

BATTLING CARD FRAUD THROUGH CHIP AND PIN TECHNOLOGY



EMV adoption is widespread globally and gaining traction in the United States

With debit and credit cards continuing to make attractive targets for criminals, financial institutions (FIs) have to continuously evolve their fraud-fighting methods to ward off a variety of attacks. According to a report by Aite Group, credit card losses in North America have remained relatively flat over the past few years. Debit card fraud losses, however, have been on the rise. These losses are the result of a number of factors, including increased debit card volume and increasingly common point-of-purchase events that lead to debit card compromise (Aite Group, 2011).

Whether it is automated teller machine (ATM) card skimming, counterfeit cards, malware or any number of other fraud tactics that create a threat, debit and credit cards are under assault. Aite Group estimates the total cost of fraud in the United States is \$8.6 billion per year (0.4 percent of the \$2.1 trillion card payment industry) (Aite Group, 2011). One method for combating card skimming and fraud at the ATM and during a point-of-sale (POS) transaction is the use of EMV chip-based cards (also known as smart cards). Chip and personal



INNOVATION DELIVERED®

identification number (PIN) technology used to support EMV standards has realized fairly widespread adoption worldwide, though not in the United States to date.

What is EMV?

EMV is a global standard for credit and debit cards based on embedded chip card technology developed by Europay, MasterCard and Visa (which is where the EMV term originated). The card's chip communicates with card-accepting devices, such as point-of-sale terminals and ATMs, through direct contact with the reader by way of a contact plate. The chip contains the information needed to use the card for payment and is protected by various security features. It can facilitate robust authentication, which can significantly reduce fraud rates at the point of sale or ATM. EMV standards also apply for contactless transactions, where a dual-interface card includes both a contact interface (chip) and a contactless interface (typically an embedded antenna).

In addition to storing payment information in a secure chip rather than on a magnetic stripe, using EMV-compliant technology improves the security of a payment transaction by adding functionality in three areas:

- Card authentication, protecting against counterfeit cards
- Cardholder verification, authenticating the cardholder and protecting against lost and stolen cards being used for fraudulent transactions
- Transaction authorization, using issuer-defined rules to authorize transactions (Smart Card Alliance, 2011)

Development of EMV Specifications was initiated in 1994. A number of FIs at the time recognized the benefits of chip-based payment methods. They also realized that international standards for such payment would help foster global interoperability. The EMV Specifications were created for that purpose. The first version of the EMV Specifications was published in 1996. The most recent version, EMV 4.2, was published

in June 2008. Today, EMVCo maintains and extends specifications, provides testing methodology and oversees the testing and approval process.

The Magnetic Stripe Alternative

The magnetic stripe that is used on cards in the United States dates back to 1960, when IBM invented a process to attach a magnetic stripe to a plastic card for security purposes. The magnetic stripe technology used today has been improved from a security standpoint, but is essentially the same technology that was developed in 1960. The magnetic stripe stores magnetically encoded data about the credit or debit card and account holder information on the stripe.

Cards with a magnetic stripe are relatively inexpensive to produce, but they can be susceptible to fraud through skimming—where criminals place a hard-to-detect, small overlay device on top of the card slot of ATMs or POS equipment that scans cards and stores the information from the magnetic stripe. Criminals will also often place a small camera near the keypad to steal personal identification numbers. Information stolen from the card can then be written to another magnetic stripe card to make a fraudulent purchase. The cardholder is most often unaware that their data has been stolen at the time of theft, making it difficult to pinpoint the timing and location of such attacks.

Global EMV Adoption

Many countries in Europe, Latin America and Asia, as well as Canada and Mexico, are in various stages of EMV chip migration. The impact on fraud reduction efforts has been significant.

In Europe, domestic issuer ATM losses (losses committed inside national borders by criminals using stolen card details) have fallen by 63 percent from a high of €62 million during the first six months of 2006, to a low of €23 million during the second six months of 2010 (European ATM Security Team (EAST), 2011).

