Chip cards are here. What’s next?

While slower than expected, EMV (Euro Mastercard Visa) chip card adoption in the U.S. has been steady since the October 2015 liability shift. Since then, merchants that don’t support EMV are liable for any fraudulent card transactions that occur at their point of sale machines.

In May 2016, Mastercard© reported that 68 percent of its cards were chip enabled and 1.4 million merchant locations were accepting them. Similarly, Visa reported more than 300 million cards in use at 1.2 million locations.¹ The use of EMV in the U.S. is expected to increase in the near future.

The Payments Security Task Force estimates that 98 percent of all cards issued will be chip enabled in 2017.²

Consumers are also responding positively to the change. Of those who use chip-enabled cards, 59 percent say they are satisfied with EMV technology.³ Processed in a manner similar to magnetic stripe versions, EMV cards are just as convenient but offer a heightened level of security and some added peace of mind. Consumers are ready and willing to use the cards, with only 12 percent complaining that not enough stores accept them.³ This is good incentive for merchants who are still building a business case for EMV adoption.

EMV is intended to reduce in-store fraud, and appears to be accomplishing its goal. The beauty of the technology is that it prohibits counterfeiters from duplicating card data. When combined with a PIN, EMV is an almost foolproof way to validate cards and their users.

**EMV is the first line of defense in card payment security**

According to Mastercard, the dollar volume of counterfeit fraud at EMV-enabled merchant sites dropped by 27 percent year-over-year in January 2016.²

While some merchants have migrated to EMV and are reaping the benefits, others remain undecided. This is understandable given the cost, time, and resources that technology improvements often require, as well as the operational impacts they might have.

*Continued...*
Should all merchants implement EMV? Yes, and here’s why:

- Forty percent of all financial fraud last year was related to credit cards. Experts believe failure to widely adopt EMV is one reason card fraud is still so high in the U.S.
- EMV technology has proven effective in fighting counterfeit fraud for merchants who use it.
- Fraudsters will continue to find and exploit any careless card security measures they find, including non-EMV compliant systems. Merchants will be increasingly liable for any associated losses — not card issuers.

Adopting EMV card technology makes good business sense

Merchants need to protect themselves from loss of revenue. Consumers expect secure transactions and confidential handling of their financial data. EMV provides a critical first step by providing security at the point-of-sale.

Triple the threat protection

Protecting data at merchant sites is just one important aspect of payment security. Losses can also include data theft and subsequent reputation damage.

There were 980 data breaches in 2016 affecting more than 35 million records. As fraudsters continue to target data, merchants must be prepared — not only to protect against future threats, but to mitigate the consequences of previous attacks. Furthermore, an increasingly complex regulatory environment demands strict adherence to the Payment Card Industry (PCI) Data Security Standard.

A multi-layered approach that combines EMV with point-to-point encryption and tokenization is an effective way to mitigate transactional and data risks, as well as to ensure PCI compliance.

### EMV vs. Tokenization vs. Point-to-Point Encryption

<table>
<thead>
<tr>
<th>EMV</th>
<th>Tokenization</th>
<th>Point-to-Point Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrate card terminals to protect against counterfeit card fraud at the point of service.</td>
<td>Return random numbers (tokens) to the point-of-sale so card numbers are never stored there and can be used for subsequent transactions.</td>
<td>Your provider secures data throughout the entire transaction loop, from card swipe to data processing.</td>
</tr>
</tbody>
</table>

While a strong security architecture prepares merchants for present and future risks, further investment in insurance coverage — to protect against losses in the event of an actual breach — can provide an extra level of confidence.

For help with securing your card payments and consumer data, contact your U.S. Bank Relationship Manager.

---

1 Stores Magazine, U.S. Transition to EMV Chip Cards Trudging Along, July 11, 2016
2 PaymentSource, EMV is Winning the Battle Against Fraud, Dec. 22, 2016
3 CreditCards.com, Poll: 70 Percent of Consumers Now Have EMV Chip Cards, March 2016
4 Statistic Brain, EMV Credit Card Fraud Statistics, Sept. 4, 2016
5 CreditCards.com, 8 FAQs About EMV Credit Cards, Dec. 20, 2016
BEC evolves to target money and confidential data

Business Email Compromise (BEC) instances are increasingly more rampant and profitable for criminals. The FBI Internet Crime Complaint Center (IC3) reported over $3 billion in exposed losses and over 22,000 victims between January 2015 and June 2016.

Phishing, the method that scammers often use to compromise emails, has been around for decades, targeting both individuals and businesses. High profile BEC incidents reported in recent years have generally involved wire transfers and payment-related schemes aimed at corporations.

While the IC3 doesn’t see any decline in reported attempts and instances of BEC, it also reports that attacks are evolving in nature and motivation. New scams targeting businesses are especially prevalent in the early months of the year, when employees are preparing to file their tax returns. A newer variant attempts to obtain employee information, specifically W-2 or Personally Identifiable Information (PII). Recently, the IRS issued an urgent alert to warn employers of the increasing impact of the W-2 scam as it targets more industries and organizations. Essentially, every business can assume to be a potential target.

