Byte by Byte: Is Our Personal Data Really Safe and Secure? A Review of the Recent Retail Data Attacks

Prepared by Staff Counsel of the
Assembly Committee on the Judiciary[1]
February 18, 2014

"We live in an increasingly connected world, and information is the new currency. Businesses in this data-driven economy are collecting more personal information about consumers than ever before, and storing and transmitting across their own systems as well as the Internet. But, as recent publicly announced data breaches remind us, these vast systems of data are susceptible to being compromised. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harms to consumers as well as businesses."

- Statement of the Federal Trade Commission [2]

"Data breaches are a fact of life in the United States."

- Mallory Duncan of the National Retail Federation [3]

Introduction and Summary

On December 19, 2013, Target Corp. announced that approximately 40 million credit and debit card accounts that had been used at its brick and mortar stores were compromised as part of a massive data breach that took place in late 2013.[4] On January 10, 2014, Target revealed that additional consumer information including customer addresses and telephone numbers regarding 70 million individuals had also been stolen. And its chief financial officer John Mulligan subsequently testified to Congress that this extraordinarily large trove of data could may have included personal data purchased from a third party on individuals who were not Target customers, .[5] A similar breach of customer payment information was also announced by Neiman Marcus following an apparent data attack that occurred earlier last year, affecting approximately

[1] Staff counsel are indebted to the excellent research assistance provided by our legal intern Vignesh Ganapathy.
[2] Testimony before the Committee On Energy And Commerce Subcommittee On Commerce, Manufacturing, And Trade United States House Of Representatives February 5, 2014.
[3] Quoted in the New York Times, "Sidestepping the Risk of a Privacy Breach," 2/7/13. http://www.nytimes.com/2014/02/08/your-money/sidestepping-the-risk-of-credit-and-debit-card-fraud.html?_r=0)
[4] Target Corp. Press Release of December 19, 2013 at http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores
[5] Target Corp. Press Release of January 10, 2014 at http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance; "Can data breaches be prevented? Congress and companies answer: For now, no," Melinda Henneberger, *The Washington Post*, February 5, 2014.

1.1 million accounts.[6] If that were not enough, on January 25, 2014, Michaels Stores, Inc. notified its customers of a possible data breach, though its severity remains unknown.[7]

This is not the first time such massive data breaches have occurred in the United States.[8] The modern era of retail data breaches can be dated to at least 2007, when more than 45 million T.J. Maxx and Marshall's customers lost their personal data as the result of a massive breach. In August, 2008, then-U.S. Attorney General Michael Mukasey announced indictments against an international ring of computer hackers who had allegedly obtained information on more than 40 million debit and credit card accounts from at least nine American retailers. According to a Javelin Strategy and Research report, credit card fraud has increased 87 percent since 2010, culminating in aggregate losses of $6 billion nationwide.[9] For the year 2013 alone, Verizon found that there were more than 600 publicly disclosed data breaches.[10] A report cited in a recent *Sacramento Bee* article stated that 740 million records were "compromised" in 2013 alone.[11]

Whatever the numbing total number may be, it seems evident that the theft of sensitive consumer data is a significant, growing and recurring problem that damages consumers, retailers and the financial services industry. More importantly, it appears that despite the potential promise of improved safeguards, experts agree that further breaches of confidential consumer information are inevitable for both brick and mortar retailers and Internet businesses. Indeed, just this past week the *Washington Post* reported that:

> No technology is fail-safe. Just ask PayPal President David Marcus. Marcus said hackers probably cloned his credit card during his recent trip to the United Kingdom, even though the card was outfitted with chip technology that makes it harder to replicate plastic. He explained in a series of tweets Monday that there were a "ton of fraudulent transactions" on his card. Marcus suspects his card was compromised at a hotel through a skimmer — a device thieves hide inside card readers to capture credit and debit information when people swipe cards.[12]

Thus if the question presented for the Legislature is whether our personal data is secure, the answer appears to be that it is not, and it may well be that it can never be made fully secure. Indeed, experts warn that further data breaches caused by the same malicious software that infected Target and other retailers should be expected, to say nothing of the many other data

---

[6] Neiman Marcus Group Press Release at http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat

[7] Hayley Tsukayama, *Michaels discloses possible customer data breach; Secret Service investigating*, Washington Post, http://www.washingtonpost.com/business/technology/michaels-discloses-possible-customer-data-breach-secret-service-investigating/2014/01/27/73a8538e-877c-11e3-a5bd-844629433ba3_story.html (Jan. 26, 2014).

[8] It is also not the first time that Assembly Committees have held hearings on the issue in response to a well-publicized breach. See, for example, *Disclosure Requirements Under the California's Breach Notification Law*, prepared for Hearing of the Assembly Judiciary Committee, November 19, 2008 (held in response to breaches at TJ Maxx, BJ's Wholesale Club, DSW, Inc., and Dave and Buster's Inc., among others.)

