Preventing Data Breaches: Smart Security in a Changing Threat Landscape

Dynamic Cybersecurity for the Future

Recent high-profile data breaches at retailers like Target and Home Depot underscore the critical need for stronger and more innovative security solutions that protect consumers.

***Dynamic solutions, not rigid one-size-fits-all mandates*:** Mandates stifle innovation in the private sector and hinder the ability to adapt and react to evolving threats. While the federal government may believe technology mandates are a way to ensure a level of security, the private sector—and more importantly, consumers — will be saddled with static technology that ultimately makes them vulnerable.

***Investing in security*:** Banks and payment networks continue to invest heavily in the development and implementation of promising new technologies capable of protecting consumers everywhere purchases are made.

***A common enemy*:** Both banks and retailers have a role to play in fighting criminal hackers who will never stop looking for new ways to steal consumers' data.

Chip Technology: Why it Works

Debit and credit cards with EMV (Europay MasterCard Visa) or "chip" technology 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. Whether the consumer signs for a purchase or enters a PIN, it is the chip technology that enables a more secure payment. Chip technology cards are:

More secure than magnetic stripe cards, because the chip generates unique data for each transaction. If that information is stolen, it won't be traceable back to the account.

Nearly impossible to replicate, thanks to the chip's ability to create a new, random number for each transaction.

Coming to a checkout terminal near you. Banks are already issuing chip cards, with 120 million cards expected to be in the hands of U.S. consumers by the end of 2014, and 575 million cards issued by the end of 2015. Javelin Strategy and Research estimates only 10 percent of merchants currently have terminals that accept EMV chips. By October 2015, banks must issue cards with chip capability and retailers must have terminals to accept them or they will be liable for fraudulent purchases made on the card.

It's the Chip that Matters

For cards with EMV chip technology, it's the chip that makes the card more secure.

A mandate, such as one requiring chip-enabled cards or PINs, does not prevent online or mobile fraud. Americans spent $263 billion online last year (most often without a PIN) and that dollar number is expected to grow to $414 billion by 2018. Less than 30 percent of merchants in the U.S. – both online and traditional storefronts – are currently equipped to accept a PIN: and some merchants prefer not to. As mobile technologies emerge, device passcodes and thumbprints are being introduced to benefit the consumer. Security should be dynamic, useful and address the realities of an increasingly digital economy, not be mandated to a single method.

A mandate could not have prevented the massive data breaches at Target, caused by hackers using malware to steal credentials through the company's heating, ventilating and air conditioning (HVAC) contractor. It also would not have prevented breaches at Home Depot, and Neiman Marcus, caused by

malware installed in checkout terminals. However, chip cards would have reduced the value of the compromised data by inhibiting the creation of counterfeit cards.

Criminals will always seek the weakest link. No single security feature is fail-proof. Creating a mandate around one static technology gives hackers an open invitation to exploit loopholes in the payments system.

No technology is fail-proof. Magnetic stripes have become more vulnerable over the years as criminals have found ways to skim the data stored in the stripe and replicate it to make fraudulent purchases. PINs have their own flaws. 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. When a PIN is compromised, it can open a backdoor for criminals to access and drain consumers' bank accounts at an ATM.

Beyond Plastic: Better Security, Wherever Purchases are Made

EMV chip technology will help protect customers at the register, but it's not a silver bullet. Expecting a single technology to successfully prevent all fraud is unrealistic, which is why banks and payment networks are implementing new technologies that can adapt and deploy in a changing threat landscape:

End-to-end encryption is helping make payments more secure, by encoding consumers' information into unreadable formats as it makes its way from checkout to card network to the bank and back.

Tokenization technology replaces sensitive consumer account information at the cash register or online with a random "token," rendering the information useless to criminals. This technology is an important feature for some mobile wallets, such as Apple Pay, and can be used online.

24/7 fraud protection is already a hallmark of banks, which employ teams of experts using advanced computer systems to monitor transactions and detect unusual activity indicating a customer's account has been hacked.

The Bottom Line: Fewer Mandates, More Collaboration

Mandates hurt consumers because they funnel valuable time and resources into static technologies that will become obsolete as cyber threats change.

A mandate could drive up the cost of doing business without addressing the fundamental cause of most future data breaches — inconsistent and outdated security practices within the retailers, which was the source of recent high-profile breaches at Target, Home Depot and others.

The security threat facing the payment card industry is a complex problem that cannot be solved by any single technology, standard, mandate or regulation. It cannot be solved by a single sector of society—businesses, standards-setting bodies, policymakers, and law enforcement—must work together to protect the financial and privacy interests of consumers.

To borrow a concept from Moore's Law of Innovation, every new technology is obsolete within 18 months. Data security technologies are no exception. Winning the war against cybercrime will take a forward-looking approach to preventing data breaches anywhere they occur— at the register, with a mobile phone or online. Money and resources should flow to the best technologies to fight these cyber attacks. Focusing on just one technology gives a false sense of security at a cost that everyone bears.