California State Senate

SENATE COMMITTEE ON BANKING AND FINANCIAL INSTITUTIONS

STATE CAPITOL
ROOM 405
SACRAMENTO, CA 95814

TEL (916) 651-4102
FAX (916) 327-7093

STAFF DIRECTOR
EILEEN NEWHALL

COMMITTEE ASSISTANT
RAE FLORES

SENATOR LOU CORREA
CHAIR

Beyond the Breach: Protecting Consumers' Personal Information in the Retail Environment

Joint Informational Hearing

Senate Banking and Financial Institutions Committee
Lou Correa, Chair

and

Senate Judiciary Committee
Hannah-Beth Jackson, Chair

February 25, 2014
1:30 p.m.
State Capitol, John L. Burton Hearing Room (4203)

BACKGROUND PAPER

INTRODUCTION

On December 19, 2013, Target Corporation announced that it had suffered a major data breach. During the height of the Christmas shopping season, hackers infiltrated the retailer's point-of-sale network and stole the debit and credit card information of an estimated 40 million Target shoppers. As forensic investigations into the breach progressed, Target announced that the personally identifying information of approximately 70 million Target customers had also been stolen from the retailer's computer network. According to the latest press reports, it appears that the hackers behind the breach successfully penetrated and lurked within Target's systems months before the breach occurred, remaining undetected while waiting for the start of the holiday shopping season before striking.

The Target data breach – the second largest in United States history – will have wide-ranging impacts on both consumers and industry for a long time to come. In the short-term, an untold number of Californians whose card numbers or personal information was stolen will be at greater risk of identity theft and payment card fraud. Financial institutions have already expended over $170 million to reissue over 17 million credit and debit cards that were compromised by the breach, a number likely to grow over time. (*See* http://www.cbanet.org.) Multiple class-action lawsuits have also been filed in jurisdictions across the country, and the Attorneys General of several states have initiated investigations into the breach. Businesses that were not directly affected by the breach are re-examining their internal security, and many are likely to redouble efforts to protect their networks from similar sorts of intrusions.

Both the upscale retailer Neiman Marcus and the craft store Michaels also reported data breaches during the 2013 holiday season. Indeed, in a notification circulated to certain retailers last month, the FBI revealed that the point-of-sale networks of no fewer than twenty retailers were attacked by hackers in 2013. Furthermore, the scope of computer networks targeted by hackers intent on stealing sensitive personal and financial information extends far beyond the retail sector. According to a database of breaches maintained by the Privacy Rights Clearinghouse, nearly 200 different organizations were subject to malicious hacking during the thirteen months that began in January 2013. (*See* http://www.privacyrights.org/data-breach.) Besides retail, the affected organizations spanned across the hospitality, education, health care, telecommunications, news media, social media, financial, and gaming sectors. Since 2005, over 660 million records have been compromised in more than 4,100 publicly acknowledged data breaches.

The scale of recent attacks against major retailers has drawn particular attention to the vulnerability of electronic payment systems and to fraud prevention and data security efforts within the retail environment. Fundamentally, electronic payment systems cannot function without the trust of those who use them. Customers want assurances that their personal information is safe when they swipe a credit or debit card at a point-of-sale terminal, or when they provide credit or debit card information to a merchant online. Retailers, card issuers, card networks, and payment processors want assurances that customers who use a card or card number in a transaction actually own or are authorized to use the card.

The task of safeguarding consumers' personal and financial information has become a multi-billion dollar industry populated by thousands of participants, each with a slightly different role in a vast and extremely complex payment network. The variation and complexity of the payment card space and the multitude of different entities that occupy it cannot and should not be underestimated, but must be understood if policymakers are to ensure the security of sensitive information within the retail environment.

On February 25, 2014, the California Senate Banking and Financial Institutions Committee and California Senate Judiciary Committee will jointly convene an informational hearing titled, "Beyond the Breach: Protecting Consumers' Personal Information in the Retail Environment." This joint hearing will take a hard look at retail electronic payment systems and will give members of the Committees and other interested parties an opportunity to ask experts from across the industry about efforts to combat fraud, prevent data breaches, and keep sensitive personal and financial information safe. The Committees will hear testimony from twenty invited witnesses, representing virtually every segment of the payment landscape, including consumer and privacy rights advocates, state and federal law enforcement agencies, depository institutions, retailers, payment card networks, point-of-sale hardware manufacturers, payment processors, and security consultants.

Major questions to be addressed during the hearing include:

- What, exactly, is meant by the terms "card fraud," "data breach," and "identity theft?" How do these topics differ, and how are they related?

- How does existing state and federal law protect consumers whose personal information has been breached? How does the law protect consumers who have become victims of card fraud or identity theft? Should the State of California add to or expand on these laws?