[9] https://www.javelinstrategy.com/brochure/254

[10] Cited in statement Of Senator Patrick Leahy (D-Vt.), Chairman, Senate Judiciary Committee Hearing on "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." February 4, 2014.

[11] Claudia Buck, *Tiny chip can make bank card smarter,"* Sacramento Bee February 5, 2014.

[12] The Washington Post, "PayPal president punches holes in chip-card conversion argument," Danielle Douglas, February 12, 2014.

vulnerabilities, and the continuing ability of cyber thieves to adapt to changing security technologies.

This conclusion raises a number of critical policy issues. Retailers and credit card issuers may now appropriately spend millions of dollars to adopt the "chip and PIN" technology in use elsewhere around the world, which may help prevent the future "cloning" of stolen payment card numbers. But such technology enhancements still may not in the longer run prevent the type of recent data breaches or reduce the risk of data thefts as cyber thieves catch up with the changing security enhancements.

In addition, the current focus on "chip and PIN" security enhancements reportedly would not help fend off data attacks via the fast-growing Internet marketplace where online transactions do not rely on the physical presentation of a payment card. As a percentage of total sales, online retail sales have quadrupled since 2004, and nearly doubled since the end of the recession. Over time, the greatest threat to consumer data protection may come from data that was transmitted via the Internet rather than data supplied in person at brick-and-mortar retail outlets.[13]

Moreover, the potential availability of more secure credit cards for in-person transactions would not address the breach of other personal information, such as the unencrypted addresses and phone numbers lost in the Target breach. Requiring encryption of such data might have been helpful, although security experts note that encryption comes in a variety of strengths, and decryption codes can be lost along with data.

As the Federal Trade Commission and others have noted, personal data is the new currency of many businesses. Thus far many businesses have strenuously resisted any suggested limits on the type, amount, or duration of the personal information they can collect and maintain. Nevertheless, if we cannot build a safe deposit box that is invulnerable to cracking, nor protect the keys to that safe, the best alternative may well be to limit the potential harm by reducing the type of valuable assets that go into the box -- or at least the length of time those assets may be held. If not, it seems reasonable for policy-makers to ask: In the absence of reasonable limitations on the receipt and storage of consumer data to minimize harm, should not those who lose control of this sensitive information be held accountable for all the resulting damages?

I. RECENT CONSUMER DATA BREACHES AT MAJOR RETAILERS

What Occurred In The Recent Payment Card Breaches? Multiple press reports, beginning in mid-December of 2013 and continuing into the New Year, treated American consumers to the sobering discovery that hackers had stolen credit card account numbers and other pieces of personal information from tens of millions of shoppers at Target, Neiman Marcus, and Michaels, among other retailers, in the latter part of 2013. By the time hearings were held before committees of Congress earlier this month, a clearer picture of what had occurred began to take shape.

[13] Census Bureau, U.S. Department of Commerce, Quarterly Retail E-Commerce Sales (3rd Quarter 2013).

This much seems to be widely agreed upon:[14] Cyber criminals, possibly based in Eastern Europe, accessed the retailers' internal computer networks and installed malicious software (malware) on the point-of-sale (POS) card-swiping devices at Target and Neiman Marcus. Although a similar breach appears to have occurred at the arts and crafts retailer, Michaels, the details of that breach have not been made public. The source of the malware in the Target case is allegedly a Russian teenager who sold the malicious program to the attackers who entered the retailers' computer systems by trying several easy passwords to access the POS system remotely.[15] Recent media reports indicate that the initial intrusion at Target has been traced back to network access permission that was obtained from a small Pennsylvania subcontractor that has managed the HVAC systems for a number of Target stores.[16]

Described variously as "memory-parsing" or "RAM-scraping" software, the hackers reportedly used the malware to capture account information from 40 million credit or debit cards used at Target, and another 1.1 million credit cards used at Neiman Marcus. The malware installed at Target apparently collected data between November 27 and December 15, 2013. Thefts at Neiman Marcus occurred over a longer period of time, reportedly from July 16 to October 30, 2013. As yet there is no evidence that the same group of hackers was involved in both attacks, but the timing and methods at least suggest this possibility.

Although the technical details of the breach reportedly vary somewhat from source-to-source, it appears that the "memory parsing" or "RAM scraping" software used in the Target and Neiman Marcus attacks gathered credit and debit card account numbers, expiration dates, three-digit security codes and, (in the case of debit cards) personal identification numbers (PINs). The malware skims this data as (or immediately after) the POS device reads it from the card's magnetic stripe. Even where the data on the magnetic stripe is encrypted, the payment card account information is at least momentarily "decrypted" and is stored as "plain text" in the POS memory. It is apparently during this critical period that the malware captures unencrypted plain text information. The malware then generates a file that stores the data temporarily within the retailer's own network before sending it to an outside computer server and, eventually, to a system controlled by the cyber thieves. Investigators, at least at this point, reportedly believe that the operation that breached Target is located in Ukraine, while the location of the Neiman Marcus hackers has apparently not been determined.

