Earlier this year, reports by media alleged EMV payment cards are vulnerable to wedge or “man-in-the-middle” attacks. Wedge attacks, as described in the reports, occur when a fraudster inserts a wedge device between a lost or stolen card and point-of-sale (POS) terminal, thereby causing the terminal to erroneously determine that the card has been verified by the PIN. Additional allegations also claim that issuers may not be able to detect that a wedge attack has occurred during the online authorization process.

In response to these allegations, EMVCo — the global standard for credit and debit payment cards based on chip card technology — issued a statement to ensure that the marketplace understands the robust security measures EMV cards employ to prevent wedge-type attacks from succeeding. MasterCard supports EMVCo’s position on the matter. The complete statement can be read at www.emvco.com.

This wedge, or man-in-the-middle attack, is technically difficult and suitable countermeasures are already available when the full picture of the payment process is taken into account. The interoperability and security features provided by the EMV card-terminal specifications are building blocks for the payment systems and financial institutions that design their products and processes in accordance with wider risk management needs.

The opportunity to launch the wedge attack is limited and countermeasures do exist:
- The attack is focused exclusively on lost and stolen fraud. This fraud type has additional controls in place to mitigate it outside EMV and by its nature the fraud is limited to the single stolen card
- The attack is not relevant to ATM transactions and does not compromise the valid PIN
- Countermeasures are already available either explicitly in EMV, or within payment system products and networks, or within issuer host systems. Indeed, the issuer can already detect if the PIN has not been verified and can decline or refer the transaction in order to minimize risks associated with signature fallback.

The risks and challenges faced by fraudsters would be major. They must:
- Steal a card
- Install the card into wedge electronics so that it can be used unobtrusively
- Perform the attack before the card is reported stolen
- Risk detection by the merchant during the fraud attempt with the resulting legal consequences
- Hope that the issuer does not have intelligent fraud detection based on behavioral and geographic data

While such an attack might be theoretically possible, it would be extremely difficult and expensive to carry out successfully. Current compensating controls are likely to detect or limit the fraud. The possible financial gain from the attack is minimal while the risk of a declined transaction or exposure of the fraudster is significant.

One of the best places to obtain unnoticed access to card data plus PIN and ultimately access to clean money can be at the point of sale (POS). Whether acting independently, or in collusion with a merchant, criminals are developing an in-depth understanding of the function and vulnerabilities of many of the terminals deployed today — and they’re working around the clock to exploit that knowledge and commit fraud.

In 2008, more than 280 million account details were compromised. This resulted in the re-sale price of account data falling dramatically. However, when track 2 data including the PIN was compromised, the price remained high.

Terminal Fraud – Defeating the Security of Terminals

The one thing you can be certain of is that criminals are focused on exploiting the weakest link in any layer of the transaction environment. They almost invariably seek out the least challenging route to easy money. Unfortunately, they are also very clever, or they have access to people who are very clever.

Indeed, history proves that the criminal will target the terminal that is easiest to get into. For example, in the United States, fuel pumps are among the easiest and most attractive targets because of their location — they sit in the open often unattended and typically have very high transaction volume. Generally, there is only one key which will unlock every pump and grant access to the payment terminal hardware, and the physical security surrounding the pay at the pump is poor at best.

One of the best places to obtain unnoticed access to card data plus PIN and ultimately access to clean money can be at the point of sale (POS). Whether acting independently, or in collusion with a merchant, criminals are developing an in-depth understanding of the function and vulnerabilities of many of the terminals deployed today — and they’re working around the clock to exploit that knowledge and commit fraud.

In 2008, more than 280 million account details were compromised. This resulted in the re-sale price of account data falling dramatically. However, when track 2 data including the PIN was compromised, the price remained high.

Terminal Fraud – Defeating the Security of Terminals

The one thing you can be certain of is that criminals are focused on exploiting the weakest link in any layer of the transaction environment. They almost invariably seek out the least challenging route to easy money. Unfortunately, they are also very clever, or they have access to people who are very clever.

