DATA SECURITY: EVERYTHING YOU NEED TO KNOW

- Data Breaches: Where, What and Why
- Federal and State Regulations to Protect Data
- EMV Chip Technology
- PIN or Signature?
- Existing and Emerging Security Options
- Mobile Payments
- Smart Security in a Changing Threat Landscape

Data Breaches: Where, What and Why

Where do most data breaches occur?
The Identity Theft Resource Center has compiled a list of all publicly reported breaches in the United States showing that through December 23, 2014 banks accounted for only 5.5 percent of all breaches this year. Other businesses (e.g., retailers) accounted for 33 percent.

Why do other reports cite higher breach numbers for banks?
Some reports, like Verizon's report on data breach statistics that is sometimes cited, are based on an international ***sample*** of breaches as opposed to an actual compilation of all publicly reported breaches in the United States. In fact, the 2014 Verizon report includes data from 95 separate countries. To the contrary, The Identity Theft Resource Center has compiled a list of ***all*** publicly reported breaches in the United States and shows that banks accounted for only 5.5 percent of all breaches in 2014.

The North American Industry Classification System (NAICS), which the Verizon report uses to classify sectors, includes a broad number of companies in its definition of "Finance and Insurance." This definition goes well beyond depository institutions and includes potentially thousands of other, non-depository companies. Among others, these include insurance, investment and annuities companies, or any other company "specializing in facilitating or supporting financial intermediation, insurance, and employee benefit programs."

What was the cause of the Target breach?
According to media reports, investigations into the Target data breach show that hackers gained access through the company's HVAC contractor using malware that collected customers' credentials.

Are we more vulnerable to security breaches than ever before?
Hackers are constantly trying to find the weakest link and access vulnerabilities. The Target breach is a good example of that. Banks have invested heavily in new technologies to fight these criminals. For example, JPMorgan Chase has announced its plan to invest $250 million annually into data security. But hackers are always looking for new ways to penetrate businesses. Banks cannot fight this battle alone. Greater collaboration between banks and retailers is critical for fighting fraud and cybercrime.

Federal and State Regulations to Protect Data

Are financial institutions regulated to ensure consumers are protected against breaches?
Yes. Financial institutions are required by federal and state laws and regulations to protect information and notify consumers when a breach occurs that will put them at risk. The Gramm-Leach-Bliley Act (GLBA) imposes stringent rules on how financial institutions must protect the security and confidentiality of information and allows for regular compliance exams by regulators. Financial institutions are also subject to regulators' "Red Flag Rules" requiring institutions to have both written and operational identity theft prevention programs in place. The extensive examination and enforcement regime ensures that financial institutions provide robust protections for personal financial information belonging to the American public.

Are retailers regulated to ensure consumers are protected against breaches?
No. In contrast to financial institutions, retailers are not subject to federal laws or regulations that require them to protect data and notify consumers when they are breached. They are only regulated by a patchwork of state regulations.

What is the current landscape of regulation on the federal and state levels for various businesses?
Currently, different business sectors are subject to federal regulations in addition to a patchwork of state regulations. Financial institutions are a type of business that is subject to federal regulations (Gramm-Leach-Bliley Act) as well as 46 separate state laws that regulate both notification and data protection standards. Retailers are subject to state regulations but not a federal standard.

Are there currently regulations requiring specific technologies?
No, given that hackers are always changing their tactics and security measures are always being improved to address new threats, policymakers from both sides of the aisle have expressed serious concerns about creating mandates requiring specific technologies. Speaking at a Senate Judiciary Committee hearing in February 2014 about data security and privacy, Federal Trade Commission Chairwoman Edith Ramirez said, "We don't recommend any particular technology. We think that any legislation ought to be technology-neutral."

EMV Chip Technology

What is EMV technology and why all the excitement about it?
Debit and credit cards with EMV (Europay, MasterCard, Visa) or "chip" technology are more secure than magnetic stripe cards. EMV cards have a microprocessor that protects your personal information through encryption—a process that scrambles personal and financial data to make it virtually useless to criminals. EMV cards also generate unique, random numbers to complete each transaction. If that information is stolen, it is useless, as the criminal cannot use it to conduct another transaction.

When will EMV chips be required?
Starting in October 2015, banks will be required to offer cards equipped with chip-based technology,

while retailers must have terminals capable of reading chip-based cards.

Will banks be ready by the October 2015 date?
Banks are already making significant headway in leading the EMV transition, with a total of 575 million EMV cards expected to be issued by the end of 2015.

Will retailers be ready by the October 2015 date?
Many large retailers are moving quickly to adopt EMV, but small businesses will have a particularly difficult time implementing the new technology. Javelin Strategy & Research estimates that only 10 percent of merchant terminals are EMV-enabled less than a year away from the deadline. A recent 2015 survey by ACI Universal Payments of 200 retail industry professionals concluded that: "Despite retailers' intent to increase investments in payments security, the survey found a notable lack of urgency regarding the migration to chip & PIN technology."

What happens if a bank or retailer doesn't comply with the transition to EMV?
Banks or retailers that are not using chip technology by October 2015 will assume liability for any fraud that occurs thereafter. Were fraud to occur with both parties in compliance with the EMV rules, the payments network (e.g., Visa, MasterCard, etc.) would determine which party must cover the cost of the fraud.

