EMV CHIPS CHALLENGE IN-STORE FRAUD, FRAUDSTERS MOVE TO TARGET WEAKEST LINK

Strategies for protecting eCommerce against the rise of digital attack

The EMV (Europay, MasterCard® and Visa®) secure payment standard was implemented by leading U.S. payment networks in October 2015, and is considered to be the global technology standard for reducing credit and debit card payment fraud in card-present, or device-present transactions. The EMV payment instrument, whether it is a card, mobile phone or other device, has an integrated microprocessor chip—as opposed to only a magnetic stripe—that stores and safeguards cardholder data using encryption.

The U.S. was one of the last developed nations to launch EMV, but a benefit of being near-last is that payment networks knew the potential for increased online payments fraud based on the events that ensued following introduction in early adopting countries.

**Good news for U.S. EMV adopters**

Since the fraud liability shift was implemented in the U.S. making businesses that do not yet accept chip cards potentially liable for certain types of fraud, EMV adoption is still growing among businesses, although not as quickly as the payments industry anticipated. Still, early data proves that EMV is having a positive impact in the U.S. on reducing fraud in brick-and-mortar, point-of-sale, card present transactions. This is because the additional level of authentication inherent with EMV increases the security of payment transactions thereby reducing fraud opportunity. Dynamic, real-time authentication addresses the vulnerability of static magnetic-stripe cards with safeguards against card skimming -- a prevalent security threat where fraudsters copy card data using simple and inexpensive card readers – as well as cloning.

Plus, chips are capable of conducting real-time risk assessments for card purchases based on the card user’s profile. So EMV technology can alert banks if the card or transaction has been modified. For businesses, this means the likelihood of accepting a counterfeit, lost or stolen card and being held liable for a fraud-related chargeback is greatly reduced using EMV cards in conjunction with EMV-capable card terminals. Another benefit is that most U.S. credit and debit cards issued are now on par with payment systems in Europe, Canada and beyond, increasing security and card acceptance when traveling.

Continued
Worldwide Chip Card Deployment and Adoption*

<table>
<thead>
<tr>
<th>Region</th>
<th>EMV Cards</th>
<th>Adoption Rate</th>
<th>EMV Cards</th>
<th>Adoption Rate</th>
<th>EMV Cards</th>
<th>Adoption Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada, Latin America, and the Caribbean</td>
<td>471M</td>
<td>54.2%</td>
<td>544M</td>
<td>59.5%</td>
<td>680M</td>
<td>71.7%</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>942M</td>
<td>17.4%</td>
<td>1,676M</td>
<td>25.4%</td>
<td>2,459M</td>
<td>32.7%</td>
</tr>
<tr>
<td>Africa and the Middle East</td>
<td>77M</td>
<td>38.9%</td>
<td>116M</td>
<td>50.5%</td>
<td>160M</td>
<td>61.2%</td>
</tr>
<tr>
<td>Europe Zone 1</td>
<td>794M</td>
<td>81.6%</td>
<td>833M</td>
<td>83.5%</td>
<td>881M</td>
<td>84.3%</td>
</tr>
<tr>
<td>Europe Zone 2</td>
<td>84M</td>
<td>24.4%</td>
<td>153M</td>
<td>40.4%</td>
<td>200M</td>
<td>52.3%</td>
</tr>
<tr>
<td>United States</td>
<td>-</td>
<td>-</td>
<td>101M</td>
<td>7.3%</td>
<td>394M</td>
<td>26.4%</td>
</tr>
</tbody>
</table>

*Above statistics from EMVCo (https://www.emvco.com/about_emvco.aspx?id=202) show worldwide EMV deployment as of Q4 2013, 2014, and 2015. The figures represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by member financial institutions globally.

eCommerce vulnerabilities exposed – the shift in U.S. payment fraud

EMV does not provide protection against fraud in card-not-present (CNP) transactions, and criminals will usually elect to target the weakest link, which remains magnetic stripe only cards and the digital commerce space. In 2016, omnichannel services provided by U.S. merchants grew by 300 percent over 2015¹. A recent study by Forter, a fraud prevention company evaluating online commerce, and the Merchant Risk Council revealed that domestic orders are 79 percent riskier now than in 2015². Again, this is because EMV is making it more difficult to commit fraud in card present transactions and criminal activity is migrating online and becoming more organized and sophisticated. Another fact to consider is that criminals in countries with EMV already firmly established have pretty much run the gamut of online fraud in those countries with businesses that have instituted stronger online protections.

To date, retailers in the U.S. remain vulnerable to fraud in card-present transactions and will remain so until the EMV technology standard is fully deployed over the next 3 to 5 years. History and statistics aside, businesses engaged in online commerce or omnichannel services can leverage safeguards available that protect their business and their customers.

Fighting back: Protecting your business and your customers in eCommerce

Strategies for brick-and-mortar and omnichannel businesses

America’s slow adoption of EMV technology likely explains why the U.S. is responsible for 47 percent of the world’s card fraud, though the U.S. only accounts for 24 percent of total worldwide card volume, according to research from Barclays. Barclays also found that when the UK first deployed chip cards, counterfeit fraud was reduced by 70 percent from 2005 to 2013. The takeaway is that if you engage in brick-and-mortar only or omnichannel sales, implement EMV technology as soon as it is feasible to do so to protect against card present fraud schemes and comply with the fraud liability shift.

Incorporate the implementation of EMV technology into your business plan. Take all aspects into consideration. After determining how best to upgrade your systems, get a clear picture of the cost, as well as the time from initiation to full implementation. If you have installed point-of-sale (POS) devices or readers in the last few years, it is highly likely that those devices are already capable of accepting chip-enabled cards; if you haven’t yet replaced legacy devices, it makes good business sense to seize the opportunity. Doing so will most likely solve for issues that could potentially arise down the road that would result in fraud, reputational and/or customer loss.