According to EMVCo, more than 1.24 billion EMV-compliant, chip-based payment cards were in use worldwide at the end of 2010.

Loss to Canadian banks from ATM fraud increased from CAN \$94.6 million in 2006 to CAN \$142 million in 2009 but dropped by 16 percent to CAN \$119 million last year. The introduction of chip cards is credited with playing a role in the decline (Canada's National Post 2011).

In the U.K., the UK Cards Association reports a dramatic reduction in fraud since the introduction of EMV cards. "Fraud on lost and stolen cards is now at its lowest level for two decades and counterfeit card fraud losses have also fallen and are at their lowest level since 1999. Losses at UK retailers have fallen by 67 percent since 2004, lost and stolen card fraud fell by 58 percent between 2004 and 2009, and mail non-receipt fraud has fallen by 91 percent since 2004," according to the UK Cards Association (2010).

Cross-Border Fraud

While these and other EMV countries have realized a reduction in domestic card-present fraud, their experiences have also shown a migration to other types of fraud, namely card-not-present fraud and cross-border counterfeit fraud, particularly ATM fraud. Criminals are known to exploit the weakest link, moving from locations where stronger authentication is present to those where it is not, or from FIs and merchants who have more sophisticated fraud detection and prevention tools to those with less. With more than 1 billion EMV cards issued in the rest of the world and projections for continued growth in EMV card issuance outside of the United States, criminals are more likely to move magnetic stripe card counterfeiting activities to the United States, leading to an increase in cross-border counterfeit fraud in the United States (Smart Card Alliance, 2011). Because many EMV card issuers still authorize magnetic stripe transactions (meaning the card has both an EMV chip and a magnetic stripe), card skimming can still take place in EMV-compliant countries since any card with a magnetic stripe is vulnerable to attack.

Visa and MasterCard Weigh In

Visa recently made a move to push the United States closer toward adopting EMV contact- and contactless-chip technology and away from magnetic stripe technology. In its announcement, Visa stated, "The adoption of dual-interface chip technology will help prepare the United States payment infrastructure for the arrival of near-field communication (NFC)-based mobile payments by building the necessary infrastructure to accept and process chip transactions that support either a signature or PIN at the

point of sale. Not only will chip technology accelerate mobile innovations, it is also expected to secure payments into the future through the use of dynamic authentication. Chip technology greatly reduces a criminal's ability to use stolen payment card data by introducing dynamic values for each transaction. Even if payment card data is compromised, a counterfeit card would be unusable at the point of sale without the presence of the card's unique elements. By reducing static authentication, we diminish the value of stolen cardholder data, benefiting all stakeholders" (Visa Inc., 2011).

In its announcement, Visa outlined three initiatives to encourage United States adoption:

1. Effective Oct. 1, 2012, Visa will expand its Technology Innovation Program to the United States., eliminating the requirement for merchants to annually validate their compliance with the PCI Data Security Standard if at least 75 percent of their Visa transactions originate from chip-enabled terminals.
2. United States processors must be able to support merchant acceptance of chip transactions no later than April 1, 2013.
3. From October 1, 2015, liability will shift for domestic and cross-border counterfeit card-present POS transactions. If a contact chip card is presented to a merchant that has not adopted equivalent terminals, liability for counterfeit fraud may shift to the retailer's acquirer. Fuel-selling merchants will have an additional two years for transactions generated from automated fuel dispensers.

In September 2011, MasterCard announced that all Maestro ATM transactions occurring in the United States will need to be compliant with EMV standards by April 2013. MasterCard's focus on the ATM is intended to reduce fraudulent redemption in a channel that is not directly addressed by Visa's plan, which focuses on the point of sale. In MasterCard's program, the liability would shift to the ATM acquirer under similar circumstances. Currently, the card's issuer bears the liability for ATM and point-of-sale transactions.

