SECURITY MATTERS

Insights on Advancing Security and Fraud Management for Payment Cards

MasterCard Worldwide

Security Considerations for Mobile Point-of-Sale Acceptance

Smartphones and tablets are providing users with an ever-expanding set of capabilities. But what does this mean for user security? Story on page 28

ALSO INSIDE

Payment System Integrity

In this Issue

In this Issue

HARDENED
MasterCard
5412 7512 3412 3456
5412
TITANIUM
VALID THRU 12-14
LEE M. CARDHOLDER
MasterCard

Promoting Stronger Data Security Through EMV and M/Chip

An Integrated Circuit Card (ICC), or chip card, contains a processing unit that is able to execute functions such as the verification of a PIN and more complex calculations using cryptographic algorithms, such as Triple-DES[1] (symmetric key cryptography) and RSA[2] (asymmetric key cryptography). By design, the advanced physical and logical security features of the integrated circuit, as they relate to tamper resistance, protect the sensitive data stored on the chip, such as PINs and cryptographic keys.

FROM MAGNETIC STRIPE TO CHIP

For many years, the card validation code (CVC) has been the only electronic security component for payment card transactions based on magnetic stripe technology. The CVC is a cryptographic value (cryptogram) derived from specific card data, including the primary account number (PAN), using the Triple-DES algorithm with an issuer-owned secret key. The CVC is coded in the track data of the card's magnetic stripe and read by the point-of-sale (POS) terminal at the time of the transaction. During an online authorization, it is verified by the issuer (or delegated entity) to validate the authenticity of the card data.

Despite the benefits first offered by magnetic stripe technology, there are two challenges with the technology that criminals have exploited. First, the CVC value is static, which means that it does not change from transaction to transaction. A fraudster who is able to capture the magnetic stripe data of a genuine card (e.g., through skimming at the point of interaction [POI]), can then copy that genuine card data (including the PAN and a correct CVC value) onto counterfeit cards. Second, CVC values can only be validated online, as they provide no data protection offline. ›

[1] DES = Data Encryption Standard

[2] RSA = Ronald Rivest, Adi Shamir, and Leonard Adleman, the co-inventors of this algorithm

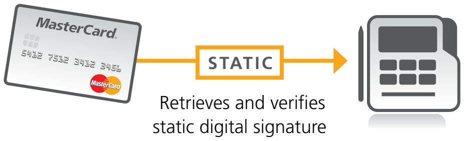
CHIP AUTHENTICATION TECHNIQUES AND ATTACK VECTORS

Chip cards address the magnetic stripe static data counterfeit attack vector by using more active cryptographic technology to authenticate the card via a challenge-response protocol. Chip cards have always provided more robust online defenses in comparison to other technologies. However, as chip card technology has evolved, issuers have been presented with various offline authentication options, starting with static data authentication (SDA), then dynamic data authentication (DDA), and now combined data authentication (CDA). During a transaction, the terminal will seek to use the strongest authentication option available on the card, starting with CDA as the highest preference, then DDA, and finally SDA.

SDA 🔒

With this technology, a static digital signature of some card data is assigned by an issuer to the card. During a transaction, the signature is verified at a POS terminal to authenticate the card data. Although a chip is used, and the data passed to the terminal is longer than the CVC on a magnetic stripe, the data itself is still static. Therefore, SDA remains vulnerable, because the static signed data can be captured (just like the CVC) and copied to make a fraudulent transaction that would be accepted offline. The copy, known as an SDA clone, can be designed to allow for the authentication of transactions offline without needing to know the original card's PIN. Further, the clone would be programmed to simply decline the transaction if the terminal chose to try to execute the transaction online. The reason for that decline is that the clone could be detected as a counterfeit device if it were to execute a transaction online, since it would be unable to produce a correct online dynamic cryptogram.