Indeed, history proves that the criminal will target the terminal that is easiest to get into. For example, in the United States, fuel pumps are among the easiest and most attractive targets because of their location — they sit in the open often unattended and typically have very high transaction volume. Generally, there is only one key which will unlock every pump and grant access to the payment terminal hardware, and the physical security surrounding the pay at the pump is poor at best.

Once a criminal has access, investigators familiar with this type of attack report that it only takes crooks about 30 seconds to remove the entire card device from a gas pump and replace it with an identical one fitted with electronic skimmers.
Given the potential for obtaining large amounts of cash through an effective terminal manipulation scheme, organized crime is attracting some very clever minds with the lure of easy money. Individuals capable of understanding the operation and hardening of a payment terminal can identify vulnerabilities and develop effective, low-cost attack methods for use in the field by a criminal network. Once the best means of exploitation is developed, the criminal in many instances has the network and resources to very quickly and efficiently deploy this attack on a very large scale across regions and around the world.

In recent times, there has been an increasing trend for criminals to target the dominant terminal in a particular marketplace. Recent mergers in the terminal manufacturing industry, where there are now significantly fewer companies offering only a limited number of terminals, have made attacks of this nature even more dangerous. If the criminals can learn to defeat the security of a particular terminal, then they will be able to use this information to attack many terminals, regardless of where it is located around the world.

Types of Attacks

MasterCard’s experience investigating compromised terminals has shown that the most common method of attack is to obtain a single terminal and use this terminal to learn about all of its security features. The terminal can either be stolen or obtained through legal means such as online auction sites. On any given day, there are over 5,000 terminals available for auction online.

Once the criminal has learned how to defeat the security mechanisms of a particular terminal, they will move on to target terminals installed at a merchant location. Stealing a live terminal, compromising that terminal, and then returning it to the merchant location, or even another location (experience has shown that in some regions, poor controls mean that terminals will often work in different locations, and even different merchants) is a very effective means of obtaining card data. Of course, adherence to accepted terminal management best practices should prevent a device from functioning anywhere but at the location from which it was removed.

The type of skimmer used has also been evolving over the years, with the current skimming devices using wireless networking technology, such as Bluetooth or GSM, to transmit the data from the terminal to the criminal. Some criminals are even encrypting stolen data and sending it outside the merchant network to servers located in countries where it is difficult, if not impossible, to trace.

MasterCard’s Role

The MasterCard Analysis Laboratory was established more than 10 years ago to investigate card security. In recent years, it has also focused on identifying and understanding attacks against terminals. Working with police forces throughout the world and using a wide range of state-of-the-art equipment along with extensive engineering expertise, MasterCard’s laboratory has successfully analyzed many compromised terminals.

A critical starting point for any evaluation is the real-time x-ray which allows images of the inside of the terminal to be taken without even needing to remove the terminal from the evidence bag, thus ensuring the integrity of any DNA evidence. This allows MasterCard to see if the terminal contains a skimming device or not.

From there, MasterCard will work to determine if the skimmer contains any actual card data, essential for any prosecution, and what methods were used to transmit the data. It will also investigate to the greatest extent possible where the data was transmitted to allow investigators to target additional entities involved in the illegal distribution and receipt of stolen payment card data.

Much of this information is provided to specialist police crime units for ongoing investigations.

GSMSkimmer

Added circuit board identified via x-ray analysis
The type of skimmer used has also been evolving over the years, with the current skimming devices using various techniques to target terminals installed at a merchant location. Stealing a live terminal, compromising that terminal, and then returning it to the merchant location, or even another location (experience has shown that in some regions, poor controls mean that terminals will often work in different locations, and even different merchants) is a very efficient means of obtaining card data. Of course, adherence to accepted terminal management best practices should prevent a device from functioning anywhere but at the location from which it was removed.

Once the criminal has learned how to defeat the security mechanisms of a particular terminal, they will move on to target terminals installed at a merchant location. Stealing a live terminal, compromising that terminal, and then returning it to the merchant location, or even another location (experience has shown that in some regions, poor controls mean that terminals will often work in different locations, and even different merchants) is a very effective means of obtaining card data. Of course, adherence to accepted terminal management best practices should prevent a device from functioning anywhere but at the location from which it was removed.

