Fighting Fraud In An EMV World

by Steve Brown

We are now 21 days past the deadline for EMV compliance. That date was set by major credit card companies of MasterCard, Visa, Discover and American Express. It was an agreed upon date when the entity that is the least EMV compliant (the merchant or the card issuer) assumes liability for counterfeit card fraud for card-present transactions. Well that is the idea anyway.

Interestingly, with just one day to go before the deadline, USA Today reported a survey found 60% of US card holders didn't even have chip-enabled credit cards in their wallets yet. Even worse perhaps, the survey found that despite 2Ys of advance warning of the change, only 27% of merchants in the US said they would be able to process chip-enabled cards by the deadline. This is truly sad when you consider the purpose of the switch is to enhance consumer security. Changing something so massively embedded in our country just isn't easy it would seem, so we will all have to be patient.

You have probably heard a lot about the security benefits of chip cards. It's true that they are harder for thieves to counterfeit because of the technology embedded within them, but thieves are still finding ways to worm their way in. These cards are not immune to fraud, so care must still be taken.

One type of malware for instance is so called "RAM-scraping," which is a particularly pervasive type of fraud. It has the potential to continue wreaking havoc with chip cards. RAM-scraping malware assaults the memory inside point-of-sale (POS) devices. It was this type of attack at the heart of the 2013 Target holiday-time breach and the chip wouldn't have helped.

Here's how RAM-scraping malware attacks work. Even though payment data is normally encrypted when it is transmitted, received or stored, it is nonetheless decrypted in the POS's RAM for processing. That's where the malware hits, allowing thieves to capture the payment data and use it for their own illicit purposes.

Some banks may erroneously believe that RAM-scraping malware attacks can't happen in an EMV environment, but security experts like Trend Micro say the possibility still exists, because decrypted data still resides in the systems' RAM. As a recent report by the security company deftly points out, EMV was developed to prevent credit card counterfeiting, not POS RAM-scraping, so be aware and alert.

RAM-scraping malware attacks can also occur when you swipe your card at an EMV-enabled POS terminal instead of inserting it. When you swipe a chip card, the payment terminal should refuse it and ask you to insert it in the smart card reader instead, but that doesn't always happen. The data on the magnetic strip can be compromised by RAM-scraping malware and used by thieves to create counterfeit magnetic strip cards.

There are other examples of potential attacks involving chip-equipped payment cards that banks need to be aware of. Researchers from the University of Cambridge have reported that attackers can

easily construct special devices to intercept and modify communications between EMV credit cards and POS terminals in order to authorize rogue transactions.

There have also been recent examples of EMV "replay" attacks, where attackers have reportedly pushed regular magnetic strip transactions through the card network as EMV purchases, duping banks in the process. The lesson here is clear: point of sale codes can be manipulated by fraudsters, so it's especially important that banks implement EMV protocols carefully and have solid authentication procedures.

Make no mistake, fraudsters are going to continue finding ways to test the limits of EMV, so banks need to keep their defenses up. Letting down your guard when new technology is rolling out nationwide is a risky proposition.

BANK NEWS

Technology Costs

Deutsche Bank research finds the average bank spends about 7.3% of revenues on IT costs vs. about 3.7% for other industries. Meanwhile, because data here is hard to come by as reporting it is not required, McKinsey research finds bank IT costs run about 4.7% to 9.4% of operating income.

ROE Analysis

Using FDIC data through Q2 2015, we find the median ROE for banks <$10B has declined almost 30% from the 2000 to 2005 period (11.6%) compared to 2010 through Q2 2015 (8.3%). Meanwhile, the median ROE for banks <$1B has declined about 31%, going from 10.6% to about 7.3%.

Cyber Breach

A PwC survey of IT and security decision makers at companies worldwide finds enterprises reported a 38% increase in detected breach incidents (this year vs. last year); saw a 565 increase in intellectual property theft; and reported a 28% increase in breaches attributed to current and former partners and suppliers (to 59% total).

No Debt

USA Today reports 67% of people age 18 to 34 surveyed say having no debt is a top priority; 64% have savings; and 60% of those who are college educated say they feel somewhat satisfied with their current finances.

Business Survey

A survey by Duke University of US CFOs finds: they expect earnings growth of 3.0% in the next 12 months; about 26% say they plan to acquire another company; 93% say they have job openings in key positions; 50% of those say they find it difficult to fill key positions; and 55% say that firms in the finance, tech, and energy industries are not adequately managing downside risk.

Settlement

Fifth Third Bancorp ($139B, OH) has agreed to pay $85mm to settle fraud charges related to FHA insured loans. The bank originated loans it later found to be defective under post-closing quality reviews, but did not immediately report them to HUD and only disclosed them after a whistleblower complaint was filed.