Ensuring United States Adoption

The announcements made by Visa and MasterCard are helping to build the growing momentum for widespread EMV adoption in the United States. An Aite Group survey of risk management executives in 2009 and again in 2011 demonstrates a shift in the EMV outlook in the United States. In Aite's 2009 survey, 36 percent of respondents said adoption would never occur. Two years later, only 17 percent of respondents said it would never occur. While the consensus was that the transition would happen, more than half of respondents said it will be five years or more before the United States payments industry begins its migration to EMV (Aite Group, 2011).

Widespread United States adoption won't be easy and it will require an investment from FIs, card issuers and merchants. In other countries, it has taken regulation to ensure adoption. Additional hurdles for the United States include the need to:

- Reissue debit and credit cards with embedded chip technology
- Replace POS devices so they are able to read EMV cards, with merchants bearing the cost to upgrade
- Ensure ATMs are able to read and process EMV cards with FIs bearing the cost of the upgrade or replacement

Early Adopters

Several FIs have chosen to begin adopting EMV chip cards and several major retailers have also been deploying EMV-compliant POS terminals, including Wal-Mart, Home Depot and Best Buy. The FIs who have begun transitioning to EMV chip cards have done so primarily to support customers traveling to EMV-compliant countries. Many international travelers have encountered problems using their magnetic stripe cards outside of the United States. In fact, an Aite Group study in late 2009 of 1,000 United States citizens who traveled abroad found that more than half experienced difficulty using their card. Card issuers are under increasing pressure to satisfy their customers who travel internationally. While not all United States citizens travel abroad, international travelers spend on average six times more on their cards than non-travelers (Banking Automation Bulletin, 2011).

One publicized example of an FI that has begun the transition to EMV technology is the United Nations Federal Credit Union (UNFCU), which migrated Visa-branded credit cards to the EMV chip standard in October 2010 for elite cardholders. Purchase volume within the elite portfolio increased by 20 percent since the launch of EMV-compliant

cards, and UNFCU plans to expand the EMV offering to more members in 2012. Wells Fargo & Company was the first national bank to offer a Visa Smart Card with a traditional magnetic stripe plus EMV chip technology to help increase acceptance worldwide. The initiative included 15,000 Wells Fargo consumer credit card customers who travel internationally.

The Security Benefits of EMV

EMV changes the way debit and credit card transactions are authenticated, plus the embedded chip in each card can store data more securely than a magnetic stripe. To authenticate a transaction, the person attempting to use the card is authorized before the transaction occurs.

Chip cards are more difficult to copy because the chip has unique security keys within it. Criminals have yet to find a way to clone a chip. The EMV chip facilitates the use of PIN verification for two-factor authentication based on the secure card (something the card owner owns that has not been copied) and a secret PIN (something the card owner knows).

According to the Smart Card Alliance, the benefits of migrating to EMV include:

- Improving the security of the United States payments infrastructure and eliminating the United States as a destination for criminals and global magnetic-stripe fraud activity
- Increasing the satisfaction of cardholders, especially when traveling internationally. In 2008, United States payment card issuers missed out on nearly \$4 billion in charge volume, including \$78.7 million in interchange fees, because of problems cardholders had with their cards while traveling abroad
- Increasing the satisfaction of international customers, who will be using EMV cards at United States merchants and ATMs
- Maintaining interoperability with the rest of the world as it migrates to EMV
- Leveraging commercially available EMV-compatible products and services for a low-risk, proven approach to fraud reduction
- Positioning the industry for other forms of payment, notably NFC-based, mobile, contactless payments

For FIs, there can be a number of benefits to implementing an EMV card program, such as increased security and fraud prevention, a boost in cardholder loyalty, the ability to retain and attract higher-spending cardholders, and a way to grow card portfolios.

While several FIs have introduced EMV chip cards, they are taking a hybrid approach with both a traditional magnetic stripe and an EMV chip because EMV is not yet the accepted standard across the United States. As long as there are magnetic stripes on cards, information is at risk from skimming.

