data with other reports that use the model. Because of limitations in our knowledge of the details of some breaches, we did not use the full spectrum of VERIS categories. We also translated the taxonomy used in our 2012 report[40] into the VERIS categories used in the 2013 report to enable analyses of the full set of breaches.

2012 Breach Types	2013 Breach Types
Physical Failure: Loss of control over physical asset (document, media, hardware) containing personal information.	**Physical Theft and Loss:** Deliberate threats that involve proximity, possession, or force, including theft, tampering, snooping, sabotage, local device access, assault, etc.
Logical Failure: Outsider Intentional access to information without access to the physical, asset by the exploitation of vulnerability by an outside attacker.	**Malware and Hacking:** Malware encompasses any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent. Examples include viruses, worms, spyware, keyloggers, backdoors, etc. Malware is defined as all attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms. Includes brute force, SQL injection, cryptanalysis, denial of service attacks, etc.

2012 Breach Types	2013 Breach Types
Logical Failure: Insider Intentional unauthorized access by an insider to information without control of the physical asset.	**Misuse:** The use by insiders or trusted partners of organizational resources or privileges for any purpose or manner contrary to what was intended. Includes administrative abuse, use policy violations, use of non-approved assets. These actions can be malicious or non-malicious in nature.
Procedural Failure: Mishandling of personal information by data custodians (unintentional web site exposure, misdirected mailing, improper disposal), exposing it to unauthorized parties.	**Errors:** Anything done (or left undone) incorrectly or inadvertently. Includes omissions, misconfigurations, programming errors, trips and spills, malfunctions. It does not include something done (or left undone) intentionally or by default that later proves to be unwise or inadequate. (In this report we include the single incident described as resulting from a phishing exploit in this category, as a failure to follow organizational policies.)

California Data Breach Notification Statutes

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.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been

breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (i) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(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 either of the following:

(1) 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:

(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.

(E) Health insurance information.

(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(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) Email notice when the agency has an email 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 Department of Technology.

(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.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, "agency" includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.

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.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in subdivision (j) or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(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 either of the following:

- (1) 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:
  - (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.
  - (E) Health insurance information.
- (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(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) Email notice when the person or business has an email 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.

(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.

Notes

[1] Javelin Strategy & Research, *2014 Data Breach Fraud Impact Report* (June 2014), p. 7, available at *www.javelinstrategy.com*.

[2] Ponemon Institute, *Fourth Annual Benchmark Study on Patient Privacy and Data Security* (Mar. 2014), pp. 2-3, available at *www.ponemon.org*.

[3] California Penal Code section 530.5.

[4] Javelin Strategy & Research, *2014 Identity Fraud Report* (Feb. 2014), p. 4, available from *www.javelinstrategy.com*.

[5] Javelin Strategy & Research, *Payment Card Data Security Report* (Nov. 2013), p. 6, available from *www.javelinstrategy.com*.

[6] *Supra* note 1.

[7] *Supra* note 1. The cost figures are based on data from breach victims for the past six years.

[8] National Intellectual Property Rights Coordination Center, *Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad* (Nov. 2011), p. v; United Nations Interregional Crime and Justice Research Institute, *Confiscation of the Proceeds of IP Crime* (Apr. 2013), p. 9.

[9] Indictment, UNITED STATES V. DRINKMAN ET AL., No. 1:09-cr-00626 (D.N.J. 2009), p. 16.

[10] California Attorney General, *California and the Fight Against Transnational Criminal Organizations* (Mar. 2014), available at *www.oag.ca.gov/transnational-organized-crime*.

[11] The complete text of the breach notice statutes, California Civil Code sections 1798.29 and 1798.82, can be found in the Appendix to this report.

[12] SB 46 (Corbett) of 2013 amended both Civil Code section 1798.29 and section 1798.82, regarding breaches of online account credentials.

[13] AB 1710 (Dickinson and Wieckowski) of 2014 amended Civil Code section 1798.82, regarding identity theft prevention and mitigation services. The bill did not make a similar amendment to Civil Code section 1798.29, the breach notice statute applying to state and local government agencies.

[14] AB 1710 (Dickinson and Wieckowski) of 2014 amended Civil Code section 1798.81.5 to include businesses that maintain personal information about California residents in the requirement to implement and maintain reasonable and appropriate security measures to protect the information.

[15] See the *National Assessment of Adult Literacy,* available at *http://nces.ed.gov/naal/*.

[16] *Supra* note 1, p. 25.

[17] The Flesch-Kincaid Grade Level index is one way to measure how difficult a text is to understand. The formula considers the average number of words per sentence and the average number of syllables per word within a given passage. The results are then converted into a score that roughly equates with a grade level in the United States. See *www.readabilityformulas.com/flesch-grade-level-readability-formula.php*.