PIN or Signature?

What is the difference in safety between PIN vs. signature cards?
When EMV is fully deployed by banks and merchants, PINs and signatures will be an additional layer of security just as they are with magnetic strip cards today. It is the chip, however, not the PIN or signature, that makes EMV cards more secure. It's no different than how PINs and signatures are used with magnetic strip debit cards today.

Should PINs be mandated?
No. The PIN is a static number that will at some point be obsolete as more dynamic forms of security are deployed. It is also important not to create the impression that PINs fully protect customers.

Wouldn't consumers feel more comfortable with a PIN on their credit card?
Many customers prefer the convenience of completing a transaction with their signature. Customers should be allowed to choose what works best for them.

What is the downside to requiring a PIN?
The average person carries four cards—three credit cards and one debit card—meaning the typical consumer would be required to remember four different PINs or make themselves more vulnerable by using the same PIN for each card. Evolving mobile payment platforms are also moving away from static PINs and credit card numbers and towards biometrics. Requiring a PIN in addition to these security measures is unnecessary.

Are PINs susceptible to vulnerabilities for criminals to exploit?
Any secondary security measure will be the subject of attacks by hackers. If PIN is mandated, you can

be sure hackers will try to steal them. A report by the Federal Reserve Bank of Atlanta published in 2012 found that PIN debit fraud rates have increased more than threefold since 2004. There is also concern that PINs used with debit cards are directly linked to the person's bank account (e.g., through an ATM). So if a PIN is stolen during a transaction, it creates the possibility that the customer's entire account might be open to fraud.

Existing and Emerging Security Options

Are there other technologies designed to protect consumers?
Yes. Banks and payment networks are implementing new technologies that can adapt to new threats. End-to-end encryption and tokenization are technologies that are currently being rolled out while neural networks have been used for years to proactively keep consumers' data safe.

What are neural networks?
For years, banks have been using sophisticated and complex systems, and intensive employee training to fight against criminals. Neural networks are one type of system that banks use to detect unusual account activity. These systems detect fraudulent charges by learning their customers' behavior to determine if a customer's account has been hacked.

Tokenization has recently been in the news. What is it?
Tokenization is a technology that replaces sensitive consumer account information at the cash register or online with a random string of letters, characters and numbers called a "token." The token is only used for that one type of transaction, rendering the information less useful to criminals if that token is stolen. The tokens are reconnected with a person's account information in "token vaults," which exist behind strong security walls controlled by the bank or payment network. The result is that merchants do not hold the customer's account information, ensuring it cannot be accessed or stolen. This technology is an important feature for some mobile wallets, such as Apple Pay, and can be used online.

What is end-to-end encryption?
End-to-end encryption is a technology that uses sophisticated algorithms that encode a consumer's personal payment information into an unreadable form as that information makes its way from a merchant's checkout stand to a card network to your local bank, and back. A separate "key" is needed to unlock the encryption.

Mobile Payments

Who offers mobile payments?
The mobile payments landscape is crowded with a variety of participants from different industries. Financial institutions, retailers and start-ups are developing platforms to make mobile transactions. The best platforms will offer a good customer experience while protecting the data of the person using the device.

Do EMV chips, PINs or signatures help protect consumers with mobile payments?

No. EMV chip cards, PINs and signatures are ways to protect against fraud committed at the point of sale for purchases made in a store with a physical card.

What technologies exist to protect customers who use mobile payments?
Banks are constantly innovating new technologies that protect consumers on the newest payments platforms. One of the newest innovations that is now being implemented on mobile platforms is tokenization. For example, American Express recently rolled out tokenization for online, mobile app and in-store mobile purchases, and it is also an important feature of Apple Pay.

Have there been any data breaches on mobile payments?
The mobile app being developed by Merchant Customer Exchange (MCX) was breached last October by hackers who gained access to customer email addresses. MCX is a consortium of retailers that includes Wal-Mart, Rite-Aid, CVS and others.

Smart Security in a Changing Threat Landscape

Would a new law requiring all EMV cards to use PINs prevent fraud?
PINs are only a minor safety feature, and enterprising crooks are already finding new ways to capture and exploit them. This is why the banking industry is investing tens of millions of dollars into promising security innovations. While the industry is committed to providing chip technology, mandating the PIN component would hurt consumers by diverting valuable time and resources toward static technologies that could be proven obsolete the minute cyber threats change.

Will a mandate calling for a specific technology help consumers?
No. Mandates would require investments in technology that will quickly become outdated and unresponsive to the evolving threats. Worse, a government mandate may create the wrong impression that the consumer is secure, and will saddle consumers with static technology that ultimately makes them even more vulnerable.

Is there one solution that will prevent fraud?
No. There is no silver bullet in an environment where cyber crooks change tactics quickly. It is critical that vulnerabilities be eliminated, as the major data breaches at retailers such as Target, Home Depot, Neiman Marcus and others have shown. Inconsistent and outdated security standards that often characterize the cyber-preparedness of retailers need to be addressed quickly. All parties—banks, retailers and payments networks—have a vested interest in keeping the payment system secure and reliable. All parties need to work together to protect consumers and provide them with innovative and secure payment options.