- How does a retail transaction involving a payment card actually work? What parties have access to a cardholder's personal and financial information? What rules must they follow to secure that information?

- What new technologies are on the horizon to better protect consumers' personal and financial information? What are the strengths and weaknesses of those technologies? Who will pay to implement those technologies? Who, besides consumers, will benefit from them?

- Which participants in the payment network pay for fraud when it occurs? Which entities pay when a data breach occurs? How does cost allocation differ in face-to-face ("card-present") and remote ("card-not-present") transactions? Does the existing cost allocation structure make sense, or should it be changed?

- Which participants in the payment network are responsible for notifying consumers when their personal or financial information may have been compromised due to a data breach? Should this duty to notify rest with other/additional participants?

- Are the data breach notices currently sent to customers useful? Should additional information be provided to consumers whose personal or financial information may have been compromised due to a breach?

- Finally, and most important: Are consumers' safe when they use a payment card to purchase goods or services? What can we do to make them safer, and how much will it cost?

This hearing will give members of the Committees valuable insight into how the electronic payment system operates, as well as an opportunity to engage with key industry and consumer protection experts on how California can make the system more secure, for the benefit of all parties.

ROLE OF ELECTRONIC PAYMENT SYSTEMS

The United States is rapidly advancing toward a cashless economy. Today, an estimated 80 percent of consumer spending (by value) is transacted using a form of payment other than cash. In 2012, the Federal Reserve estimated that American consumers performed 122.8 billion noncash payments, collectively valued at $79 trillion. Of these noncash payments, approximately two-thirds were made using credit cards, debit cards, and prepaid debit cards (collectively "payment cards"). The number of payment card transactions as a percentage of total noncash transactions has increased dramatically over recent years, rising from 43 percent in 2003 to 67 percent in 2012.

Despite an apparent growing reliance on payment cards in the United States, the majority of American consumers have expressed "serious concern" about fraud and other security risks involved in using credit and debit cards. A 2012 survey found that 52 percent of Americans are "seriously concerned" about other people obtaining and using their credit or debit card accounts, and 54 percent expressed "serious concern" over identity theft. (*See* Unisys Security, *Unisys Security Index: US* (April 18, 2013) <http://www.unisyssecurityindex.com/usi/us/reports> [as of Feb. 21, 2014].) The survey also found that 33 percent of Americans are "seriously concerned" about the security of shopping or banking online, and two-thirds (67 percent) are "at least somewhat concerned about data breaches hitting their banks and financial institutions." Overall, the survey concluded that financial security was the largest threat concerning U.S. residents, driven principally by worry about identity theft and payment card fraud.

Regarding the amount of fraud occurring on electronic payment systems, the Federal Reserve estimates that 31.1 million unauthorized transactions (third-party fraud) occurred on electronic payment systems in 2012, with a value of $6.1 billion. Ninety-two percent of these fraudulent transactions (65 percent by value) occurred using payment and ATM cards. By contrast, only 8 percent of fraudulent transactions (35 percent by value) were made using checks and automated clearinghouse (ACH) direct-debit account transfers.

BASIC OVERVIEW OF PAYMENT CARD TRANSACTIONS

The payment card industry has undergone significant transformation since Bank of America introduced the first general purpose revolving credit card in California in 1958. What used to be

an industry involving relatively few participants has evolved into a highly diversified and specialized marketplace, offering consumers a range of noncash payment systems to choose from that include credit cards, debit cards, prepaid debit cards, ATM cards, charge (non-revolving credit) cards, and private-label cards. Across the payment card industry, merchants, banks, payment processors, card networks, and other specialized entities enter into contracts with one another to enable customers using these products to purchase goods and services electronically without having to carry cash. Because of the varied approach taken by market participants who offer payment card services, there is no single method by which payment card transactions are handled. However, as a general matter, payment card transactions tend to operate as follows:

Credit Cards

Credit cards are issued by an issuing bank or issuing credit union to a consumer after an assessment of the consumer's risk of default. Credit cards are issued by these financial institutions under an agreement with one or more card networks (e.g. Visa, MasterCard, Discover, or American Express), who set certain terms for the use of the card and who oversee (or operate) the electronic transaction network used to facilitate credit card transactions. Cardholders can use their credit card to purchase goods or services from merchants that accept cards branded for use on a particular card network. In order to accept those cards, merchants must contract with an acquiring bank and establish a merchant account for the receipt of credit card payments. Often times, merchants contract with acquiring banks via third-party resellers of credit card services called Independent Sales Organizations (ISOs) instead of entering into direct relationships with acquiring banks. Actual processing of credit card transactions across the card network's data infrastructure – known as the interchange – may be performed by an acquiring bank, an ISO, or a dedicated third-party payment processor (e.g. First Data or TSYS). Design and manufacture of payment terminals for use on the interchange is typically carried out by an independent terminal manufacturer (e.g. Verifone, Equinox Payments, or Integrated Peripherals).