As described in a recent background paper by a Congressional committee, this type of malware reportedly first appeared about a decade ago, according to security experts, and has been improved incrementally by cyber criminals over the years such that it is now difficult for anti-

[14] Much of the summary in this section is drawn from the following sources unless otherwise noted: "What is Known About U.S. Card Breaches," *The Nilson Report*, January 2014; the following statements made before the U.S. Senate Committee on Judiciary hearings on "Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime." In particular, see the statements of Delara Derakhshani, Consumers Union; Fran Rosch, Symantec; William Noonan, U.S. Secret Service; Michael Kingston, CIO of Neiman Marcus; John Mulligan, CFO of Target; Edith Ramirez, Federal Trade Commission; and Mythili Raman, Department of Justice. These statements may be accessed at
http://www.judiciary.senate.gov/hearings/hearing.cfm?id=138603a26950ad873303535a6300170f&2

[15] Security firm IntelCrawler says it has identified Target malware author, Washington Post, 1/17/13 (http://www.washingtonpost.com/business/technology/security-firm-intelcrawler-says-it-has-identified-target-malware-author/2014/01/17/258efa48-7fa4-11e3-9556-4a4bf7bcbd84_print.html)

[16] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

virus software to detect its presence. The software also is relatively inexpensive, making it widely accessible to would-be hackers. A version of the malware used in the Target attack which has surely resulted in substantial costs to the company – dubbed Kaptoxa – reportedly sold for a mere $2,000 on the black market earlier in 2013.[17]

Loss of Personal Information in Addition To Payment Card Data. In addition to the theft of the credit card account information acquired through the POS system, once the malware had been installed on the Target computer network the hackers were also reportedly able to capture the personal information of 70 million consumers stored in Target's internal marketing database. This information was apparently not encrypted. According to media reports, data from this source included consumer contact information, including names, addresses, e-mail addresses, and telephone numbers, as well as potentially some personal information about individuals who were not Target customers that may have been purchased by Target from third parties.[18] There is no indication that personal contact information was stolen from Neiman Marcus.[19]

How Likely Is It That Consumer Data Breaches May Recur? While some observers have criticized Target for allegedly lax computer security,[20]others have noted the increasing sophistication of computer malware that can avoid detection and is quickly modified to evade security defenses.[21] Whatever the details of the recent data breaches, they follow many other prominent data breaches, including the well-known incident involving TJ Maxx in 2007 noted earlier, and experts appear to agree that more such breaches should be expected. Only 11 percent of businesses have adopted industry standard security measures, according to a recent report by Verizon Business Solutions, and outside experts say even these "best practices" fall short of what is needed to defeat aggressive hackers lured by the prospect of a multimillion-dollar heist.[22]

A recent Congressional hearing focused on the question whether data breaches can be prevented, the short answer was: no.[23] According to media reports, the rash of attacks against Target and other top retailers is likely to be the leading edge of a wave of serious cybercrime, as hackers become increasingly skilled. Nearly two dozen companies have been hacked in cases similar to the Target breach and more almost certainly will fall victim in the months ahead, the FBI recently warned retailers. The names of all of the compromised firms have not been revealed, nor

[17] U.S. House of Representatives Committee on Energy and Commerce (Feb. 3, 2014) http://docs.house.gov/meetings/IF/IF17/20140305/101714/HMTG-113-IF17-20140305-SD002.pdf
[18] "Can data breaches be prevented? Congress and companies answer: For now, no," Melinda Henneberger, *The Washington Post*, February 5, 2014.
[19] *See e.g.* Symantec, *A Special Report on Attacks on Point of Sales Systems,* February 3, 2004. A copy of the report is available on U.S. Senate Judiciary Committee website, supra note 9.
[20] "A Sneaky Path Into Target Customers' Wallets," New York Times, Jan. 18, 2014 (http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html); *See also* https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[21] U.S. House of Representatives Committee on Energy and Commerce (Feb. 3, 2014) http://docs.house.gov/meetings/IF/IF17/20140305/101714/HMTG-113-IF17-20140305-SD002.pdf
[22] Experts warn of coming wave of serious cybercrime, Washington Post, Feb. 9, 2014 (http://www.washingtonpost.com/business/economy/target-breach-could-represent-leading-edge-of-wave-of-serious-cybercrime/2014/02/09/dc8ea02c-8daa-11e3-833c-33098f9e5267_story.html)
[23] "Can data breaches be prevented? Congress and companies answer: For now, no, Washington Post, 2/5/13 (http://www.washingtonpost.com/business/economy/can-data-breaches-be-prevented-congresss-and-companies-answer-for-now-no/2014/02/05/94d607ae-8e9d-11e3-b46a-5a3d0d2130da_story.html)

is it clear how many shoppers have had their credit card numbers and other personal data stolen.[24] The computer security firm IntelCrawler said it expects more retailers to announce that their systems were breached, because more than 60 versions of the malware have been sold to cybercriminals overseas.[25] A three-page memo from the Federal Bureau of Investigation, titled "Recent Cyber Intrusion Events Directed Toward Retail Firms" and distributed to retailers on January 17, said that 20 U.S. retailers were compromised by the malware in 2013. The FBI memo reportedly said, "We believe POS malware software crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it."[26]

