Forensics Update:

Trustwave's investigations of credit card compromises through October 2008

Trustwave®
Information Security & Compliance

Introduction

Following is an analysis of Trustwave's investigations of credit card compromises through October 29, 2008. We've derived the information and statistics in this paper from 443 cases of cardholder data compromise investigated by Trustwave since 2001.

The information contained within this report is the culmination of almost seven years of card compromise investigations.

Trustwave®
Information Security & Compliance

70 W. Madison Street, Suite 1050, Chicago, IL 60602 www.trustwave.com 1.888.878.7817

Key Developments in 2008:
The Theft of Cardholder Data in Transit

In 2008, the most notable development in payment card compromises is the shift from the theft of cardholder data at rest to its theft in transit.

In Trustwave's seven years of card compromise investigations, businesses have made progress in protecting cardholder data. Unfortunately, criminals have matched that progress and moved beyond, adapting their techniques to access more carefully protected data. In 2008, the most notable development in payment card compromises is the shift from the theft of cardholder data at rest to its theft in transit. In other words, Trustwave experts have noted that attackers, sometimes called hackers—thieves who seek unauthorized access to proprietary data—seem to be stealing data in real-time. Attackers do this by eavesdropping on a certain device and stealing the data as it passes to or through that particular system rather than stealing data that is simply stored on that system.

In the past, the majority of compromises were the result of an unauthorized party penetrating network defenses and breaking into a database that stored cardholder data. In most cases, that party collected the data and either took advantage of it themselves, or sold it to other criminals via black markets on the Internet. The card brands (American Express, Discover Financial Services, JCB, MasterCard Worldwide, Visa Inc. and Visa Europe) prohibited the storage of some of this data to stifle this type of theft and ran marketing campaigns to increase awareness of the prohibition.

As Trustwave's statistics show, the card brands' efforts appear to be working. Fewer and fewer compromised organizations investigated by Trustwave store prohibited data. More often than not, upon meeting a Trustwave investigator, a representative from the compromised entity will say something akin to, "We don't store track data." Working toward the elimination of the storage of prohibited data is progress and deserves recognition. However, because of new attack vectors observed by Trustwave, more work is needed to protect against cardholder data theft.

Organizations continue to fall victim to compromise. Due to weaknesses in these organizations' security controls, and, as Trustwave believes, their failure to comply with the whole of the Payment Card Industry Data Security Standard (PCI DSS), attackers still gain entry to computer networks.

The parties responsible for cardholder data theft have adapted and found ways to steal sensitive data even if it is not stored to disk. One example of this is Trustwave's observation of attackers' use of unauthorized applications (referred to as malware) that steal cardholder data from a computer's Random Access Memory (RAM).

With this technique, an attacker installs malware on a computer that hosts a payment application. A host computer uses its RAM to perform operations and interact with a payment application (for example). The malware is capable of gathering information passed from the payment application to its host computer through RAM. The information passed by the application includes unencrypted/plain-text cardholder information. In this scenario, although cardholder data is never actually written to disk or stored, an attacker can still pilfer it.

The possibility of parsing track data from RAM has existed for years, but only recently has Trustwave discovered real-world examples of its use. What's perhaps most unsettling about the trend is that a merchant can use a payment application that complies with the Payment Application Data Security Standard (PA-DSS) or Visa's Payment Application Best Practices (PABP), but still fall victim to a compromise of this sort.

[1]This prohibited data includes full magnetic stripe data, card verification codes (such as CAV2, CVC2, CVV2 or CID depending on the card brand) and PIN/PIN block data.

Other examples of the theft of cardholder data in transit include compromises investigated by Trustwave that involve malware, but of a different sort than RAM-parsing software. In their investigations, Trustwave experts have encountered a number of cases involving packet analyzing software and key-logging software installed on the systems that interact with cardholder data. Both key-logging and sniffing or packet-analyzing programs are malware that eavesdrop on data as it enters or leaves a system. A sniffing program can intercept traffic entering or leaving a particular system and record that traffic. In many cases, that traffic will include unencrypted or plain-text cardholder data.

Key-logging software is used in a similar way to steal cardholder data. A key-logger records the information entered on a keyboard (or card reading device) as it travels from the magnetic stripe reader to the computer or payment application. Many Point-of-Sale (POS) systems consist of a typical computer and a magnetic stripe reader. The magnetic stripe reader may be built into a keyboard and connect to the computer by a PS/2 connector (a standard keyboard cable). Stand-alone magnetic stripe readers are also available that connect via USB cable. Either way, the data from the magnetic stripe of a payment card is transferred to the computer in the same way, as input from a keyboard. The majority of that information is not encrypted. These sorts of techniques allow a thief to steal cardholder data in transit even if it is not stored to disk at any point.