The actual processing of credit card transactions across the interchange occurs in two distinct phases. First, when a cardholder swipes his or her credit card through the magnetic stripe reader of a payment terminal, the payment processor submits the transaction across the interchange for initial approval in what is commonly referred to as authorization. During the authorization phase, the payment terminal transmits certain basic information about the transaction – the credit card number, name on the card, amount, and transaction type – to the acquiring bank. The acquiring bank then verifies the account information with the issuing bank and reserves an amount equal to the transaction on the customer's account held by the issuing bank. If the account information is authentic and the customer has sufficient credit available, the issuing bank sends an authorization or approval code back through the system to the merchant, who stores the code with the transaction. The authorization process takes a matter of seconds to complete.

The second phase of a credit card transaction – the settlement phase – typically involves merchants sending authorized transactions in batches to the acquiring bank (via an ISO or payment processor) at the end of the business day. Merchants may accept credit cards used on more than one credit network (e.g. both Visa and MasterCard), in which case the merchant may contract with different acquiring banks, ISOs, or payment processors to process credit transactions across each network. A device known as a switch or gateway separates approved

transactions according to issuing bank (using the first four digits of the account number) and routes the data to the appropriate payment processor (if more than one is used) and card network. The card network then uses each authorized transaction to debit the transaction amount from the issuing bank and credit it to the acquiring bank. The acquiring bank then credits the amount to the merchant account, minus an interchange fee shared by the issuing bank and the card network for use of the payment card system, as well as a fee called a discount rate which is retained by the acquiring bank as payment for processing the transaction. Contracts executed between merchants, acquiring banks, ISOs, and payment processors may modify what fees are collected during the settlement phase and who receives the fees. During the settlement phase, the issuing bank places a charge equal to the approved transaction amount against the consumer's line of credit.

Debit Cards

Debit card transactions are handled differently depending on whether a transaction is processed in real-time using a PIN (Personal Identification Number), or whether the transaction is processed "offline" using the customer's signature instead of a PIN. Offline debit card transactions, also known as check card transactions, are handled in the same manner as credit card transactions, using a two-stage or dual-message authorization and settlement process. Because check card transactions are processed via the same card networks as credit cards, they often incur the same discount rate and interchange fees. In contrast, online debit card transactions using a PIN are processed in a single-message format, where authorization and settlement occur at the same time. Both types of debit card transactions draw funds directly from a consumer's bank account to pay for whatever goods or services are being bought.

As with credit cards, merchants contract with acquiring banks, ISOs, and payment processors to accept debit card transactions as a form of payment. Transactions made with a debit card travel across a payment network (e.g. Pulse, STAR, or Maestro) analogous to the card networks used for credit card transactions, and may even use some of the same infrastructure.

When a customer swipes a debit card through a payment terminal during an online or PIN-based transaction, he or she is prompted to enter a PIN in order to complete the transaction. Upon entering the PIN, information about the transaction – account number, PIN, amount, date, transaction type, etc. – is sent across the payment network to the consumer's financial institution. The financial institution verifies that the account is valid and has sufficient funds to cover the transaction, and then immediately authorizes the transaction and transfers funds equal to the transaction amount plus associated processing fees (unless paid by the merchant) back across the payment network to the acquiring bank. The acquiring bank then transfers the funds, less any fees, to the merchant's account at the acquiring bank. As with credit card processing, contracts executed between merchants, acquiring banks, ISOs, and payment processors may modify what fees are collected during a debit card transaction and who receives the fees.

UNDERSTANDING THE DIFFERENCES BETWEEN PAYMENT CARD FRAUD, IDENTITY THEFT, AND DATA BREACHES

Payment card fraud is the use of a payment card to purchase goods or services by an individual who is not the card owner and is not authorized by the card owner to use the card. *Existing* card fraud can occur when an unauthorized person gains physical access to a payment card that has been lost, stolen, or discarded by its owner without being destroyed. It can also occur when the card physically remains with the cardholder, but the card number and other identifying cardholder information is stolen and either counterfeited to create a new card with the same number or fraudulently used in card-not-present transactions. Existing card fraud affects accounts that were opened by the actual card owner, but subsequently used for fraudulent purchases not authorized by the card owner.

New card fraud involves the establishment of a new payment card account in the name of someone whose identity has been stolen. Because the person in whose name the account is opened is often unaware of the existence of the new account, *new* card fraud can be harder to detect and can go on for longer periods of time than existing card fraud.

Identity theft, or more accurately identity fraud or impersonation, occurs when one person uses someone else's personal information (e.g., name, date of birth, or social security number) to commit fraud or other crimes. Although there are many different types of identity theft (e.g., criminal, financial, and medical), financial identity theft is the type of identity theft most relevant to this hearing. Financial identity theft includes the creation of new payment card accounts in the name of the person whose identity was stolen.