Personal Data Is The New Currency, And Experts Agree it is Vulnerable to Theft. Attacks on the POS systems of brick-and-mortar retailers are only one example of a much larger issue that includes many businesses, including Internet retailers, credit reporting companies, data brokers and others who collect and store sensitive personal information. As noted above, the Federal Trade Commission recently testified before Congress that hackers and others will continue to seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and potentially misuse it in ways that can cause serious harms to consumers as well as businesses.[27]

Others at the Congressional hearings opined similarly. "The innovations that are driving the industry forward and presenting consumers with exciting new methods of making purchases is also rapidly expanding beyond the bounds of our existing regulatory and consumer protection regimes," said James A. Reuter, speaking on behalf of the American Bankers Association. "And, as has historically been the case, the criminals are often one step ahead as the marketplace searches for consensus." William Noonan of the Secret Service echoed this sentiment in his testimony, noting the rapid increase in the number of criminals trying to acquire financial information and the sophistication of their methods.

Are There Ongoing Risks To Businesses And Consumers From Use of Credit Card Information? To say breaches of credit card information are potentially costly for banks and card issuers is an increasing understatement. They are currently responsible for paying for fraud under current federal law and bear the cost of reissuing compromised credit cards, as Citibank and JP Morgan Chase have recently done following the Target breach. The Consumer Bankers Association, a trade group, says that more than 15.3 million credit and debit cards have been reissued as a result of the Target breach at a cost of $153 million. The Javelin Strategy & Research consulting firm estimates the total damage to banks and retailers could exceed $18 billion.[28] According to

[24] "Experts warn of coming wave of serious cybercrime," Washington Post, Feb. 9, 2014
[25] Security firm IntelCrawler says it has identified Target malware author, Washington Post, 1/17/13 (http://www.washingtonpost.com/business/technology/security-firm-intelcrawler-says-it-has-identified-target-malware-author/2014/01/17/258efa48-7fa4-11e3-9556-4a4bf7bcbd84_print.html)
[26] Target security breach: Eric Holder vows to find hackers, Washington Post, 1/29/13 http://www.washingtonpost.com/business/economy/holder-pledges-to-hunt-down-thieves-in-target-breach/2014/01/29/6f97517a-8900-11e3-833c-33098f9e5267_story.html; Nilson Report, "What is Known About U.S. Card Breaches?" (http://www.nilsonreport.com/publication_the_current_issue.php)
[27] Statement of the Federal Trade Commission before the Committee On Energy And Commerce Subcommittee On Commerce, Manufacturing, And Trade United States House Of Representatives February 5, 2014 (http://www.ftc.gov/system/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-consumer-information-can-data-breaches-be/140205databreaches.pdf)
[28] http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html

reports, the Neiman Marcus breach has already caused at least 2,400 fraudulent transactions.[29] There has been no announcement regarding the number of fraudulent transactions tied to the Target breach.

The ongoing risks from the loss of credit card data arise from the potential use of the credit card account information to either (1) purchase goods online or by phone ("card-not-present" fraud) or (2) create counterfeit credit cards with the information placed on a magnetic stripe. Both the credit card account numbers and the counterfeit cards can be sold on an apparently thriving black market. Indeed, it appears that some of the recently hacked card numbers have already appeared on the black market. For example, according the Nilson Report, the U.S. Secret Service noticed a spike in the number of credit and debit accounts for sale on the Internet in early December 2013. In addition, federal authorities reportedly arrested two Mexican citizens in Texas who were in possession of 96 counterfeit cards, apparently with numbers tied to Target data breach.[30]

More than 70 class action lawsuits, mostly against Target, have reportedly been filed to date, including many by banks and credit unions who may have a stronger case for damages than do consumers, in part because as noted banks typically reimburse customers for any fraudulent charges on stolen cards, and because banks suffer uncompensated expenses associated with canceling and reissuing cards, and lost interest and fees. Some of these cases have been filed in Target's home state of Minnesota where a state law prohibits businesses from retaining "the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data" of its customers past a certain period.[31] If a security breach occurs due to a violation of the statute, the business must reimburse costs incurred by any financial institution that issued those cards, according to the banks.[32]

Data Breach Insurance Policies. Following the massive TJ Maxx data breach of 2007, many companies reportedly began to obtain new insurance policies that protect against data breach. According to news reports, at the time of the 2013 holiday season data breach Target Corp. had $165 million in insurance coverage that could be used to pay claims on the breach, including $100 million in cyber insurance and $65 million in directors and officers liability coverage.[33] Such polices may cover, among other things, forensic services, liability expenses, including defense costs, notification expenses, crisis management and public relations costs. While some businesses may have insurance to cover these losses, all consumers inevitably pay these costs when businesses and insurers pass such costs along in the form of higher prices. As discussed below, however, consumers by contrast largely reportedly do not have similar access to effective insurance products to protect against the theft of their personal data.