The type of skimmer used has also been evolving over the years, with the current skimming devices using wireless networking technology, such as Bluetooth or GSM, to transmit the data from the terminal to the criminal. Some criminals are even encrypting stolen data and sending it outside the merchant network to servers located in countries where it is difficult, if not impossible, to trace.

### Types of Attacks

MasterCard's experience investigating compromised terminals has shown that the most common method of attack is to obtain a single terminal and use this terminal to learn about all of its security features. The terminal can either be stolen or obtained through legal means such as online auction sites. On any given day, there are over 5,000 terminals available for auction online.

Once the criminal has learned how to defeat the security mechanisms of a particular terminal, they will move on to target terminals installed at a merchant location. Stealing a live terminal, compromising that terminal, and then returning it to the merchant location, or even another location (experience has shown that in some regions, poor controls mean that terminals will often work in different locations, and even different merchants) is a very effective means of obtaining card data. Of course, adherence to accepted terminal management best practices should prevent a device from functioning anywhere but at the location from which it was removed.

The type of skimmer used has also been evolving over the years, with the current skimming devices using wireless networking technology, such as Bluetooth or GSM, to transmit the data from the terminal to the criminal. Some criminals are even encrypting stolen data and sending it outside the merchant network to servers located in countries where it is difficult, if not impossible, to trace.

### MasterCard's Role

The MasterCard Analysis Laboratories was established more than 10 years ago to investigate card security. In recent years, it has also focused on identifying and understanding attacks against terminals. Working with police forces throughout the world and using a wide range of state-of-the-art equipment along with extensive engineering expertise, MasterCard's laboratory has successfully analyzed many compromised terminals.

A critical starting point for any evaluation is the real-time x-ray which allows images of the inside of the terminal to be taken without even needing to remove the terminal from the evidence bag, thus ensuring the integrity of any DNA evidence. This allows MasterCard to see if the terminal contains a skimming device or not.

From there, MasterCard will work to determine if the skimmer contains any actual card data, essential for any prosecution, and what methods were used to transmit the data. It will also investigate to the greatest extent possible where the data was transmitted to allow investigators to target additional entities involved in the illegal distribution and receipt of stolen payment card data. Much of this information is provided to specialist police crime units for ongoing investigations.

MasterCard Analysis Laboratory regularly conducts forensic analysis of manipulated terminals

Added circuit board identified via x-ray analysis

GSM Skimmer

### Case Study

**Mitigating POS PIN Pad tampering and skimming attacks at Quick Service Restaurants (QSRs)**

**Author**

Moneris Solutions | www.moneris.com

**Background**

The QSR sector has become a prime target for POS terminal tampering and skimming based on the following factors:

- National QSR chains have virtually identical payment configurations in each location.
- Franchises in metropolitan areas typically have high payment card volumes.
- Most establishments have multiple service lanes and POS devices are left unattended during non-peak periods.
- Extended hours of operation usually coincide with reduced staffing levels.
- New employees are not aware of the indicators associated with tampering or skimming activities.

**Solution**

After conducting a comprehensive review of skimming and tampering techniques that fraudsters used against a Moneris QSR client, Moneris recommended a layered device security approach that encompassed both physical security solutions and process-related best practices. Per Moneris' recommended mitigation strategies, its QSR client implemented the following actions:

- Strategic replacement of stands with tethers and the storage of POS devices when they are not being used.
- A security seal applied to POS devices to indicate possible tampering.
- Management training on how to perform POS device integrity checks and serial number verifications.
- An incentive-based education program for front-line employees that teaches them how to identify both common POS device skimming activities and if a POS terminal has been tampered with or is a decoy.