Merchants and service providers must recognize that payment card security extends beyond just using PABP or PA-DSS-validated payment applications and eliminating the storage of prohibited cardholder data.

Merchants and service providers must recognize that payment card security extends beyond just using PABP or PA-DSS-validated payment applications and eliminating the storage of prohibited cardholder data. Any entity involved in the processing, storage or transmission of payment card data must ensure that their network environment complies with the PCI DSS. In the cases of in-transit cardholder data theft that Trustwave has examined, the intruder gained the access necessary to execute the attack because the victim organization did not comply with the entire PCI DSS.

70 W. Madison Street, Suite 1050, Chicago, IL 60602 www.trustwave.com 1.888.878.7817

General Payment Card Compromise Statistics

It's difficult, if not impossible, to say that the occurrence of payment card compromise is increasing, decreasing or staying the same. Any organization that claims to be able to make these assertions is—at best—estimating the trend. This is due to a number of factors. First, the reporting of data security compromises is unreliable. Despite the various disclosure laws now in place at the state level, many compromises go unreported. Some compromises are discovered and investigated years after they occurred. Even when discovered, without proper security controls in place, it's difficult to determine the exact date and duration of a breach.

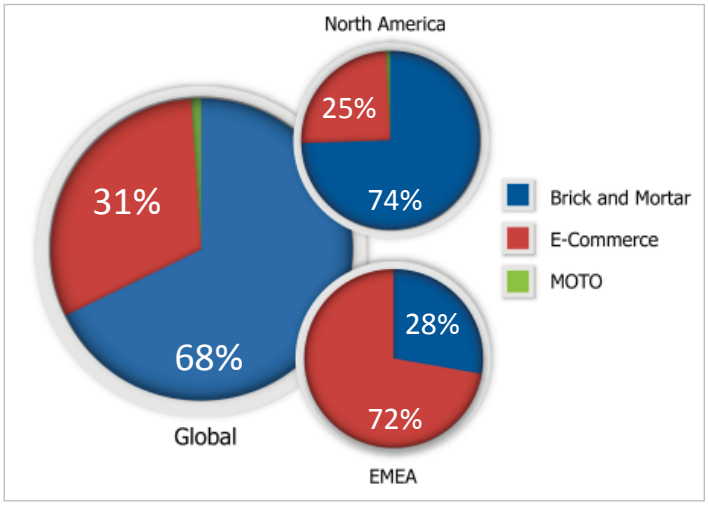
What can be said, however, is that payment card compromises continue to occur. Not a week goes by without another organization engaging Trustwave to conduct an investigation of a suspected payment card compromise. The information below is based solely on cases investigated by Trustwave. While this introduces bias into the information, these statistics provide insight into what types of organizations have fallen victim to payment card compromises and how.

Due to the nature of these payment card investigations, data is not always available for every case on every data point discussed below. For instance, a compromised merchant may have altered their system after the breach was discovered and before Trustwave was engaged for the investigation. Therefore, each set of statistics does not necessarily include information from all 443 Trustwave cases conducted in North America and EMEA (Europe, the Middle East and Africa). In addition, North American cases outnumber EMEA cases by a ratio of six to one.

Cases Segmented by Payment Card Acceptance Channel

In this statistic that compares compromised merchants by the manner in which they accept payment cards... we see the greatest variation between cases in North America and those in EMEA.

In this statistic that compares compromised merchants by the manner in which they accept payment cards—whether over the Internet (e-commerce), in person (brick-and-mortar) or over the telephone or through the mail (MOTO)—we see the greatest variation between case in North America and those in EMEA. In North America, the majority of compromises investigated by Trustwave were of brick-and-mortar merchants. In EMEA, the majority of compromises investigated were of e-commerce merchants. This fact is the reason many of the statistics from North America and EMEA differ as they do. We begin our analysis with this data because it affects all other data presented throughout this paper.