The longer you wait to adopt EMV, the more vulnerable to card-present fraud your business becomes, as fraudsters are set to continue targeting the weaker magnetic stripe only cards. It just makes good business sense to mitigate or eliminate unnecessary vulnerability and risk where possible, and EMV technology is a means to that end. Once deployed, omnichannel businesses need to look beyond POS terminals and closely evaluate their ecommerce policies, processes and protections.

Continued
**Strategies for protecting sales and customers online**

Begin with the basics in order to determine what you can change to protect physical systems and clients. Educate yourself and your employees about the many types of online fraud. Then take a look at best business practices for your technology, evaluate compliance and check to ensure that you are taking advantage of all common sense security measures to protect your business and your customers.

**Educating yourself and your employees**

Make sure associates are well versed in the basic types of ecommerce fraud so they are more equipped to recognize and prevent fraudulent attempts. Are employees savvy to account takeover and identity theft, and do they follow best practices to prevent fraud?

- **Account takeover:** If your ecommerce store retains personal customer information, purchase history or financial data, this information can be compromised through stealing data that is not properly secured or through phishing schemes. With phishing, your customers can be duped into revealing access information like user names and passwords. The fraudsters can then log in to your customers’ accounts, change passwords and make unauthorized purchases.

- **Identity theft:** Simply stated, identity theft is the fraudulent acquisition and use of customer data – a person’s private identifying information – most often for the purpose of financial gain. This can occur when data is not adequately secured or through hacking.

- **Chargeback fraud:** This occurs when a customer makes an online purchase using a credit card and then disputes the purchase with the card issuer once the goods are received. Chargeback fraud is often perpetuated by either the true cardholder or someone in relation to the cardholder with access to the card.

In addition to phishing and hacking risk, businesses are also exposed to loss if a fraudulent payment is accepted. Consider the following best practices for protecting your business and your customers in the digital space:

**SIMPLE STEPS TO TAKE:**

- **Review online orders for red flags:** Know your customer first and foremost and watch for red flags. Does the email address appear fake or suspicious? Do billing and shipping addresses match or are they geographically far apart; does the billing address match the IP location? Are contact details complete? Review any orders that are out of the ordinary. Watch for suspiciously large orders; shipping address anomalies where multiple orders from different customers are shipped to the same address, requests to change a shipping address after an order is placed, and orders shipping to P.O. boxes. Also check international orders closely, although it is just as important to watch domestic orders for suspicious activity given increased vulnerabilities for ecommerce. If something with the order is suspicious, contact the client by calling or emailing to verify details.

- **Monitor business accounts and reconcile daily:** Not only will monitoring and reconciling help you spot any anomalies, you will have a better handle on cash flow for making more informed business decisions.

- **Implement transaction controls:** Consider reviewing customer order trends and revenue to reasonably limit the number of purchases and the total dollar value per purchase, per account daily. This will limit your fraud exposure in turn. Also consider limiting the number of declined transactions.

- **Require strong passwords to authenticate your eCommerce gateway:** Do you require a maximum number of characters for passwords, and are numbers or special characters also required for access? Your software should have integrated verifications for access parameters.

- **Retain a file of fraud, fraudsters and fraudulent attempts:** By verifying against historically negative transaction information future fraudulent attempts can be mitigated. Check for every aspect of customer data that has previously been related to fraud.
Technology:

- **Replace legacy systems:** Does your business review transactions manually, or are your payment acceptance systems old? If so, consider replacing antiquated systems that are most vulnerable to fraud with newer technologies that have the ability to analyze transactions in real time or are capable of leveraging behavioral analytics.

- **Payment processing systems:** Ensure that payment acceptance systems compare payment information against Card Verification Value (CVV) and Address Verification Systems (AVS).

- **Keep software up-to-date:** Are you running the latest operating systems that include current malware and virus protections and security patches? Separately, make sure you are running the latest business suitable versions of anti-malware and anti-spyware.

- **Maintain the latest version of shopping cart software:** Check with your vendor to ensure you are enrolled in automatic updates.

Compliance:

- **Payment Card Industry Security Standards Council (PCI SSC) Compliance:** Review PCI SSC standards to ensure your ecommerce practices are compliant as mandated. Otherwise, customer data could be at high risk, and your business could be heavily fined should a breach occur. Not sure whether your business is compliant? See the PCI SSC website at www.pcisecuritystandards.org/pci_security/educational_resources.

Regardless whether your business consists of a physical location or you are an online retailer or a combination of the two, fraud exposure can be reduced by leveraging best practices. It is important for your business to remain receptive and adaptable to new technologies as well to stay ahead of criminals, particularly when it comes to digital vulnerabilities. A little time or monetary investment spent now can safeguard against potentially large financial, reputational or customer losses down the road. Always follow best practices for online security. See regions.com/stopfraud for tips.

**Haven’t adopted EMV yet?**
Visit http://www.gochipcard.com/merchant/ -- a resource created by the EMV Migration Forum to help educate business owners and their customers about chip cards.

**Learn more**
For more about EMV technology, the fraud liability shift, or the Regions Commercial Card program, contact your Regions representative or email RegionsCommercialCardServices@regions.com. Or, for more about fraud prevention or merchant service solutions, contact your Regions relationship manager or Treasury Management officer.

**By the numbers**

Did you know that online fraud attacks increased by 137% between the second quarter of 2015 and the first quarter of 2016, the period just after EMV introduction in the U.S.?

Fraud attacks also increased by 27%.

---
