AGE VERIFICATION TECHNOLOGY SAFEGUARDS RETAILERS

NACS®
nacsonline.com
THE ASSOCIATION FOR CONVENIENCE & FUEL RETAILING
May2014

HALF COVERED

WITHOUT BOTH CHIP AND PIN, RETAILERS REMAIN VULNERABLE TO DATA BREACHES

THE NON-LIQUID FUELS MARKET

BASKET MISSION ANALYSIS BOOSTS COMMISSARY INITIATIVE

On December 23, 2013, Visa issued a press release reminding consumers of important security tips and fraud protections. "Regularly monitor your accounts, carefully review statements and notify your issuing financial institution promptly of any unusual activity. Studies have shown engaged consumers are less impacted by fraud," Visa instructed. "While identity theft is uncommon, it's always a good idea to regularly check your credit report for incorrect information."

If there were a way to definitively illustrate the exact opposite of proactive, this announcement would serve capably.

Approximately 38 days prior, on November 15, 2013, Russian hackers breached Target's network using credentials stolen from one of the mass retailer's vendors. More than 40 million debit and debit card numbers were compromised, along with personal information for 70 million consumers. And that breach came *four months after* data from 1.1 million customer payment cards for Neiman Marcus were stolen.

For consumers, the news was dispiriting on a number of levels. If the nation's third largest retailer (according to NRF data) could be hacked, where could one safely shop without risk of personal data theft? Indeed, Target is considered by many industry observers to be at the forefront of technological innovation. "Target is no ordinary retailer. It's long been among the most tech savvy," penned tech journalist Rocky Agrawal for *Venture Beat*. "Target had mobile payments before Starbucks ... In fact, the first Starbucks that accepted mobile payments were the Starbucks inside Target stores ... Its iPad app has full versions of the Sunday circular and the ability to make lists."

For convenience store operators, the Target breach triggered a sharp WTF reflex, followed quickly by a self-conscious head turn to see if any help was forthcoming. It's no wonder. The time and effort to pursue PCI compliance is a nagging chore for any retailer, with complexities and costs that — absent a breach at their store — seem punitive at best. But if Target can be breached, what's the point, is the collective lament. What's the point of pursuing these burdensome steps that are mandated by the card companies if the ultimate goal — data security — is futile?

COMPLIANCE ≠ RISK MITIGATION

The underlying problem, said Gray Taylor, executive director of Conexxus (formerly called PCATS) and payment consultant to NACS, is that a retailer's goal is fundamentally different than that of the card companies.

"PCI is really a liability shift strategy," Taylor said. "There are good guidelines as to risk mitigation. But it doesn't buy you anything as a retailer ... Target was breached because it [allegedly] didn't control all of its vendor passcodes. But it didn't have control over them." Rather than providing Target with true data security, Taylor said, PCI compliance provides it with a viable defense argument, which will just shift the blame elsewhere. And that's exactly what is transpiring.

In March, two banks, Trustmark National Bank of New York and Green Bank of Houston, filed suit against Qualified Security Assessor (QSA) Trustwave, alleging that the company failed to detect vulnerabilities in Target's handling of card data prior to its data breach. Qualified security accessor (QSA) comapnies are organizations that have been qualified by the council to have their employees

assess compliance to the PCI DSS standard. The suit claims Trustwave found Target to be in compliance with PCI standards last September, two months before the attack, without finding any vulnerabilities with the way Target handled card data.

"This is a trend that will continue, given the costs of a breach," Taylor said. "But I don't believe the banks will have standing, as their agreements with card brands outline their cost recovery in such an event." Rather, Taylor said, the real blame should point to the card companies.

"The product is designed by the cards — not by banks or merchants ... I would suggest that, like any other product, the product manufacturer would be liable. But [instead], the victim (in this case Target) gets punished."

HOUSE OF CARDS

The PCI Security Standards Council (PCI SSC), comprised of the major credit card companies, wouldn't comment specifically on the Target breach, only to clarify the organization's focus. "The Council's role is to develop and maintain standards," said Bob Russo, general manager of the PCI SSC, in an email. "Compliance is a separate matter and is managed by card brands and acquiring bank partners."

PCI EMPHASIZES THE WRONG THING: COMPLIANCE. WE DON'T CARE ABOUT COMPLIANCE, WE'RE FOCUSING ON RISK MITIGATION.