---

[29] Target security breach: Eric Holder vows to find hackers, Washington Post, 1/29/13 http://www.washingtonpost.com/business/economy/holder-pledges-to-hunt-down-thieves-in-target-breach/2014/01/29/6f97517a-8900-11e3-833c-33098f9e5267_story.html;

[30] Nilson Report, January 2014. *See also* testimony of William Noonan, *supra* note 9.

[31] Banks Targeting Target, National Law Journal, Feb. 3, 2014 (http://www.nationallawjournal.com/id=1202640955981/Banks-Targeting-Target?slreturn=20140103125015

[32] MN Statutes, chapter 325E, section 64. Available at https://www.revisor.mn.gov/statutes/?id=325E.64

[33] Sital S. Patel, *Target could tap $165 million in insurance to pay cyberbreach claims*, MarketWatch (Jan. 21, 2014), available online at http://blogs.marketwatch.com/thetell/2014/01/21/target-could-tap-165-million-in-insurance-to-pay-cyberbreach-claims

II. PROMISE AND PROSPECT OF NEW SECURITY TECHNOLOGIES

An accompanying background paper prepared for this hearing by the staff of the Assembly Committee on Banking and Finance effectively discusses in much more detail the retail payment system, voluntary industry data security standards, the security issues presented by existing credit card magnetic stripes, and the potential costs and benefits that may be offered by the adoption of so-called "chip and PIN" or the less-protective "chip and signature" technology that many retailers and financial services companies have pledged to pursue. These issues are critical because more than $3 trillion in U.S. customer transactions reportedly take place each year through the point-of-sale (POS) systems infiltrated by the hackers, according to the Nilson Report, a California-based industry newsletter.

Importantly, however, whether or not the adoption of these technologies might prevent the type of retail POS scams at issue in the recent breaches, commenters have noted that it will do nothing to prevent the many other significant types of consumer data breaches – such as the loss of customer information that occurred in the Target breach, which may be especially damaging if the customer data can be connected with credit card data – as well as the potential for credit card and other data breaches involving other types of businesses, including online retailers. According to the Privacy Rights Clearinghouse, there have been a significant number of consumer data breaches by companies other than brick-and-mortar retailers that have exposed consumers to identity theft. In fact, some experts are predicting that the adoption of microchip technology is likely to inadvertently shift retail transaction fraud away from brick-and-mortar retailers to e-commerce, because this technology does not deter fraudulent use of credit card numbers when the card is not presented in person.[34]

III. IF DATA CANNOT BE PROTECTED FROM BREACH, CAN THE RISKS TO CONSUMERS BE REDUCED BY BETTER PREVENTATIVE MEASURES OR IMPROVED REMEDIES?

Identity Theft Is A Common And Costly Problem. For consumers, data breaches involving payment card information and other customer data present the problem of identity theft. The Federal Trade Commission warns that once identity thieves have personal information, they can drain bank accounts, run up charges on credit cards, open new utility accounts, or get medical treatment on a customer's health insurance. An identity thief might even file a tax return in the name of another person and take the taxpayer's refund. Although identity theft may occur shortly after a data breach, it can also be perpetrated long afterward. Thus, the effects of the recent data breaches may continue to play out for many years to come, and the full price tag may not be known as well.

Identity Theft Reportedly Costs $25 Billion a Year. According to the United States Justice Department's Bureau of Justice Statistics, an estimated 16.6 million people experienced at least one incident of identity theft in 2012.[35] The Bureau of Justice Statistics' report, *Victims of*

[34] Sarah Chandler, *The dysfunctional state of America's credit cards*, CNBC.com, http://www.cnbc.com/id/101327705/ (Jan. 13, 2014).

[35] Erika Harrell and Lynn Langton, *Victims of Identity Theft,* (Bureau of Justice Statistics 2012).

Identity Theft, found that the financial losses due to identity theft, totaled $24.7 billion, over $10 billion more than the losses attributed to all other property crimes. About 14 percent suffered an out-of-pocket financial loss, with half of them reporting the loss as less than $100.

The report defined identity theft as the attempted or successful misuse of an existing credit or debit card or bank account, the misuse of personal information to open a new account, or the misuse of personal information for other fraudulent purposes. Approximately 7.7 million people reported the fraudulent use of a credit card and 7.5 million reported the fraudulent use of a bank account including the fraudulent use of a debit card. An additional 1.1 million individuals had new credit card or bank accounts opened with fraudulent information, and another 800,000 individuals had their information misused for other fraudulent purposes.

Identity Theft After A Breach Is Difficult, Time Consuming and Potentially Costly. A recent report by the industry research group Javelin Strategy and Research found that one in three people who received a notification that their data had been compromised becomes a victim of identity theft.[36] If this percentage holds true in the case of the Target breach, which involved breach of data from up to 110 million people, 36 million individuals could, under this formula, be subject to some variation of identity theft from the Target breach alone. Of course, while this number is undoubtedly subject to debate, the fact that any large number of Target customers (and perhaps non-customers) may face identity theft challenges in the future is of great concern.