[18] In making these recommendations, we recognize the limitations of our sample and of our knowledge of the details of some of the incidents.

[19] *Supra* note 1.

[20] The term EMV comes from the names of Europay International (acquired by MasterCard in 2002), MasterCard and Visa, which originally established the standard for chip card technology in 1994. The standard is now managed by EMVCo, a joint venture of MasterCard, Visa, JCB and American Express.

[21] Douglas King, Retail Payments Risk Forum, *Chip-and-PIN: Success and Challenges in Reducing Fraud* (Jan. 2012), p. 6, available at *www.frbatlanta.org*.

[22] Chase Paymentech, *EMV: The New Way to Pay*, p. 5, available at *www.chasepaymentech.com/documents/emv_chip_technology.pdf*. See also Smart Card Alliance, *EMV Chip Payment Technology FAQs*, available at *www.smartcardalliance.org/resources/pdf/EMV-FAQ-update-012814.pdf*.

[23] Payment Security Task Force, *More Than 575 Million U.S. Payment Cards to Feature Chip Security in 2015*, (Aug. 13, 2014), available at *www.businesswire.com/news/home/20140813005329/en/575-Million-U.S.-Payment-Cards-Feature-Chip#.U-tfB9NqxAU.*

[24] First Data, *Avoiding a Data Breach: An Introduction to Encryption and Tokenization* (Aug. 2014), available at *www.firstdata.com*.

[25] PCI Security Standards Council, *Information Supplement: PCI DSS Tokenization Guidelines* (Aug. 2011), p. 3, available at *www.pcisecuritystandards.org*.

[26] *Supra* note 21, p. 8.

[27] The ANSI tokenization standard is being defined as ANSI X9.119 Part 2; see *www.ansi.org*. The EMVCo tokenization standard, *EMV Payment Tokenisation Specification – Technical Framework* (Mar. 2014), is available at *www.emvco.com/specifications.asp?id=263*. The PCI Security Standards Council's PCI DSS *Tokenization Guidelines* (Aug. 2011) is available at *www.pcisecuritystandards.org*.

[28] *Id. PCI DSS Tokenization Guidelines*.

[29] Retail Industry Leader Association, *Merchant Industry Coalesces Behind Open Process for Security Standards to Better Protect U.S. Consumers and Business from Cybercriminal Activity* (Jul. 2014), available at *www.rila.org/news/topnews/Pages/Merchant-Community-Coalesces-Behind-Open-Process-for-Security-Standards-to-Better-Protect-U.S.-Consumers.aspx*.

[30] California Attorney General, *Cybersecurity in the Golden State: How California Businesses Can Protect Against and Respond to Malware, Data Breaches and Other Cyberincidents* (Feb. 2014), available at *www.oag.ca.gov/privacy/business-privacy*.

[31] *Id.* See also: California Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* (Jan. 2012), available at *www.oag.ca.gov/privacy/business-privacy.*

[32] *Supra* note 1.

[33] The Truth in Lending Act, 14 USC 1601 et seq.

[34] The Electronic Funds Transfer Act, 15 USC 1693 et seq.

[35] Ponemon Institute, *2013 Survey on Medical Identity Theft* (Sep. 2013), available at *www.ponemon.org*.

[36] California Attorney General, *Medical Identity Theft: Recommendations for the Age of Electronic Medical Records* (Oct. 2013), available at *www.oag.ca.gov/privacy/business-privacy*.

[37] 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 the eighth grade. The National Assessment of Adult Literacy is administered by the National Center for Education Statistics in the Department of Education. An overview of the 2003 assessment is available at *http://nces.ed.gov/naal/kf_demographics.asp*.

[38] The North American Industry Classification System (NAICS) sectors represented in the breach data are Retail, Finance and Insurance, Health Care, Professional Services, Government (Public Administration), Hospitality (Accommodation and Food Service), Education and Other. The Other category includes, agriculture, utilities, manufacturing, wholesale trade, transportation, real estate and waste management, each of which subcategories accounted for eight or fewer incidents in 2013. The most recent version of the NAICS is available at *www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012*.

[39] VERIS (Vocabulary for Event Recording and Incident Sharing) is a taxonomy designed to provide a common language for describing security incidents. Information on VERIS can be found at *http://veriscommunity.net/.*

[40] The *2012 Data Breach Report* classifies breaches according to the taxonomy developed by Matthew Curtin and Lee T. Ayers. See Curtin and Ayres, *Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry, 4 I/SJLP* 525-922 (2008), 569-601.

California Department of Justice
Privacy Enforcement and Protection Unit

www.oag.ca.gov/privacy