SDA CARD AUTHENTICATION

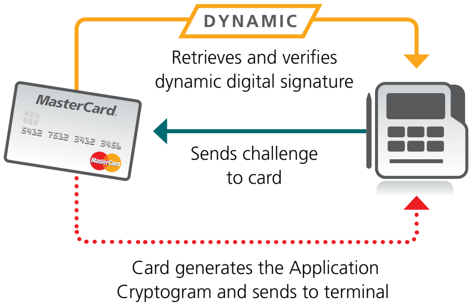


DDA 🔒🔒

This technology provides offline security by utilizing an offline, active challenge-response protocol (i.e., the card generates a new cryptogram for every transaction). During a DDA chip card transaction, the POS terminal requests that the card generate a cryptogram based on a random data element sent to the card. In contrast to SDA, which is passive, DDA chip cards actively use this random data element together with card dynamic data and a cryptographic key stored in its secure memory to compute a dynamic digital signature that is sent to the terminal for validation. Because the data signed by the card is unpredictable (dynamic) for each transaction and the fraudster does not have access to the key used to generate it, the fraudster will not be able to recreate a transaction, as is the case for a static CVC value or an SDA-enabled card.

DDA technology, however, is vulnerable to an attack vector known as a wedge or man-in-the-middle attack. In this attack, a wedge device is inserted between a lost or stolen genuine card and the terminal that makes the terminal erroneously believe that the card successfully verified the PIN and that the card approved the transaction offline. Although such attacks have been reported, the possible financial gain from the attack is limited to transactions that would be accepted offline by the terminal. However, CDA addresses this risk and provides additional protection.

DDA CARD AUTHENTICATION


DYNAMIC
Retrieves and verifies dynamic digital signature
MasterCard
5432 7512 3432 3456
Sends challenge to card
Card generates the Application Cryptogram and sends to terminal

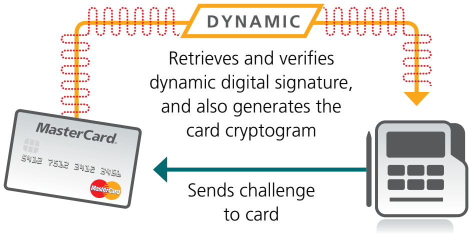
CDA 🔒🔒🔒

CDA is an inexpensive enhancement of DDA, essentially changing the timing during the transaction flow in which the card generates the Application Cryptogram (AC). More precisely, the card computes the AC before the DDA, and includes the AC together with proof that the PIN was verified and other transaction data in the digital signature, which can be verified by the terminal. This change prevents offline wedge attacks, while maintaining the additional benefits of DDA. CDA further provides a complete transaction integrity solution by enabling the card to generate a digital signature on the completed transaction that can be verified by the terminal. Currently, CDA has no known implementation attack vectors short of compromising the tamper resistance of the chip card itself.

🔒 = Authentication strength

CDA CARD AUTHENTICATION

Card computes the AC before the DDA, and includes the AC together with proof that the PIN was verified and other transaction data in the digital signature. This change prevents offline wedge attacks.


DYNAMIC
Retrieves and verifies dynamic digital signature, and also generates the card cryptogram
MasterCard
5432 7512 3432 3456
Sends challenge to card

M/CHIP SECURITY FEATURES

In the 1990s, the payment brands of Europay, MasterCard, and Visa (EMV) jointly established a common industry standard for the usage of chip cards for payment transactions. Since then, updated versions of the EMV standard have been published and MasterCard has developed the M/Chip product from this standard. The security features of the M/Chip product used during a transaction are summarized below.

Offline PIN Verification: The chip card can verify the accuracy of a customer PIN entered at the POI. The transmission of the PIN between the PIN Entry Device (PED) and the card can either be in the clear or encrypted. The encryption mechanism used is based on asymmetric cryptography with digital certificates.