Data breaches involve the theft or unintentional disclosure of data residing on a computer system or other electronic device. A data breach may not result in payment card fraud or identity theft if the data breached are encrypted or otherwise unusable, or if the people whose data are stolen take immediate steps to close existing accounts, monitor their accounts for fraudulent activity, and monitor their credit reports for unauthorized account creation. In the alternative, a data breach can lead to identity theft and/or payment card fraud, if enough payment card and other personal identification information in a usable form is stolen.

DATA BREACHES BY THE NUMBERS

There is no single, definitive, complete source of information regarding data breaches. However, there are several data sources which can be combined to provide a sense for which entities are most frequently targeted by data breaches, what types of methods are most commonly used to perpetrate breaches, and where the breaches originate.

One of the most comprehensive sources of information is produced by Verizon Enterprises, which has published an annual Data Breach Investigations Report (DBIR) since 2003. In its most recent report, the 2013 DBIR (available at http://www.verizonenterprise.com/DBIR/2013/), Verizon incorporates information from 19 global organizations regarding 621 confirmed data breaches that occurred during 2012. Although the authors of the report are quick to warn readers that their report is limited to information gleaned from breaches that were reported and to caution

readers against drawing definitive conclusions from a single year's worth of data, they do see several trends, which are consistent from year to year, and are reflected in 2012 data.

According to the 2013 DBIR, financial organizations are most likely to be affected by data breaches (they comprised 37 percent of the breaches identified during 2012), followed by retail environments (15 percent) and restaurants (9 percent). Entities attacking these three types of organizations are most likely to be looking for information that can be used to perpetrate financial fraud. Many of the other targets of data breaches, including manufacturers, professional service organizations, and information organizations, are more likely to be targeted in connection with industrial espionage.

The majority of data breaches are perpetrated by outsiders; 92 percent of the data breaches tracked by Verizon during 2012 originated outside the company that was attacked. Seventy-six percent of network intrusions exploited weak or stolen credentials, 52 percent involved some form of hacking, 40 percent incorporated malware, 35 percent involved physical attacks (such as ATM skimming), and 29 percent leveraged social tactics (numbers do not add to 100 percent, because more than one method was often used to perpetrate a single breach). Some industries are more likely to be subject to physical attacks (e.g., financial institutions), while other institutions are more likely to be subject to attacks involving social tactics (which are typically tied to industrial espionage).

With respect to malware intrusion, Verizon found that the two most common vectors included direct installation by an attacker who gained access to a system and indirect installation through use of an infected e-mail attachment sent to one or more people within the organization. Moreover, two-thirds of data breaches take many months to discover, and are discovered by external parties rather than by the company that is breached.

Two other useful sources of information about data breaches that affect Californians are maintained by the Privacy Rights Clearinghouse (PRC) (*see* http://www.privacyrights.org/data-breach) and the Office of the California Attorney General (*see* https://oag.ca.gov/sites/all /files/agweb/pdfs/privacy/2012data_breach_rpt.pdf [as of Feb. 21, 2014]). Like Verizon, both PRC and the Attorney General can only report on breaches about which they are made aware, thus leaving an unknown number of breaches unavailable for analysis.

The Attorney General's 2012 Data Breach Report includes information from 131 breaches, each of which affected more than 500 California residents. According to information contained in that report, data breaches affected over 2.5 million Californians during 2012. Five breaches affected the personal information of over 100,000 individuals. The average breach incident involved the information of 22,500 individuals. (*See* Attorney General's 2012 Data Breach Report.)

The retail industry was subject to the greatest number of breaches reflected in the Attorney General's 2012 report (34 breaches, reflecting 26 percent of the breaches reported to the Attorney General), followed by finance and insurance with 30 breaches (23 percent). More than half of the breaches (56 percent) involved Social Security numbers, while 40 percent involved payment card information.

Importantly, the Attorney General's 2012 report concludes that data breaches do sometimes lead to fraud. Citing a nationwide survey, the report states that "[i]ndividuals who received a data breach notification in 2012 had an identity theft incidence rate of 22.5 percent, more than four times the 5.3 percent rate for all adults." (*See* Attorney General's 2012 Data Breach Report.)

ALLOCATION OF FINANCIAL RESPONSIBIILTY WHEN PAYMENT CARD FRAUD OCCURS

Generally speaking, as long as a consumer notifies their card issuer that a transaction is fraudulent, the card issuer will not require the cardholder to pay for the goods or services that were fraudulently obtained. But, if the consumer doesn't pay, who does? It depends.