Cases Segmented by Payment Card Acceptance Channel

Trustwave experts believe that more e-commerce merchants than brick-and-mortar merchants are compromised in EMEA for several reasons. One key factor is that a majority of payment systems in EMEA connect for authorization via leased lines that connect two locations via a private circuit, rather than over the Internet. The opposite is true in North America. In Trustwave's investigations in North America, the majority of compromised systems connect for authorization over the Internet. Any connection to the Internet should be considered a connection to an un-trusted, public network and secured accordingly. In many cases, hackers use automated scanners to troll the Internet for vulnerable systems. If a merchant is not connected to the Internet, their system—vulnerable or not—cannot be discovered via the Internet. Trustwave experts believe that because fewer brick-and-mortar than e-commerce merchants connect to the Internet in EMEA, the majority of compromises investigated by Trustwave are of e-commerce merchants.

Another contributing factor to the difference between Trustwave statistics from EMEA and North America is payment application technology. An overwhelming majority of compromises in North America are due to the exploitation of older, insecure payment applications. The Chip and PIN[2] initiative in the U.K., launched in 2004, required many brick-and-mortar merchants in the U.K. to overhaul their payment application systems. This resulted in merchants using updated payment applications that not only included increased functionality (allowing Chip and PIN transactions), but also increased security. While a large problem in the U.S. is the use of out-dated payment applications that store data that the payment card industry prohibits, this refresh of technology in the U.K. resulted in the use of newer payment applications and devices that did not store such data.

Put simply, in EMEA it's much more viable for criminals to steal cardholder data from an e-commerce merchant because it's much easier to use that information for fraud. In compromising a brick-and-mortar merchant, an attacker would need to collect both the card data and the PIN associated with the embedded chip. And even with that information, creating a counterfeit or clone card with valid, working Chip and PIN technology is difficult, if not impossible. However, the information that can be stolen from an e-commerce merchant allows a criminal to use that information to make purchases on other Web sites.

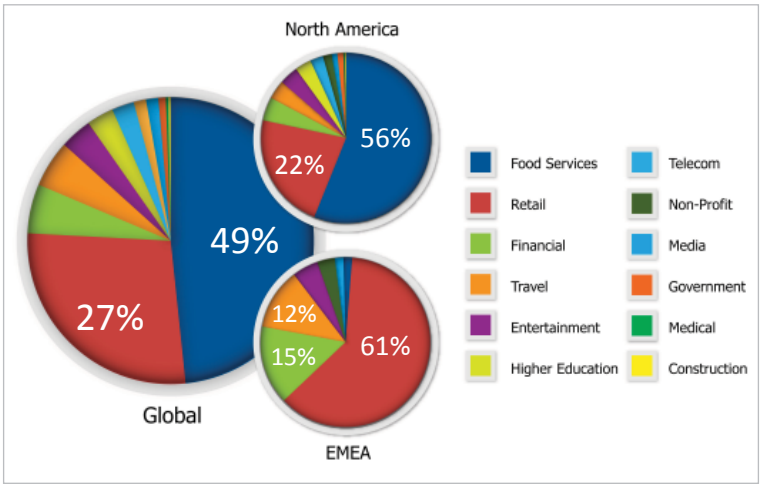
The effects of Chip and PIN technology on the statistics below cannot be overstated. Trustwave experts believe that the adoption of Chip and PIN across EMEA contributes significantly to the differences in other Trustwave statistics from EMEA and North America which will be seen throughout the rest of this report.

In contrast to the EMEA region, the majority of compromised merchants investigated by Trustwave in North America conduct card-present transactions at a physical location. While Trustwave is seeing an increase in the theft of cardholder data in transit and expects the trend to continue (as mentioned at the beginning of the paper), the majority of Trustwave's past investigations were of compromises involving insecure, legacy Point-Of-Sale (POS) payment applications that stored prohibited cardholder data.

Cases Segmented by Industry

Businesses involved in the food service and retail segments make up the majority of compromises investigated by Trustwave, with approximately half of the compromises occurring at food service locations.

For the most part, we don't see changes in the trending of this statistic. Businesses involved in the food service and retail segments make up the majority of compromises investigated by Trustwave, with approximately half of the compromises occurring at food service locations. Globally, approximately 76 percent of payment card compromises investigated by Trustwave took place at either a food service establishment or retail location.



Cases Segmented by Industry

Trustwave experts believe that the majority of compromises occur at food service establishments in North America due to the industry's reliance on third-party software POSs that are, many times, supported remotely. Remote control software allows for remote access to a networked computer and the payment application it hosts. For many years, hackers have been exploiting remote control software that is not securely configured. In fact, the exploitation of remote access is the number one technical cause of a breach in the compromises investigated by Trustwave in North America.