These PII phishing attempts are aimed at human resources or payroll departments, unlike past payment scams targeting finance or payments. These new targets may be less prepared to identify and respond to phishing attempts. In a recent, urgent alert, the IRS indicated that there has been a rise in instances where scammers are coupling the PII and wire transfer scams through one BEC.

In each phishing scenario, the initial target is the same: an employee. A successful attack requires only one employee to open an email and follow the instructions, whether clicking a malicious link or attachment or sending actual payments or data. In some reported cases, employees receive a follow-up phone call, to impose a sense of urgency and make the scam seem more believable. It is increasingly important that a healthy cybersecurity program permeate throughout all departments in organizations.

This security culture needs to start at the top, and security awareness training should be provided to all employees and contractors.

Continued...
Here are some important steps you can take to get started:

1. Review policies for e-mail use, receipt of payment instructions and handling of confidential data. Determine whether there is appropriate communication of policies and amendments to policies to all employees.

2. Develop procedural guidance where necessary to enforce policies. All levels of the organization need to adhere to policies and procedures without exception.

3. Encourage a security mindset. Remind employees of the importance of security, and recognize and reward them for exercising the appropriate level of skepticism in receipt of actual phishing attacks and internal phishing tests.

4. Establish an incident response and management process. Communicate incidents immediately. When appropriate, contact local law enforcement and/or the IC3.

5. Notify your bank as soon as possible if you discover a fraudulent transaction has been sent as a result of a compromise.

If you've been a victim of identity theft through a data breach, visit www.IdentityTheft.gov where you can report the incident and receive a recovery plan.

To learn more about how you can protect your organization from BEC, contact your U.S. Bank Relationship Manager.
Stop payment fraud in its tracks

Conducting business in a hyper-connected world has many benefits, but it can also be precarious.

In the current threat landscape, fraudsters are becoming more ruthless and sophisticated. They exploit vulnerabilities before software providers identify them using zero-day attacks, and make headlines with exorbitant payment thefts. Often after an attack, investigations and forensic analyses determine fraudsters that may have been lurking in the network undetected for long periods, reviewing employees’ activities and behaviors or moving laterally through system resources in search of more privileged access.

Check fraud remains predominant, but electronic payment fraud is becoming more common. According to the Association of Financial Professionals 2016 Payments Fraud and Control Survey, wire fraud exposure increased from 27 percent in 2015 to 48 percent in 2016.

It’s time to perform a payments risk assessment and control review for your organization.

A payment environment with layered prevention and detection controls can help fight fraud before an incident occurs. When considering the effectiveness of your controls, it’s important to understand where the risk of fraud exists in your unique payment environment.

- **Understand the process.** Identify payment initiators and approvers, and track the flow of payments from individual users’ desks and IT systems. Review payment monitoring activities to determine if they’re sufficient to catch an anomaly. After any process risks are identified, conduct a gap analysis to determine whether current policies and system controls can carry out a new mitigation strategy.

- **Review system security.** Network and software security are crucial elements for safeguarding your environment from intruders.

- **Review user security,** including standard and privileged access to sensitive systems. For workstations with financial software, limit the ability for personal use and web surfing. Review password requirements and methods for accessing online resources remotely. Consider requiring multifactor authentication to access sensitive data or resources.

- **Check for system updates and patches** and ensure systems are up to date. In addition to intrusion prevention and detection software, consider using IBM Trusteer Rapport to identify and defend your system from financial malware. U.S. Bank offers IBM Trusteer Rapport to SinglePoint® customers at no cost.

*Continued...*
SinglePoint security settings, when enabled and used correctly, further strengthen payments security. Multi-level approval options allow administrators to set payment limits for approvers. Dual authorization requires approvals from two separate authorized individuals prior to submitting a payment. System messages, such as notifications of payment initiation or approval, alert users to activities occurring within SinglePoint. System processing reviews payments to filter out possible illegitimate transactions.

SinglePoint requires multiple levels of authentication for certain services, such as ACH and Wires Money movement and authorization is automatically revoked from users after an extended period of inactivity. Contact your U.S. Bank representative for more information about SinglePoint security settings.

Re-evaluate risks and controls as needed
Understanding the motives of fraudsters and performing a risk and controls review are essential first steps, but the best defense will evolve as threats become more sophisticated. Stay informed of current trends in cybercrime so you can continually enhance your secure payment strategy.

Continued...
Consider using the following resources to stay up to date with the threat landscape:

- https://fbi.gov/investigate/cyber
  The FBI is the lead federal agency for investigating cyberattacks by criminals, foreign adversaries and terrorists. The FBI outlines valuable best practices and key cybersecurity priorities to help strengthen a defensive posture for organizations and individuals.

- https://msisac.cisecurity.org
  The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a focal point for cyber threat prevention, protection, response and recovery for state, local, tribal and territorial governments. The MS-ISAC 24/7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.

- https://www.fsisac.com
  The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the only industry forum for collaboration on critical security threats facing the global financial services sector. When attacks occur, early warning and expert advice can mean the difference between business continuity and widespread business catastrophe. Members of the FS-ISAC receive timely notifications and authoritative information specifically designed to help protect critical systems against physical and cybersecurity threats.

- https://www.nascio.org
  The mission of the National Association of Chief Information Officers of the United States (NASCIO) is to foster government excellence through business practice, information management and technology policy.