If payment card fraud occurs in an in-person (card-present) transaction, despite every party's adherence to their contractual obligations to prevent fraud, the card-issuing financial institution is typically responsible for covering the cost of that fraud. According to information provided by one of the major payment networks, financial institutions cover the cost of approximately 80 percent of card-present fraud.

On the other hand, if the fraudulent transaction is of the "card-not-present" (CNP) variety (e.g., online, phone, or mail order transactions), the merchant generally bears the cost of fraud. According to a report prepared by specialty publisher Nilson based on 2012 data (*see* Nilson Report, *Issue 1023* <http://www.nilsonreport.com> [as of Feb. 21, 2014]), retailers bear just over one third of the cost of payment card fraud losses annually. CNP fraud represents the largest category of merchants' fraud costs.

However, the general cost allocation rules summarized above are based upon the assumption that each party involved in authorizing a fraudulent transaction complies with all of their contractual responsibilities to prevent fraud. Often, mistakes are made by one or more party when a fraudulent transaction is authorized. For this reason, financial responsibility for covering the cost of payment card fraud is often determined by overlaying the results of forensic security investigations with the terms of contracts that govern the responsibilities of each party in a payment transaction. In reality, the cost of holding customers harmless for fraudulent transactions involving their cards is allocated based on the responsibility of each party for authorizing the fraudulent transaction.

One of the other significant costs of payment card fraud involves card-reissuance. When a valid card number is fraudulently obtained, card-issuing financial institutions typically cancel the card whose number was compromised and re-issue a new card to the legitimate cardholder. The cost to reissue these cards is borne by the card-issuing financial institutions.

TECHNOLOGIES FOR USE IN COMBATTING CARD FRAUD AND DATA BREACHES

Multiple technologies exist for use in combatting card-present fraud, CNP fraud, and preventing data breaches.

EMV (Integrated Circuit Card Technology): A Tool Against Card-Present Fraud

Originally an acronym for Europay, MasterCard, and Visa, EMV is a brand rather than a technology. When people refer to EMV as synonymous with "chip and PIN," they are incorrect in the same way that people who refer to Band-Aids or Kleenex are technically incorrect when they use those terms to describe adhesive strips and facial tissues; EMV is a brand owned by EMVCo and is just one set of standards developed to facilitate the use and compatibility of payment chip cards and payment terminals.

According to the Debit Network Alliance, "integrated circuit card" is the most accurate term to use when one wishes to refer to a plastic card that includes an embedded integrated circuit that communicates information to a payment or ATM terminal. Other accurate terms include "chip card," "contact chip card," and "smart card" (although "EMV card" is often used to represent all chip cards, rather than just chip cards designed to be read by the proprietary EMV network). Technically, all EMV cards are integrated circuit cards.

Integrated circuit cards can be read either directly via contact with a reader (chip cards are dipped rather than swiped) or with a remote, contactless radio frequency interface. Because they are equipped with embedded microcontrollers, chip cards are able to securely store large amounts of data, carry out their own on-card functions such as encryption and authentication, and interact more intelligently with card reader than cards equipped with magnetic stripes. Unlike cards equipped with magnetic stripes, whose stored data are static, chip cards generate a new code for each transaction, making them far less susceptible to cloning than traditional stripe cards.

Although the majority of integrated circuit card implementations worldwide to date have been of the "chip and PIN" variety, other options for authenticating the card's user are possible, including "chip and signature" and "chip and choice (of either PIN or signature)." According to a white paper written by payment processor First Data, there are over 1.2 billion integrated circuit payment cards in circulation worldwide, and over 15 million point-of-sale terminals capable of reading those cards. (See First Data, EMV in the U.S.: Putting It into Perspective for Merchants and Financial Institutions <http://www.firstdata.com/downloads/thought-leadership/EMV_US.pdf> [as of Feb. 21, 2014].) Nearly all of those cards and card readers reside outside the United States.

Despite their popularity abroad, integrated circuit cards are not a panacea. Although valuable in combatting card-present fraud, these cards are no more or less secure in combatting CNP fraud than cards equipped with magnetic stripes. As a result, countries that have migrated to integrated circuit cards have seen a shift away from card-present fraud to CNP fraud following the adoption of chip cards (see Smart Card Alliance, Card-Not-Present Fraud: A Primer on Trends and Authentication Processes (February 2014) <http://www.smartcardalliance.org/resources/pdf/CNP-WP-012414.pdf> [as of Feb. 21, 2014]). Not surprisingly, fraudsters attack the most vulnerable point in a payment system; when steps are taken to make card-present fraud more difficult to perpetrate, fraudsters shift to CNP fraud.

