Preparing for the Change to EMV and New Fraud and Security Risks: What U.S. Merchants Need to Know
Introduction

Recent large-scale data breaches and growing rates of credit card fraud have some U.S. merchants accelerating their efforts to transition to the Europay, MasterCard, and Visa (EMV) global standard. Merchants who are EMV compliant are able to process “chip and PIN” credit and debit cards in card-present channels, such as point-of-sale (POS) terminals at retail locations, through secure EMV transactions. These plastic payment cards, which contain a computer microchip, can help to reduce fraud in card-present channels because the microchips are virtually impossible to duplicate.

Transitioning to EMV requires merchants to make a significant investment in new technology infrastructure, including implementation of dual-interface terminals at the POS for processing both chip-and-PIN and magnetic-stripe cards. Unlike traditional card processing at the POS, where customer data stored on magnetic-stripe cards is read when the card is swiped in the card reader, a unique and un-reusable “digital signature” is generated for authentication purposes with every EMV transaction. In addition, in an EMV transaction, a customer’s PIN (personal identification number) is protected with encryption, which is enabled by the card’s microchip.

EMV has already been adopted in Australia, Canada and Europe, and other countries are currently migrating to the standard. Major card brands (American Express, Discover, MasterCard and Visa) have been pushing in recent years to get EMV-enabled cards out to consumers in the U.S. market. To help incent U.S. merchants to embrace the costly undertaking of becoming EMV compliant, Visa launched a Technology Innovation Program (TIP) in 2012 that allows merchants that update their POS infrastructure to waive their obligation to complete an annual Payment Card Industry Data Security Standard (PCI DSS) validation assessment; however, these merchants still need to be PCI DSS compliant.¹

Beware the Liability Shift

Although there is no mandate for U.S. merchants to become EMV compliant, there is a deadline they all should be fully aware of: October 1, 2015. This deadline, set by the major card brands, is the date for the so-called “liability shift” of counterfeit transactions. This is what it means: If U.S. merchants are unable to process EMV transactions by the October 1 deadline, but still accept transactions with EMV-compliant cards (i.e., swiping chip-and-PIN cards with non-EMV compliant devices), they will assume 100 percent liability for all fraudulent transactions. This means merchants are responsible for all fraud chargebacks.

This white paper provides an overview of the potential implications of EMV for U.S. merchants, including new risk areas, and offers tips for making a successful transition to the new standard.

UNDERESTIMATING OTHER EMV-RELATED RISKS

Many U.S. merchants have been slow to embrace the EMV standard, primarily because becoming compliant is so expensive and time-consuming. For some merchants, the process of updating POS technology could involve hundreds or even thousands of stores. Some merchants are also at the mercy of third-party providers that supply their POS solutions; they must wait for these vendors to update their codes or applications in order to handle EMV transactions.

Two other factors have prevented many U.S. merchants from focusing their attention and resources on EMV compliance. One is meeting the new, mandatory PCI DSS 3.0 requirements, which took effect January 1, 2015. The other is the need to respond to increasingly sophisticated and frequent attacks by hackers, including recent high-profile attacks that have affected millions of consumers.

Chargeback Fraud

Even with the October 1, 2015, liability shift deadline now only months away, many merchants do not appear to be picking up the pace to become EMV compliant. More than likely, this is because they do not see full liability for chargebacks as a significant risk, as they are only dealing with a low volume of chargeback activity at this time. This is a potentially serious underestimation of future risk.

Chargeback fraud is likely to increase dramatically once consumers realize that merchants have no recourse to dispute charges made with an EMV-enabled card in a card-present channel that was not processed as an EMV transaction. Non-EMV compliant merchants that sell expensive goods, such as electronics or jewelry, through card-present channels could be particularly at risk for chargeback fraud.