Many experts argue that simple credit monitoring after a breach is not sufficient to protect consumers from the type of new-account fraud that can be most damaging. Rather, they argue that consumers must (1) review current credit statements across all three credit reporting bureaus; (2) review public record reports and address any inconsistences; (3) install an ongoing monitoring of credit trade lines across all three credit bureaus; (4) install public record monitoring services; (5) monitor for identity elements in play through automated malware feeds; and (6) install change detection monitoring to alert the customer when identity elements are used for authenticating on applications, in and out of traditional credit.

Are Individual Identity Theft Insurance Policies For Consumers The Best Solution? As a result of the increase in identity theft, more insurance companies are reportedly beginning to offer policies that, to some degree or another, cover individual's loss from identity theft. In fact, as part of its package of protection offered to individuals whose data had been compromised as part of the Target breach, Target announced that it is providing, among other things, a $1 million identity theft insurance policy, which can help those individuals cover at least some potential costs associated with potential identity theft, "including lost wages, private investigator fees, and unauthorized electronic fund transfers for one year."[37]

While identity theft insurance policies are not new, interest in them has been growing as the risk of identity theft has been increasing. Homeowners or renters polices may now include such coverage or it may be added as a rider for $100 or less a year. Alternatively, individual policies can also be issued, although the cost would be higher.

[36] Javelin Strategy & Research, 2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends, February 5, 2014.
[37] https://corporate.target.com/about/payment-card-issue/credit-monitoring-FAQ.aspx

However, it is not at all clear if such policies are cost-effective or sufficiently protective. While such policies may provide peace of mind to worried consumers, the cost of the policies, the deductible amount (the amount the insured must pay before the insurance policy kicks in), and the limitations on what is covered appear to raise serious questions as to their usefulness. The Privacy Rights Clearinghouse weighs whether such policies make sense for most consumers: "The risk of financial loss from identity theft is generally very low. If you report a loss promptly after discovery and you have not done anything to contribute to the loss, it is unlikely that you will have financial responsibility. You may encounter a few costs in documenting your loss, such as postage, notary, and copying costs, but these are likely to be minimal. The biggest cost will be your time. [Yet most] policies will not compensate you for your loss of time. For this reason, it's unlikely that you need to purchase identity theft insurance."

Does The Breach of Non-Credit Card Data Present A Greater Potential Risk To Consumers? As noted earlier, current federal law precludes consumer liability for unauthorized credit card transactions. Without minimizing the impact of credit card data breaches on consumers, which some estimates have tagged at up to $4 billion in uncovered losses and other costs from the Target breach,[38] the loss of credit card information by itself may therefore be largely a problem of time and inconvenience for consumers, in comparison to the far larger financial costs incurred by banks and others businesses. However, experts have warned that although victims may not be liable for the unauthorized debts racked up, their credit reports — and in turn their credit scores — can be damaged for weeks or months or even years. Experts have also warned of the impact that credit score problems can have on the larger economy, including the sensitive real estate market if struggling home sales are knocked off track by reduced credit scores resulting from fraudulent charges.[39]

In contrast to credit cards, breaches of debit cards may be more harmful for consumers – particularly if accompanied by breach of PIN data, or if the PINs can be determined from other sources or guessed because many people choose common passwords and often use the same passwords for many of their accounts. Unlike credit cards, debit card purchases take money directly from the user's checking account. These fraudulent transactions may go unnoticed, and once detected it frequently takes banks some time to investigate and put the money back, during which time automated mortgage payments and other bills may bounce, causing a host of hassles and potential damages to the consumer's credit report. People who must rely on debit cards because they do not qualify for credit cards – such as young people, those with low-incomes, and those with less-desirable credit scores – are therefore more at risk than others.

Perhaps more troubling is the loss of non-credit card data, such as mailing addresses, phone numbers, and email addresses. Information of this type was apparently lost for 70 million individuals in the Target breach, independently of the 40 million customers whose payment card information was lost. In recent Congressional testimony, Target acknowledged that among those affected could be some individuals who were not Target customers but whose personal

[38] http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html
[39] Target data breach could affect real estate transactions, LA Times, Feb. 2, 2014 (latimes.com/business/realestate/la-fi-harney-20140202,0,7259625.story)

information Target may have purchased from a third party, although Target stated that such data purchases are purportedly rare.[40]

While the single most important piece of information needed to steal someone's identity is his or her social security number, these other pieces of personal information can also reportedly be used to steal someone's identity. With some or all of this information, an identity thief may be able to obtain credit cards from banks and retailers, potentially open new bank accounts or steal money from the victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, or even obtain a job using the victim's name.