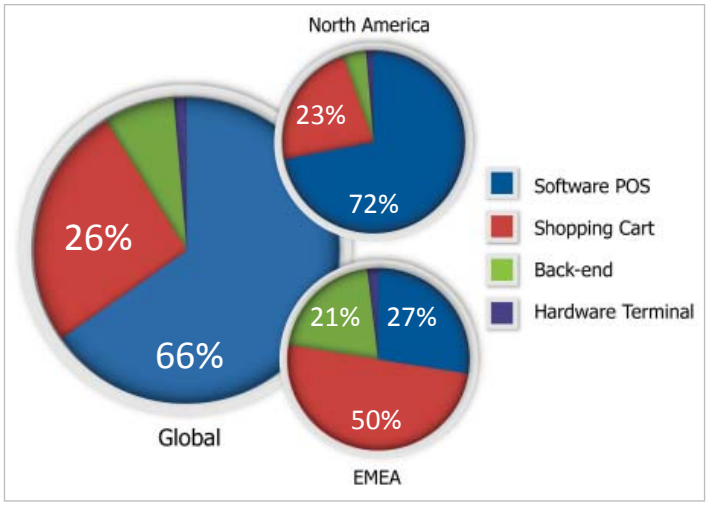
[2]A program launched in the U.K. to implement the EMV (Europay, MasterCard and Visa) standard for payment cards and payment card transactions. Other countries in EMEA use similar programs. Instead of a magnetic stripe, a Chip and PIN card uses a microchip embedded within the card to store cardholder information (the cards also include a magnetic stripe, but most brick-and-mortar merchants in countries with EMV programs only accept Chip transactions). The Chip requires that a PIN be entered to authenticate the user before the data on the card's chip can be used.

In the EMEA region, the majority of Trustwave investigations were of payment card compromises of merchants within the retail sector (61 percent) followed by organizations in the financial services sector. Companies in the food service industry make up a mere 3 percent of breaches investigated by Trustwave in EMEA. Trustwave experts believe the inconsistency regarding food service compromises between North America and EMEA is because the majority of merchant compromises in EMEA are of e-commerce merchants. Food service rarely if ever qualifies as e-commerce while most e-commerce merchants are considered retail.

Cases Segmented by System Type

Because Trustwave investigates more e-commerce than brick-and-mortar compromises in EMEA, this statistic varies widely between the two regions. The terms used in the chart legend are defined as follows:

- Software POS: a payment application that runs on a PC-based system in a retail environment
- Shopping Cart: an e-commerce tool used to facilitate payment card purchases over the Internet
- Back-end: a centralized processing system, often called a "transaction switch," used by merchants to aggregate transactions from multiple software POS systems
- Hardware Terminal: a dedicated device used by merchants in lieu of a software POS system.



Cases Segmented by Type

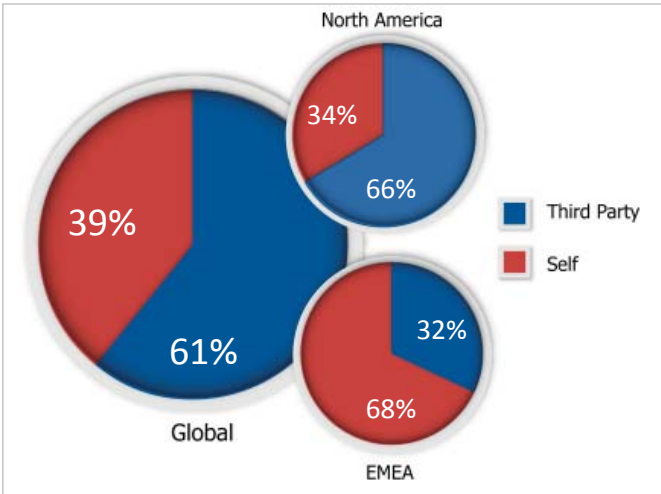
As explained in the Industry statistic, Trustwave experts believe the majority of compromises in North America involve software POS systems because many times these systems are supported remotely by their vendors. Insecure remote access practices are the number one technical cause of breaches in North America.

Insecure remote access practices are the number one technical cause of breaches in North America.

In this statistic, the difference between cases in North America and those in EMEA are due to the more frequent breach of e-commerce merchants in EMEA. E-Commerce merchants use some sort of shopping cart application to accept payment from online customers. Attackers will then compromise the shopping cart software, most frequently, via SQL injection.