**Outcome**

Following the implementation POS fraud mitigation strategies, the QSR customer determined:

- Device theft dropped 42 percent in one year.
- Tampering losses decreased 26 percent in one year, with an estimated savings of more than $2 million.
- Employees identified multiple decoy devices following the launch of the incentive program.
POS Tampering is Everyone’s Problem

MasterCard, as a member of the Payment Card Industry Security Standards Council (PCI SSC), is working hard at tackling this problem. From a terminal security perspective, this is through the PIN Transaction Security Requirements (PCI PTS).

This standard, which impacts new POS terminals, was updated in 2009 such that it is not only difficult to defeat the security of the PIN entry Point of Interaction (POI) device the first time, but each and every time. The standard also provides the opportunity for fuel pump and other unattended terminal manufacturers to submit their devices for evaluation.

Terminal manufacturers must continually improve the security of their terminals, but merchants also must realize that they have an important role to play.

To help, the PCI SSC has also released Skimming Prevention-Best Practices for Merchants, a guide on how to prevent skimming attacks against their terminals in merchant locations.

Issuing banks can help by continuing to implement a comprehensive set of fraud fighting tools that enable the early detection of fraud with effective transaction monitoring techniques. For those regions that have migrated or are migrating to chip and PIN authentication, issuers should ensure that they utilize the latest secure chips being offered by the industry and by adopting the use of Combined Dynamic Data Authentication which not only ensures that the PIN is never handled in clear text, but also prevents man-in-the-middle wedge attacks.

Acquirers can help by ensuring that their merchants use terminals certified to meet the requirements of the latest version of the PCI PTS program. In addition, they should develop programs to provide support and training on how to protect terminals at the merchant location, and how to identify signs of tampering or the addition of skimmers.

This is a never-ending race, yet by working together and adopting the above best practices we can ensure that terminal manipulation becomes a much less inviting target for organized criminals.

Stakeholder Feedback Helps Advance Compliance

Both the Payment Card Industry Data Security Standard (PCI DSS) and the MasterCard Site Data Protection (SDP) Program rely on active participation by customers, merchants, and service providers to successfully protect all stakeholders against the compromise of payment account data.

The MasterCard SDP Program seeks to achieve this goal by identifying and correcting vulnerabilities in organizations’ security processes and procedures. Another key focus of the SDP Program is helping to ensure that merchants and service providers securely store account data in accordance with PCI DSS requirements.

Feedback from our customers is critical to the success of any MasterCard compliance program. By understanding customer needs and concerns, MasterCard is better informed to make prudent adjustments to its rules and procedures. Such updates help establish obtainable goals for achieving compliance, thereby encouraging increased participation and maintaining a secure payments environment.

For example, MasterCard introduced SDP Program changes last year to help enhance existing safeguards and ensure the integrity of payment account data. These changes were designed to help increase quality and consistency in the assessment and implementation of PCI DSS requirements.

- In June 2009, MasterCard announced revisions to its SDP Program requiring Level 1 and Level 2 merchants to validate their PCI DSS compliance by completing an annual onsite assessment by a Payment Card Industry Security Standards Council (PCI SSC) certified Qualified Security Assessor (QSA) by 31 December 2010. Based on feedback that we received from our customers and the merchant community regarding this announcement, we postponed this requirement by six months.
- MasterCard also exercised flexibility in its SDP Program rules in December 2009 by announcing that Level 1 merchants can use an internal auditor to conduct the annual onsite assessment and Level 2 merchants can use their internal staff to complete a self-assessment questionnaire, under the condition that such auditor or staff pass a PCI SSC offered merchant training and accreditation program each year. Level 1 and Level 2 merchants still have the option of using a PCI SSC-certified QSA to complete an annual onsite assessment. For additional details regarding the SDP Program revisions announced by MasterCard in December 2009, please refer to the “New and Noteworthy Global Security Bulletins” section of this brochure.
- In the latter half of 2009, MasterCard revised its PCI merchant level descriptions to promote its alignment with Visa’s PCI DSS compliance program and alleviate any potential confusion caused by the term, “competing payment brand,” since the business models and associated compliance programs of American Express, Discover Financial Services, and JCB International differ from those of MasterCard Worldwide.