In a relatively new phenomenon, hackers who obtain email addresses have posed as consumers to instruct banks and investment firms to withdraw money from financial accounts.[41]

Moreover, thieves who have retail or card information and email addresses may try to send messages, pretending to be from the company, in an attempt to phish for additional information. For example, an email might instruct the consumer to click a link, which may download malware on the recipient's computer that can extract usernames and passwords and other information. More elaborate scams link to a web site that resembles the company's, where users may be prompted to type in personal data, including even social security numbers. According to the Nilson Report, customers whose names, addresses, email addresses, and phone numbers were lost in the Target breach have already been the subject of attempts by fraudsters to gain additional information from breach victims by email, text message, or phone.[42]

IV. CURRENT LAW IS DESIGNED TO PREVENT IDENTITY FRAUD BY REQUIRING REASONABLE SECURITY MEASURES AND NOTIFYING CONSUMERS WHEN A DATA BREACH HAS OCCURRED. HOWEVER, THERE ARE AS YET NO LIMITS ON THE TYPE OR DURATION OF DATA COLLECTION

California currently attempts to prevent identity theft in two important ways – by requiring businesses that obtain personal information to maintain reasonable security measures, and by requiring notification when data is breached, but then only if the data is unencrypted. However California law apparently does not yet restrict the type of personal information that may be obtained, nor does it generally govern the sharing, storage and duration of the data, despite the generally recognized principle known as "data minimization" which holds that data collection should be focused -- and minimized -- in order to limit the risk of breach. As the recent Congressional hearings show, federal law generally does not regulate consumer data breaches by

[40] "Can data breaches be prevented? Congress and companies answer: For now, no," Melinda Henneberger, *The Washington Post*, February 5, 2014.

[41] Keeping Swindlers Out of Your Bank and Brokerage Accounts, New York Times, Feb. 7, 2014 (http://www.nytimes.com/2014/02/08/your-money/keeping-swindlers-out-of-your-bank-and-brokerage-accounts.html?hpw&rref=business&_r=0)

[42] Nilson Report, "What is Known About U.S. Card Breaches?" (http://www.nilsonreport.com/publication_the_current_issue.php

private entities at all.[43] Although a number of proposals have recently been introduced in Congress, none of them is expected to see enactment any time soon.

Security of Customer Information under California Law. Outside of a few particularly sensitive pieces of personal information – such as medical, financial, and educational information – California law currently imposes relatively few restrictions on the way that businesses can use, handle, or disclose customer information. Of most relevance to the recent data breaches, California Civil Code Section 1798.81.5 requires that many businesses that "own or license" personal information about California residents "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Furthermore, covered business that discloses personal information to a third party pursuant to contract must require by contract that the third party similarly maintain reasonable security procedures and practices. Perhaps surprisingly, this obligation does not apply to financial institutions, health care providers and other specifically exempted entities.

Beyond this general proscription, however, there is nothing in the statute and, to the Committee's knowledge nothing yet in case law, defining "reasonable" security procedures and practices. Although a person who is injured as a result of a violation could in theory bring a civil cause of action pursuant to Civil Code section 1798.84 (b), the Committee is not aware of any private plaintiff or public prosecutor who has sought to enforce this provision, much less who has succeeded, and there may be difficult problems of proof if an individual consumer is required to establish a direct link between the lack of reasonable security and the specific harm suffered by the consumer due to a data breach. Absent a remedy against the data breacher, a consumer's only recourse currently would appear to be to potentially seek criminal or civil sanctions against the perpetrator of the identity theft in the unlikely event he or she could be found.

California's Data Breach Notification Law For Unencrypted Data. In 2002, California adopted the nation's first data breach notification law with the enactment of AB 1386 (Chap. 915, Stats of 2002). Since that time, almost every other U.S. jurisdiction has adopted some form of data breach notification law.[44] California's approach requires any person, agency, or business that "owns or licenses" computerized personal information to notify any person whose data is accessed by any unauthorized person or entity if the data is unencrypted.[45] This obligation arises whenever a breach occurs or is "reasonably believed" to have occurred. The notification is to be made in the most expedient time possible and without unnecessary delay, consistent with the legitimate needs of law enforcement or measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system. The notification requirement specifies the minimum information that must be included in the notice. The statute also requires businesses and government agencies that are required to notify consumers to also submit copies

[43] For further discussion of federal data breach notification laws, see the Congressional Research Service's memorandum on *Federal Information Security and Data Breach Notification Laws*, Gina Stevens, http://www.fas.org/sgp/crs/secrecy/RL34120.pdf (January 28, 2010).

[44] With the exception of Alabama, Kentucky, New Mexico and South Dakota. *See* Reid J. Schar and Kathleen W. Gibbons, *Complicated Compliance: State Data Breach Notification Laws*, Bloomberg Law, http://about.bloomberglaw.com/practitioner-contributions/complicated-compliance-state-data-breach-notification-laws/

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

of the data breach notices to the California Attorney General's Office whenever a breach affects 500 or more California residents. In 2012, the first year of operation, the Attorney General's Office received reports on 131 such incidents.[46]

Separately from the obligation of "owners" to notify individuals in the event of a data breach, California law requires businesses that "maintain" computerized personal information data that the business does not own to notify the owner or licensee of the information of any breach of the security of unencrypted data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In other words, California's breach notification law distinguishes between businesses that "own or license" computerized data and businesses that "maintain" such information. As generally understood, the payment card account information is owned or licensed by the credit card issuer, while the retailer is usually considered to be the entity that only "maintains" the data.