Cases by Responsibility for Payment System Administration

In North America, Trustwave finds that the most troublesome aspect of a merchant's payment system is the payment application. Many victims of Trustwave-investigated compromises use outdated systems or do not have them configured in a secure manner.
In addition, many North American merchants depend heavily on third party vendors or integrators to install, configure and support their payment applications.
These two findings together explain the statistic above. Misconfigured payment applications will store or insecurely transmit cardholder data that can be stolen by an attacker. Because Trustwave often finds that a third party configured those payment applications, negligence on the part of the third party more often contributes to the payment card compromises investigated by Trustwave in North America.



Cases by Responsibility for Payment System Administration

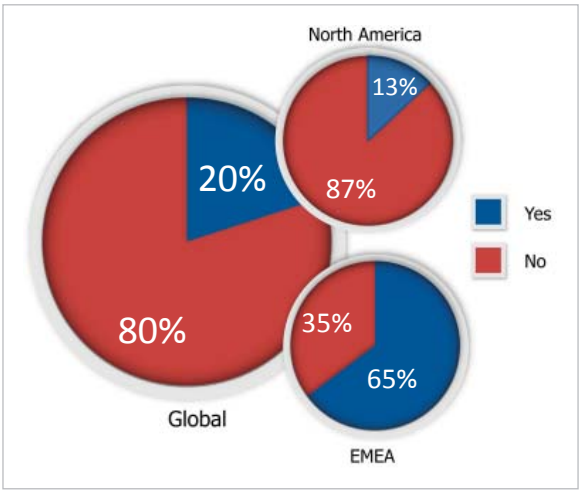
Because the use of outmoded payment applications is not as prevalent in EMEA as in North America, neither are the problems caused by third-party installation, configuration or maintenance of such payment applications. Additionally, the e-commerce merchants compromised in EMEA tend to be smaller businesses. Trustwave experts suspect that because of this, some of these merchants take a do-it-yourself approach in which security may not take the priority it should in system architecture and development. In EMEA, it's more likely that a weakness elsewhere in a merchant's system, and under the merchant's purview, led to a breach.

In EMEA, it's more likely that a weakness elsewhere in a merchant's system, and under the merchant's purview, led to a breach.

Cases by Storage of Card Security Code

A card security code is a three or four-digit code printed on the front or the back of a payment card (but not encoded on the magnetic stripe) to confirm that a cardholder has physical possession of the card they're using in card-not-present transactions (in e-commerce transactions for example). Depending on the card brand, this is called the Card Verification Value (CVV2), Card Validation Code (CVC2) or Card Identification number (CID).

Card-present or brick-and-mortar merchants have no reason to ask for or store the card security code. Therefore, because Trustwave sees more compromises of brick-and-mortar merchants, more of these merchants do not store card security codes. Because the global statistic is heavily weighted with North American cases, the chart shows far fewer merchants storing card security codes.



Cases by Storage of Card Security Code

Because Trustwave finds that fewer e-commerce merchants are compromised in North America, this statistic shows that fewer North American merchants store the card security code.

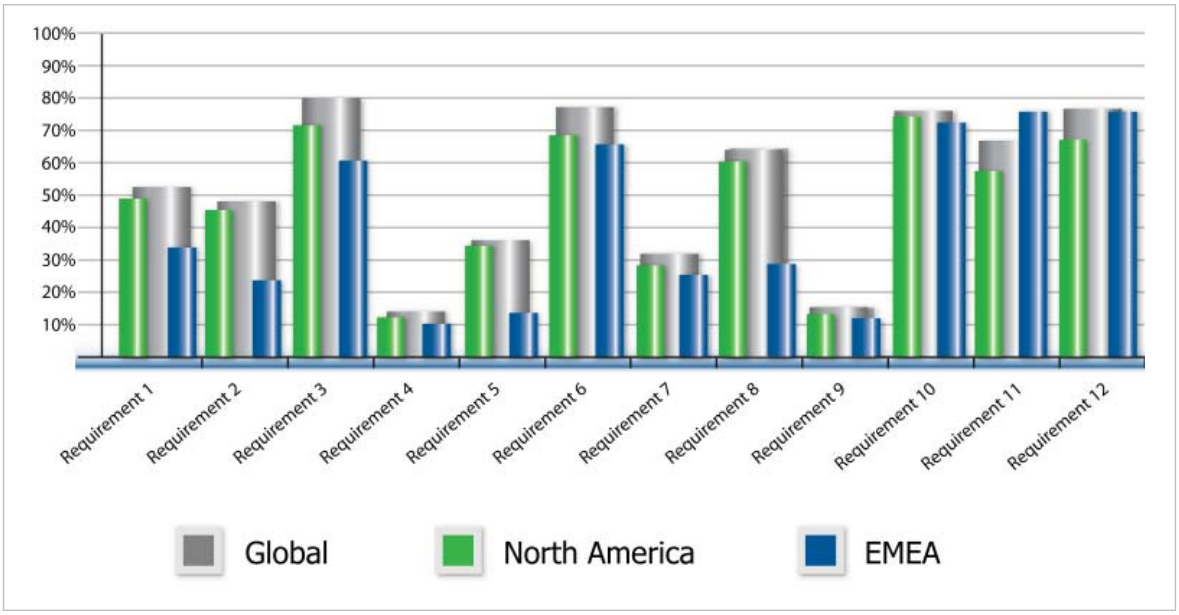
If an attacker cannot gather both card information and the card security code from a particular merchant, that merchant is a less enticing target.