EMV and the ATM Chain of Trust

Consumers place their trust in FIs that their information will be protected from the time they take their card out to the time they put it back in their wallet or purse. With an ATM transaction, there are seven areas along the “chain of trust” that can be attacked by fraudsters, leading to a broken chain of trust with consumers. In all cases, there is a latent risk of loss. Consumers don’t lose confidence and FIs don’t lose money until the stolen card information is redeemed.

EMV-based chip cards excel as a defense against skimming (card with a chip only, not a hybrid chip/magnetic stripe card) in ATM transactions. They offer fraud protection for the first three links in the chain.

1. Access control reader—these types of skimming attacks were diminishing, but are on the rise again. An inside camera can be used to steal PINs.
2. External skimmer—a camera or keypad overlay is used to capture PINs.

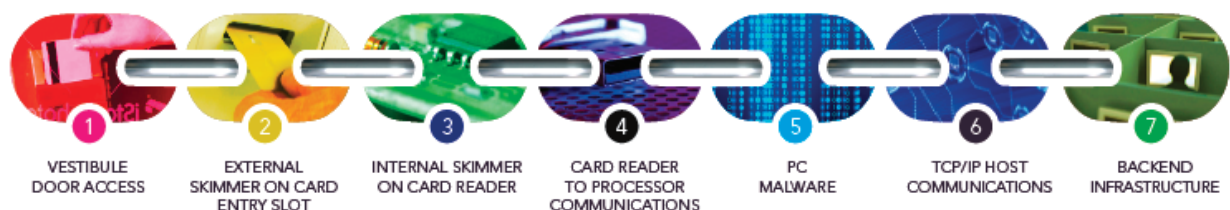
3. Internal skimmer—attacks have been increasing, especially at gas pumps where criminals open the pump and attach an internal skimmer. These attacks are impossible for consumers to detect and difficult for gas stations to detect.
4. USB “sniffing”—criminals intercept and store card information, coupled with a PIN camera.
5. Malware—placed on a PC and ATM; most criminals use a USB drive to steal data.
6. TCP/IP theft—not all FIs have encrypted data, leaving them vulnerable to brute-force attacks.
7. Back-end infrastructure infiltration—steft from where card information is stored.

A Foundation for the Future

Strategies for card security continue to evolve. Magnetic-fingerprint and single-use cards have fallen out of favor, while EMV-compliant cards have gained favor (Aite Group, 2011). NFC technology has also increased appeal for use in contactless credit cards and continues to grow as it is incorporated into mobile phones, enabling them to be used as a payment method. EMV serves as a foundation for mobile NFC payments.

As card-related fraud losses remain a problem that is expected to grow as criminals are more likely to move counterfeit magnetic stripe card activities to the United States, EMV-based chip cards can be an important component of a comprehensive security program to combat fraud. EMV-compliant technology is a global standard for the payment industry that improves the security of card authentication against counterfeiting, cardholder verification against lost/stolen cards and transaction authorization against interception and replay.

Chain of Trust



Notes

1. From Mag Stripe to Malware: Card Security Risks in 2011 (2011).
Aite Group
2. Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure? (2011, February).
Smart Card Alliance
3. European ATM Security Team (EAST) (2011, June) update
4. Time 'running out' for ATM fraudsters: police (2011, August).
National Post
5. New Card and Banking Fraud Figures (2010, March).
UK Cards Association
6. Visa Announces Plan to Accelerate Chip Migration and Adoption of Mobile Payments (2011, August). Visa Inc.

Call on Diebold for the latest in product, service and security solutions.
Since 1859, Diebold has put the customer first.

Contact Information:
Diebold, Incorporated
P.O. Box 3077
Dept. 9-B-16
North Canton, Ohio 44720-8077

800.999.3600 USA
330.490.4000 International
email: productinfo@diebold.com
www.diebold.com

© Diebold, Incorporated, 2011.
File No. 98-178

DIEBOLD
INNOVATION DELIVERED®