At the present time, the timeline for United States migration to integrated circuit cards is uncertain. The major card networks are pressuring card-issuing depository institutions and merchants to migrate to the EMV standard by October 2015. However, full migration represents a chicken-and-egg challenge. Banks and credit unions are hesitant to issue integrated circuit cards to their card-holding customers if those cards cannot be read by the point-of-sale devices used by merchants. Merchants are hesitant to expend the significant costs necessary to update their point-of-sale devices to chip readers before integrated circuit cards are in wide circulation. The cost to achieve full migration is estimated at approximately $8 billion ($6.8 billion to replace point-of-sale devices, $1.4 billion to issue new cards, and $500 million for ATM upgrades).

One of the other challenges to widespread use of integrated circuit cards tracks back to the cost allocation issue described earlier. Integrated circuit cards are valuable at combatting card-present fraud; they are no more valuable than magnetic stripe cards at combatting CNP fraud. As noted above, card-issuing financial institutions (rather than merchants) bear most of the costs of card-present fraud, while merchants bear most of the costs of CNP fraud. Thus, merchants are being asked to shoulder the majority of costs attributable to integrated circuit card migration, while the card-issuing financial institutions will receive most of the cost savings from this migration.

Combating Card-Not-Present (CNP) Fraud

As described above, integrated circuit cards have a role to play in combatting card-present fraud, but are not effective in combatting CNP fraud. There is no single technology that has become accepted among payment network participants at combatting CNP fraud in the way that smart cards seem to be the future tool for combatting card-present fraud.

Multiple tools are available with which to combat CNP fraud, most of which focus on multi-factor authentication. Generally speaking, multi-factor authentication relies on a person providing authentication factors from two or more of the following groups: 1) ownership factor: something the person has, such as a credit card number; 2) knowledge factor: something the person knows, such as a PIN, street address, or zip code; and 3) inherence factor: something the person is or does, such as a fingerprint. Examples (but by no means an exhaustive list) of the tools available to those who wish to combat CNP fraud include static passwords or PINs, random static passwords, static knowledge-based authentication, random knowledge-based authentication, one-time password using hard tokens, one-time password using soft tokens, scratch cards, bingo cards, voice verification, chip authentication programs with personal card readers or mobile devices, physical biometrics, and behavioral biometrics.

Combatting CNP fraud is often a balancing act. Retailers want to collect enough information from purchasers to ensure that the person providing the card number is the legitimate card owner, without creating a purchasing process that is so onerous they lose customers through transaction abandonment. Most retailers use commercial intermediaries to help provide CNP fraud prevention tools that best match their size, amount of customer traffic, and the nature of their customers. All of the major card brands offer forms of CNP fraud prevention (e.g., Verified by Visa and MasterCard Secure Code). Combatting CNP fraud is also a focus of numerous security consultants that design payment platforms for use by merchants.

Encryption and Tokenization: Tools to Prevent Data Breaches

According to First Data Corporation, there are two points in the payment process where cardholder data is at greatest risk of being exposed or stolen: 1) pre-authorization, when a merchant has captured a consumer's card data and is either about to send it or is in the process of sending it to be authorized; and 2) post-authorization, after the transaction has been authorized by the cardholder's depository institution, when cardholder data is stored for analytics and other processes. (*See* First Data, *Avoiding a Data Breach: An Introduction to Encryption and Tokenization* < https://www.firstdata.com/en_us/insights/6203-Data-Breach-Market-Insight.html> [as of Feb. 21, 2014].)

First Data describes encryption as a means of providing security at the pre-authorization stage, while tokenization is a means of providing security post-authorization. Encryption is the process of using an algorithm to encode plain (i.e., readily understandable) text into a non-readable form called cypher text. Once data are encrypted, a key is required to decrypt the information and return it to its original, plain text format. (*See* First Data, *Avoiding a Data Breach: An Introduction to Encryption and Tokenization.*)

Tokenization involves the use of a token as a replacement for a payment card number. Once a transaction is authorized, cardholder data are sent to a server for storage. At the same time, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. Because the token number cannot be used by anyone but the merchant that owns the token, it lacks value if stolen.

USE OF DATA SECURITY STANDARDS TO PREVENT DATA BREACHES

Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry (PCI) Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard, and Visa in 2006 to develop and manage security standards for global payment card data protection. The Council's membership includes representatives of all five founding brands and other industry stakeholders, including merchants, processors, technology vendors, and others key members of the payment chain.

PCI Data Security Standards (PCI DSS) were developed by the PCI Security Standards Council to establish a baseline set of controls, which, if followed and applied consistently by entities that handle card data, are intended to minimize the risk of data breaches and the resulting damage if breaches do occur. PCI DSS cover all types of payment cards (credit, debit, and prepaid) that carry the logo of PCI payment brand members and apply to any organization that accepts, processes, transmits, or stores these types of payment card data. These standards apply across all types of transactions involving payment cards, regardless of the specific technologies used to process transactions and protect consumer data.