While storing the card security code is prohibited by the PCI DSS, and in turn by the card brands, Trustwave finds that more than half of compromised merchants in EMEA store this information. Much of this has to do with the higher number of e-commerce merchants investigated by Trustwave in EMEA. Because a brick-and-mortar merchant has no need for the card security code, it's less likely that they will store this information. Because of misconfigured shopping cart applications, some e-commerce merchants will, often unknowingly, store this code. Had they not stored the code, it would be more difficult for a criminal to make fraudulent e-commerce purchases with the stolen data. Most merchants require the card security code for e-commerce purchases. If an attacker cannot gather both card information and the card security code from a particular merchant, that merchant is a less enticing target.

Common PCI DSS Failures of Compromised Merchants

For the most part, while the frequency of failure may be less, the PCI DSS requirements that compromised merchants fail to meet correspond in EMEA and North America.

The PCI DSS requirements that Trustwave investigators find merchants fail to fulfill are the following:



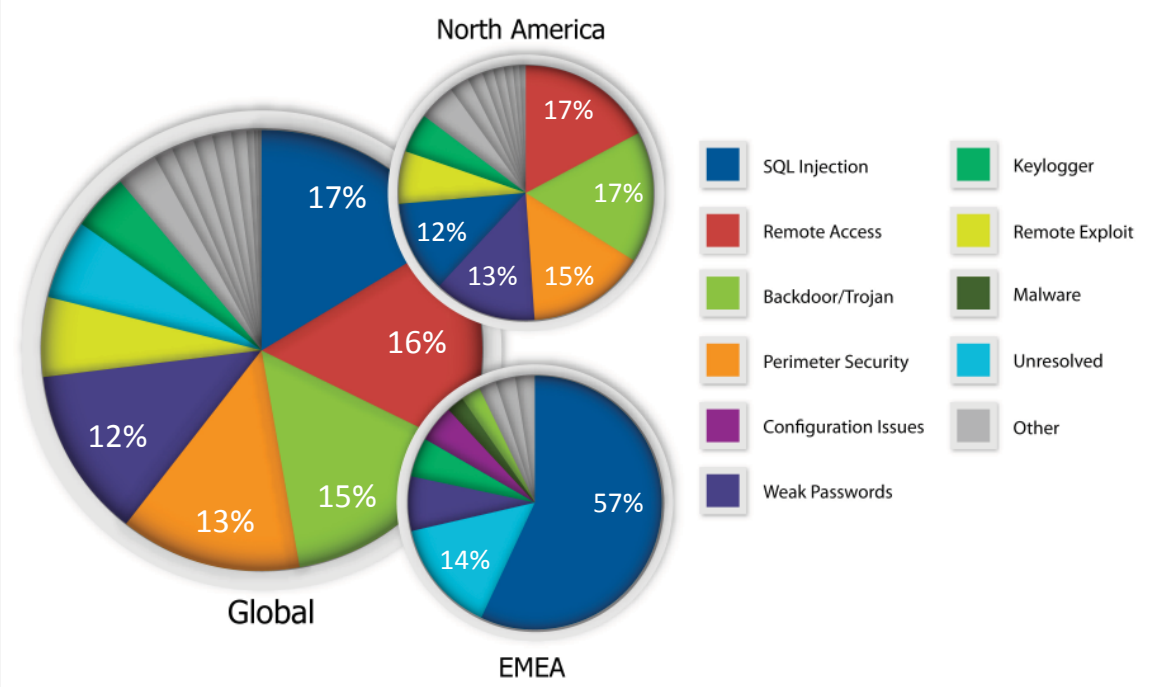
Common PCI DSS Failures of Compromised Merchants