Thus, under current law the retailer is generally required to notify the card issuers in the event of a breach, and the card issuers in turn must notify consumers.

Curiously, as noted above, California's current breach notification law is triggered only if the data is not encrypted. The broad exemption from the notification process for encrypted data is apparently unconditional. Although encryption comes in many different forms and strengths, any encryption is currently sufficient under our state law to relieve businesses from any obligation to notify consumers. Moreover, the encryption exemption appears to apply even when the encryption key may be potentially stolen along with data. It may be argued that the encryption exemption was appropriately included when this landmark law was enacted since it would work as an incentive to encourage much safer data protection through encryption, or that it eliminated the problem of "false positives" – that is, a person might perceive a risk of fraud and take steps based on this assumption when, in fact, there is no apparent danger because the information cannot be deciphered and misused. This line of reasoning, however, appears to rest on what some experts now acknowledge may not be a good assumption – namely, that hackers who are skillful enough to breach the database are not skillful enough to decrypt the data. Indeed, as the representatives of Target and Neiman Marcus stated more than once during Congressional hearings, the hackers were "very sophisticated." Because consumers may be at risk even when encrypted data is disclosed, it may be useful for policy-makers to revisit the question whether the unconditional encryption exemption continues to strike the right policy balance.

The breach notification law puts the onus on consumers to take what may for many consumers be potentially complicated and time-consuming measures to protect themselves from the harms caused by a breach. It does not as of yet require the source of the breach to take responsibility to protect the consumer from these harms, although businesses sometimes appear to voluntarily take steps to protect their consumers, such as Target's recent offer of one-year free credit monitoring. Nor is it yet clear, in California law at any rate, as to what extent if any the breaching party is accountable to consumers for harms they suffer from identity theft or the costs of protecting themselves against identity theft. Although the breach notification law

[46] The California Attorney General's Data Breach Security Reporting web portal is located at http://oag.ca.gov/ecrime/databreach/reporting.

theoretically allows recourse to court enforcement by victims and public prosecutors, no such action has apparently been litigated to a reported decision.

California Law Generally Does Not Yet Restrict The Type of Personal Information That May Be Collected, With Whom It May Be Shared, Or How Long It May Be Stored. For decades the Federal Trade Commission and other consumer protection watchdogs have recognized that one of most important "best practices" to guard against identity fraud is the principle of "data minimization" or "focused collection" and sound retention policies. [47] This means collecting only as much information as is necessary to perform the transaction and not retaining the information for longer than is necessary to perform the transaction.[48] This principle is also reflected in documents issued by the Attorney General of California, including "Privacy on the Go: Recommendations for the Mobile Ecosystem" (January 2013) which identifies limits on the collection and retention of data as one of its basic principles.

In the Target breach, 70 million individuals were reportedly affected by the loss of personal information such as addresses and telephone numbers, compared to 40 million customers whose credit card information was reportedly breached. In addition, the company has acknowledged that some of the personal information it lost could have involved personal information about individuals who had never been Target customers but whose information Target could have purchased, though a Target executive has noted such purchases of personal information from third party data brokers are done rarely by the company. Of course it is not unusual for companies to collect and keep as much information as they wish on as many customers or potential customers as possible, and it is broadly reported and advertised that there is an active market in the sale of this information by data brokers and others. That information may be beneficial when it is used to offer advertising or discounts that customers desire, but it comes with what could be a very significant cost when the information is breached and made available to international cyber criminals.

Commenters have argued that personal data collection should be limited to the information needed to complete the transaction.[49] Nevertheless existing California law regulating the collection, storage and sharing of information appear to be limited to a few specific contexts such as those restricting disclosure of Social Security Numbers, regulation of medical information under the California Medical Information Act, and provisions of the California Education Code that track federal restrictions on sharing educational records.

---

[47] See Testimony of the Federal Trade Commission on Data Security Before the U.S. House of Representatives June 15, 2011 (available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf)

[48] The FTC's "Fair Information Practice Principles" (FIPPs), dating back to 1973 have been updated in various executive agency reports, most recently the White House Consumer Data Privacy Framework and the White House Consumer Privacy Bill of Rights. These documents reflect the common principle that a business should collect and maintain only that information that is needed for legitimate business purposes. (*See* Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 2012. See also, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers, Federal Trade Commission (March 2012).)

[49] *E.g.*, D. Lazarus, Businesses gather more information than they need from consumers, LA Times (Jan. 30, 2014)(latimes.com/business/la-fi-lazarus-20140131,0,1818704.column)