PCI DSS are not law in California or at the federal level. Instead, these industry-developed standards are enforced contractually by private parties within the payment space. Companies

that do not agree to comply with PCI DSS are likely to receive less beneficial commercial terms from those with whom they contract, and may be denied contracts altogether. When fraud or data breaches occur, entities found to be out of compliance with PCI DSS are likely to be forced to shoulder more of the monetary burden than other, more-compliant parties within the payment stream.

PCI DSS are updated by the PCI Security Standards Council at regular intervals. One such update recently occurred; PCI DSS Version 3.0, which was released on January 1, 2014 and must be fully implemented by December 31, 2014, includes twelve broad requirements and nearly 400 sub-requirements called controls. Version 3.0 replaced Version 2.0, which included twelve broad requirements and 289 sub-requirements.

The twelve requirements that comprise the PCI DSS include:

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendors' default passwords or security parameters.
- Protect Stored Cardholder Data.
- Encrypt transmission of cardholder data across open, public networks.
- Protect systems from malware and keep anti-virus software up to date
- Develop and maintain secure systems and application.
- Restrict access to cardholder data by business need to know.
- Identify and authenticate access to system components (i.e., assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security for all personnel.

Legislative History Pertaining to PCI DSS

As stated above, none of the PCI DSS are codified in California law. Bills attempting to codify some of the data security standards were proposed in both 2007 and 2008, but vetoed by Governor Schwarzenegger. In 2007, Assemblyman Dave Jones authored AB 779, which was sponsored by the California Credit Union League, and would have mandated compliance with seven of the twelve requirements of PCI DSS Version 1.0. AB 779 was vetoed by Governor

Schwarzenegger on the basis that the bill attempted to legislate in an area where the marketplace had already assigned responsibility and liability that protected consumers. Governor Schwarzenegger was concerned that the static requirements in the bill might fail to keep up with changes in technology, and that, as data security technology evolved, the bill could place California law in conflict with those standards. The Governor also expressed concern about the compliance costs of the bill and its impact on businesses, particularly small businesses. Another bill introduced by Assemblyman Jones in 2008 (AB 1656) was vetoed for similar reasons.

APPENDIX A

STATE AND FEDERAL PRIVACY AND DATA BREACH NOTIFICATION LAWS

APPENDIX A

STATE AND FEDERAL PRIVACY AND DATA BREACH NOTIFICATION LAWS

CALIFORNIA LAW

Privacy is a fundamental right in California. Article I, Section 1 of the California Constitution declares that all people have an inalienable right to pursue and obtain privacy. (Cal. Const., art. I, § 1.) The development of sophisticated information technology systems and data aggregation industries have challenged both how we think of privacy in the modern age, as well as the direction public policy should take in preserving this fundamental right. California's legislature has expressly recognized that:

> (1) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies;
>
> (2) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information; and
>
> (3) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798.1.)

California has responded to these threats to privacy by creating some of the strongest consumer privacy laws in the country. In 2003, California enacted the first-in-the nation security breach notification law. (*See* Civ. Code §§ 1798.29(a), 1798.82(a).) This law requires state agencies and businesses to notify residents when the security of their personal information is breached. The law ensures that residents are given timely notification of data breaches affecting them, allowing them to take appropriate action to mitigate or prevent potential financial losses due to fraudulent activity, as well as to limit the potential dissemination of personal information. Since 2003, all but four states have enacted similar data breach notification laws, and governments around the world are considering enacting such laws. In particular, California's breach notification law:

- Requires any agency, person, or business that owns or licenses computerized data to disclose a breach of the security of the system to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement. (Civ. Code §§ 1798.29(a), (c) and 1798.82(a), (c).)

- Requires any agency, person, or business that maintains computerized data that the agency, person, or business does not own to notify the owner or licensee of the information of any security breach immediately following discovery if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. (Civ. Code §§ 1798.29(b) and 1798.82(b).)

APPENDIX A

STATE AND FEDERAL PRIVACY AND DATA BREACH NOTIFICATION LAWS

California also imposes (with limited exceptions) an across-the-board data security standard on businesses that own or license personal information about California residents. The Information Security Law requires such businesses to "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." (Civ. Code § 1798.81.5(b).) Businesses that disclose personal information about a California resident pursuant to a contract with a nonaffiliated third party must also require by contract that the third party adhere to similar data security standards.

Other California laws concerning data protection and information privacy include:

- Confidentiality of Medical Information Act: This act states that no provider of health care is to disclose medical information regarding a patient without first obtaining an authorization, except under certain enumerated circumstances. Under the act, in addition to any other remedies available at law, a patient whose medical information has been used or disclosed in violation of the act and who has sustained economic loss or personal injury as a result may recover compensatory damages, punitive damages not to exceed three thousand dollars, attorney's fees not to exceed one thousand dollars, and the costs of litigation. (Civ. Code § 56 et seq.)