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 3: Protect stored cardholder data
- Requirement 6: Develop and maintain secure systems and applications
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- Requirement 12: Maintain a policy that addresses information security for employees and contractors

Cases by Technical Cause

Trustwave finds that five technical causes contribute to the majority of payment card compromises across both North America and EMEA:

- SQL Injection: An attack technique that exploits flaws in a Web application to force a back-end database to answer queries submitted by the attacker and disclose information stored in the database (such as cardholder data) through the application itself.
- Remote Access: An attacker gains control over remote control software used to access a merchant's network from a remote location to gain access to the merchant's network and steal cardholder data.
- Backdoor/Trojan: An attacker installs malware (unauthorized software) onto a system without the operator's knowledge to gain access to a network and steal cardholder data.
- Perimeter Security Issue: The lack of a firewall or an improperly configured firewall allows an attacker to penetrate a merchant's network via the Internet and steal cardholder data.
- Weak Passwords: Because a merchant's passwords are not complex enough, an attacker is able to guess authentication credentials (username and password) and gain access to the merchant's network to steal cardholder data. This is typically done through the "brute force" method of attack.



Common PCI DSS Failures of Compromised Merchants

The majority of compromises investigated by Trustwave in North America occurred due to insecure payment applications that store prohibited data; however, as noted in the first section of this report, the theft of cardholder data in transit is on the rise. In addition, many times those payment applications are supported and maintained remotely by their vendors. Many organizations do not have security policies in place to ensure the security of their remote access software.

The continued prevalence of the lack of a firewall is troubling. Many merchants continue to fail to institute one of the most basic data security controls.

The continued prevalence of the lack of a firewall is troubling. Many merchants continue to fail to institute one of the most basic data security controls. Or if they do implement a firewall, they fail to configure it correctly to block inbound or outbound access that isn't imperative to business. Also, the lack of good password policy also allows many attackers to guess them and use credentials to gain administrative access of a system and find cardholder data. Many times, this is the result of a merchant or integrator failing to change the default/factory-installed credentials for a piece of technology.

Trustwave also sees many cases involving the use of SQL injection attacks to steal data from a back-end database that includes cardholder data. More often than not, these cases involve the compromise of an e-commerce merchant. However, the use of SQL injection can extend beyond just querying a database. For example, an attacker could use SQL injection to attack a Web server and eventually a processor's network switch (a network device that directs data to different network segments). SQL injection is extremely dangerous because it can be used to not only extract data but also gain a foothold in a network.

As illustrated in the chart above, SQL injection is the number one cause of compromise cases investigated by Trustwave in EMEA. Again this can be attributed to the fact that more e-commerce merchants are compromised in EMEA. In order to conduct business, an e-commerce merchant must use a public-facing Web site that may make their system vulnerable. An attacker will scan the Internet for sites that may have coding weaknesses and then exploit those sites to gain access to a backend database that includes cardholder data.

Conclusion and Merchant Action Items

The key take-away from this report is that merchants must comply with the PCI DSS. Plenty of data security pundits continue to disparage the standard. However, the PCI DSS provides a comprehensive security standard that when followed, prevents the theft of cardholder data.

Trustwave could pull out what we deem especially important requirements for merchants to follow. Unfortunately, this defeats the purpose of the standard. Emphasis on one requirement over the other forces other requirements into the background. Complying with one requirement and not another leaves gaps in an organization's security stance. An organization may have eliminated the storage of data prohibited by the card brands, but if they do not comply with the entire standard, a criminal can penetrate their network and gather that same data even if it isn't stored to disk.

An organization may have eliminated the storage of data prohibited by the card brands, but if they do not comply with the entire standard, a criminal can penetrate their network and gather that same data even if it isn't stored to disk.

Merchants must comply with the PCI DSS in its entirety. This statement is redundant because compliance requires the fulfillment of every requirement in the standard. To protect themselves and their customers, merchants must take a holistic approach to data security—an approach such as that prescribed and explained in the PCI DSS.