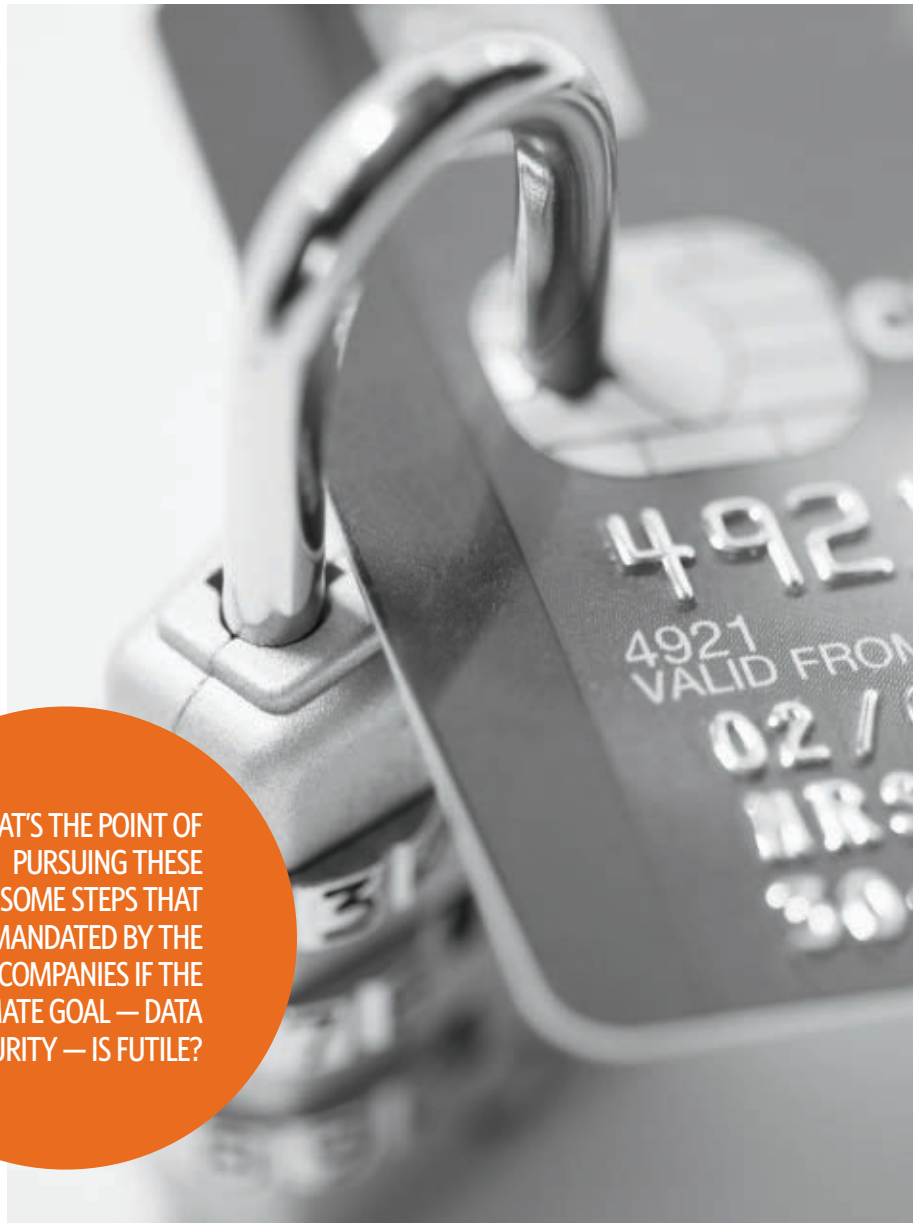
Therein lies the problem, Taylor said. "PCI emphasizes the wrong thing: compliance. We don't care about compliance, we're focusing on risk mitigation. The card brands are still focused on creating clean environments for card transactions but you can't have that in an Internet society. Target proved you can't have a clean environment."

CHIP ON THEIR SHOULDER

A major security-inspired fix is already underway, as the industry moves toward EMV adoption (See "A Chip on Their Shoulder" in the September 2012 issue of *NACS Magazine*). However, the process is slow with its own vulnerabilities. "Europe went through [the EMV transition] and it still took them 10 years," said Paige Anderson, director of government relations for NACS. "So it will take a decade to have everything up and operational, but by that time, we'll all be using our mobile devices for payment." Recall that EMV — a standard for credit

and debit card payments originally developed by Europay, MasterCard and Visa — incorporates an embedded chip rather than a magnetic stripe, a system indisputably more secure.