CNP Fraud

Another potential EMV-related risk for U.S. merchants: an increase in the rate of card-not-present (CNP) fraud. It is important for merchants to understand that EMV is designed to help reduce fraud in card-present channels only – for example, when a customer uses a chip-and-PIN card at an EMV-enabled POS terminal at a store location. However, EMV is not intended to help reduce fraud in CNP channels such as e-commerce, mobile and call centers.

U.S. merchants can expect to see CNP fraud surge – as it did in the United Kingdom, for example, following implementation of EMV in 2001 – as criminals shift their focus toward compromising users through these less-secure payment channels.

Mobile is poised to become a particularly active attack vector. More consumers are looking to pay for goods and services using their mobile devices. And because the mobile payment channel is still very new, it is somewhat immature from a security perspective, since mobile coding standards and other security measures are still being developed.

Merchants investing in new technology to become EMV compliant may want to take the extra step to invest in technology that can accommodate emerging mobile pay options, like Apple Pay; this will help them avoid an additional upgrade in the near future.


EMV AND P2PE: BETTER TOGETHER

U.S. merchants moving to embrace EMV also must understand that implementing EMV technology is not the same as implementing point-to-point encryption (P2PE) technology.

According to the PCI Security Standards Council, validated P2PE solutions, when correctly implemented, “may simplify merchants’ PCI compliance programs by eliminating clear-text cardholder data from their environment and reducing the scope of PCI DSS requirements.”

With P2PE, a consumer’s credit or debit card information is encrypted at the point of swipe and directly transmitted to a P2PE vendor for authentication. Because of the way the data is encrypted and handled in the P2PE process, credit card companies and banks allow the merchant to consider that data as no longer being cardholder data. This means the merchant does not have to protect the data – and the merchant’s downstream liability is therefore reduced.

When investing in EMV technology, it is recommended that merchants invest in a P2PE solution at the same time, so they can become EMV compliant while also reducing their PCI scope.

PREPARING FOR EMV

Implementing new technology to support EMV transactions, and working with POS vendors that are EMV-enabled-ready, are critical steps toward making a successful transition to EMV compliance. However, while the technology component of the process can be very resource-intensive, it should not overshadow the need for merchants to focus on potential EMV-related risks. Merchants must:

• Not underestimate the substantial financial burden of increased chargeback fraud that will likely arise after the October 1, 2015, “liability shift” by major credit card companies.

• Ensure that CNP channels are adequately protected, because it is essentially guaranteed that adversaries will expand efforts to compromise users through these less-secure channels. Merchants should therefore look to increase testing of CNP channels and focus on strengthening web application and mobile security.

• Recognize that EMV does not make their network more secure or prevent data breaches. If networks are not secure, data breaches are a risk. Merchants will face the same penalties and liabilities they have today if they are found to be the source of a breach.

To make a successful transition to the EMV standard while reducing risk, U.S. merchants should consider working with third-party experts who can provide guidance on EMV strategy; identify and evaluate both EMV and P2PE solutions; help oversee the implementation of EMV technology; and assist in hardening and testing of e-commerce environments and mobile technologies, especially in CNP channels.

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Named one of the 2015 Fortune 100 Best Companies to Work For®, Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Our IT Consulting Practice

Our global IT Consulting practice helps CIOs and IT leaders design and implement advanced solutions in IT governance, security, data management, applications and compliance. By partnering with us, you ensure that your IT organization performs with the same focus and excellence with which you manage day-to-day business operations. We will work with you to address IT security and privacy issues and deploy advanced and customized application and data management structures that not only solve problems, but also add value to your business.

Our comprehensive suite of IT consulting services covers three main areas of focus to help our clients leverage technology to address critical business priorities:

• Technology Strategy & Operations
• Security & Privacy
• Enterprise Application Solutions

For more information about the issues discussed in this white paper or about Protiviti’s IT consulting services, please contact:

Scott Laliberte  
+1.267.256.8825  
scott.laliberte@protiviti.com

Jeffrey Sanchez  
+1.213.327.1433  
jeffrey.sanchez@protiviti.com