- Consumer Credit Reporting Agencies Act: In relevant part, this law permits a consumer to place a "security freeze" on his or her credit report, prohibiting consumer credit reporting agencies from releasing the consumer's credit report or any information contained in it unless the consumer expressly authorizes the release. (Civ. Code § 1785.11.2(a).)

- Financial Information Privacy Act of 2005: This act states that, except in limited circumstances, a financial institution shall not sell, share, transfer, or otherwise disclose nonpublic personal information to or with any nonaffiliated third parties without the explicit prior consent of the consumer to whom the nonpublic personal information relates. (Fin. Code § 4052.5.)

- Online Privacy Protection Act of 2003: This law requires an operator of a commercial website or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its website to conspicuously post its privacy policy. (Bus. & Prof. Code § 22575.)

- Tort for Invasion of Privacy: A litigant can state a claim for violation of the constitutional right to privacy by establishing the following three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by the defendant that constitutes a serious invasion of privacy. (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1.) Existing law recognizes four types of activities considered to be an invasion of privacy giving rise to civil liability, including the public disclosure of private facts. (*Id.*)

APPENDIX A

STATE AND FEDERAL PRIVACY AND DATA BREACH NOTIFICATION LAWS

FEDERAL LAW

Federal law protects the personally identifying information (PII) of consumers in a number of discrete areas, but generally lacks any overarching mandate that entities who possess PII maintain a particular level of data security. The "deceptive trade practices" prohibition in section 5 of the Federal Trade Commission Act (15 U.S.C. § 45(a)) has been successfully used as a stopgap to bring cases against certain entities that fail to secure customer data when they act in a manner inconsistent with their stated data security policy. More recently, the Federal Trade Commission (FTC) has brought cases alleging that a failure to employ reasonable and appropriate measures to protect PII against unauthorized access constitutes a violation of the FTC Act's "unfair acts or practices" prohibition independent of any deceptive conduct. (*See* First Amended Complaint in *FTC v. Wyndham Worldwide Corporation*, No. 212-cv-01365-SPL, Docket No. 28 (D. Ariz., 2012).) Federal law does not currently mandate consumer notification in the wake of a data breach except for breaches involving certain health-related information governed by the Health Insurance Portability and Accountability Act of 1996 (HIPPAA). Legislation has been introduced in both the House of Representatives and Senate that would create new nationwide data security and breach notification requirements, but it is unclear what its prospects are for becoming law. Other federal laws concerning data protection, breach notification, and fraud prevention include:

- Children's Online Privacy Protection Act (15 U.S.C. § 6502): This act generally prohibits the operator of a website or online service directed to children under the age of 13 from collecting personal information from a child, including the child's first and last name, home or other physical address including street name and name of city or town, e-mail address, telephone number, or Social Security number.

- Electronic Fund Transfer Act (15 U.S.C. § 1693g): This act limits a consumer's liability to $50 for unauthorized account activity transacted with a lost, stolen, or fraudulently used debit card, provided the consumer notifies their financial institution within two business days after learning of loss or theft of the card or associated access code. If a consumer does not inform the card issuer within two business days of learning of the loss or theft of the card or access code, the act provides that they could be liable for up to $500 of fraudulent activity. If a consumer fails to report an unauthorized transaction appearing on an account statement within 60 days after the statement is mailed, the consumer risks incurring unlimited losses on unauthorized transfers made after the 60-day period.

- Fair and Accurate Credit Transactions Act (15 U.S.C. § 1681 et seq.): This act gives consumers the right to one free credit report per year from the credit reporting agencies and contains provisions designed to prevent and mitigate identity theft, including a section that enables consumers to place fraud alerts in their credit files.

- Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.): This act protects consumers from being harmed by inaccurate or misleading information contained in files maintained by credit reporting agencies by requiring these agencies to disclose the contents of credit

files to consumers and by giving consumers the ability to correct errors. The act also gives consumers the right to know what information credit reporting agencies are distributing about them to creditors, insurance companies, and employers.

- Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.): Among other things, this act requires financial institutions to insure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to the customer. The act also requires covered entities to give customers privacy notices that explain their information-sharing practices, and give customers an opportunity to direct that their personal information not be shared with certain non-affiliated third parties.

- Stored Communications Act of 1986 (18 U.S.C. § 2701 et seq.): Among other things, this act provides that a valid subpoena issued in connection with a criminal investigation or an order from a court of competent jurisdiction may compel an electronic communications service (e.g., an internet service provider or website operator) to preserve or disclose personal identifying information to law enforcement authorities.

- Truth in Lending Act (15 U.S.C. § 1601 et seq.): Among other things, this act limits a consumer's liability to $50 if a credit card is lost, stolen, or used without authorization.