In the meantime, EMV will require significant equipment upgrades for store operators, both inside the store as well as at the gas pumps. And the cards are expensive, too, costing up to $2 per card, according to a CNN report, which is roughly 10 times more expensive to produce than magnetic stripe cards. "It's kind of a chicken and egg problem. Merchants need to make the upgrade, but do consumers have cards?" said Jason Oxman, CEO of the Electronics Transaction Association, to CNN.



CHIP, MEET PIN.

Even if — when — the EMV transition does occur, Anderson stresses the technology itself will still be vulnerable, absent a move away from signature. "If we're going to make the decision to make these [EMV] changes, let's make it as safe as possible."

WHAT'S THE POINT OF PURSUING THESE BURDENSOME STEPS THAT ARE MANDATED BY THE CARD COMPANIES IF THE ULTIMATE GOAL — DATA SECURITY — IS FUTILE?

To do so requires the adoption of PIN, something the card companies are loath to do. "In the signature world, Visa and MasterCard have the market locked up," explained Doug Kantor, partner for Steptoe and Johnson, a D.C. law firm. Not so when it comes to PIN, though. "In the debit world, there are several competitors for the network routing of those transactions, which reduces market share for Visa and MasterCard ... If it's a Visa card using signature, it only goes across Visa's network. But on the PIN transaction, the merchant sends it over different networks and the network gets a per-transaction fee that is separate from interchange."

To make sure signature has remained the industry standard, the card brands have provided incentives to consumers to use signature rather than PIN, such as offering contests that are open only to signature cards and assessing PIN fees. As a result, when a retailer tries to unilaterally introduce the more secure PIN transaction, consumers reject it. In 2003, Target introduced chip and PIN technology to its REDcard but ended the experiment after just three years, citing high costs and low consumer adoption. "[T]he technology at that time would have only been usable in our stores, making for a confusing experience for customers, overall," said John Mulligan, CFO of Target.

Even with chip and the more secure PIN rather than signature, experts say that's still not enough to maintain network security. There's a long process in between swiping a card and approval, and that chain of command is currently being overlooked. "Once the swipe occurs, data can be stolen at different points in the process," Anderson said. "We should be looking at end-to-end encryption and tokenization — [replacing the sensitive data with 'tokens' that are placeholders of the data] — so that if your network is breached, the data would be worthless."

WHAT NACS IS DOING

NACS is advocating on behalf of its members on Capitol Hill, but lawmakers have, to date, been unable to reach a consensus as to how to proceed. "They're worried that if they write technology into a law whether the law will be able to evolve with technology," Kantor said. "And they're also a little perplexed as to how to do it ... Not everybody believes legislation is the best place to incentivize an industry to act ... and nobody yet has put out real legislation as to what you do to prevent data theft in the first place."

While the topic began to gain traction on Capitol Hill in February, Kantor said the attention may be fleeting. "That depends on whether we see more breaches or not. There's a lot of interest in it now but it's a tough year to legislate and it's an election year. The success of legislative efforts may turn on whether there's more high profile data breaches that push the conversation or if things quiet down for a while, in which case some of the momentum may go away."

In the meantime, Target announced in February that it will deploy chip and PIN card readers at its stores, part of a $100 million POS transformation, and the retailer urged others to follow suit. "A reason the U.S. has been slow to embrace change is that all players in the payments system — merchants, issuers, banks and the networks — have not been able to find common ground on how to share the costs of implementation," Mulligan said.

> Even with **CHIP** and the more secure **PIN** rather than signature, experts say that's still not enough to maintain network security. There's a long process in between swiping a card and approval, and that chain of command is currently being overlooked.

To understand why, one need only look at the numbers. According to advisory firm Sonecon, financial institutions earned $41.2 billion from credit card swipe fees in 2012 while losing just $5.33 billion to fraud, according to payment industry newsletter *The Nilson Report*.

Such an imbalance is why the card companies continue to act like regulators, Taylor added, which is why "it's time to break that up ... What happened at Target does not have to happen at your store, but it will take an overhaul and cooperation of the entire payment system.

"Target is a victim here, don't forget that," Taylor said. "We need to mitigate risk, and to do that, we must steer our outrage to a reasoned conversation about how all the stakeholders can make a better payment system." NACS

Jerry Soverinsky is a Chicago-based freelance writer and a NACS Magazine *and* NACS Daily *contributing writer.*