Offline Card Authentication: The aim of this process is for the terminal to authenticate the validity of the card, thereby allowing the authentication to occur offline. The dynamic offline card authentication method is based on the challenge-response protocol. More precisely, the card dynamically signs a random challenge from the terminal together with specific card data. Then, using digital certificates retrieved from the card, the terminal can verify the accuracy of the dynamic signature (response) generated by the card. This process establishes the authenticity of the card and the integrity of the card data. It also takes place between the card and the terminal, and does not require interaction with the issuer or other parties.

Risk Management: Besides the terminal executing risk management protocols, M/Chip uses the computational capabilities of the card to execute its own risk management protocols based on features configurable by the issuer. Such features include determining the total cumulative amount of the transactions or the number of transactions approved offline since the last online transaction, and if these values exceed certain thresholds, the card will request an online authorization.

If either the card or the terminal risk management protocols concludes that an online authorization is required, this conclusion will always supersede the decision of the other to approve the transaction offline.

Application Cryptogram: This function enables the card to generate a dynamic cryptogram (called the Application Cryptogram) over a random challenge sent by the terminal, card data, and transaction data (including the transaction amount) using a secret key securely stored in the card and shared with the issuer. If an online authorization is required, the Application Cryptogram together with the other data is sent to the issuer, which can then verify the accuracy of the cryptogram and thereby establish the authenticity of the card and the integrity of the card and transaction data. The response of the issuer (i.e., approve or decline the transaction) is then sent back to the card protected by another cryptogram, which can be verified by the card.

If the transaction is approved offline, the Application Cryptogram can be stored and used later by the issuer to verify that the transaction was genuine (e.g., in case of a dispute).

SUMMARY

M/Chip uses the full computational capabilities of a chip card to implement state-of-the-art security functions to secure a transaction when executing:

- Offline customer PIN verification by the card;
- Dynamic offline (terminal) and online (issuer) card and data authentication; and
- Card risk management protocols as defined by the issuer.

Furthermore, it is important to note that the three basic security functions contained in M/Chip—namely the cardholder verification via offline PIN, the card and data authentication using symmetric cryptography, and the card and data authentication using asymmetric cryptography—can be used as generic functions to secure any system requiring some form of authentication.

And finally, the usage of M/Chip cards in conjunction with a user device, such as a Chip Authentication Program (CAP) reader or a keyboard and display, enable a cardholder to generate dynamic passwords for various applications, such as home banking and MasterCard® SecureCode™ authentication. ■

PROMOTING THE INTEGRITY OF THE GLOBAL PAYMENTS SYSTEM THROUGH LIABILITY SHIFT INITIATIVES

In its role as a founder and early proponent of EMV technology, MasterCard has executed a strategy to combat card fraud in many regions around the world that relies heavily on enabling chip-based payment transactions. MasterCard has been a primary driver behind the impressive strides that EMV technology has made in addressing fraud in regions that have migrated or are in the process of migrating to chip-based payments. EMV has exceeded expectations in reducing counterfeit and lost & stolen fraud. EMV also has provided the marketplace with increased operational efficiencies, improved offline risk management, and a host of enhanced value-added solutions that go beyond simply making transactions more secure for cardholders.

As part of this global effort, MasterCard instituted an EMV chip liability shift program (recently extended to the U.S. region) to help ensure global payment card interoperability, while appropriately acknowledging the substantial global investments that various entities in the payment value chain have made to protect and safeguard sensitive data from fraud.

Across mature EMV markets, the migration to this technology has greatly reduced the viability of certain fraud attack vectors. Additionally, as more markets move towards widespread adoption of EMV, the entire payment card ecosystem will continue to reap the benefits.

To help foster that reality, MasterCard is committed to working with issuers and acquirers worldwide in building new EMV roadmaps and enhancing existing ones to ensure that key learnings and best practices for migration are clearly understood and implemented. Throughout the migration process, MasterCard will work with its customers to ensure that the balance of risk in the global payments system reflects the balance of investments made to promote stronger data security by the thoughtful and conscientious stakeholders that support this technology.

Preventing BIN Attacks

Bank identification number (BIN) attacks on unprotected accounts have the potential to cause significant financial losses in a short amount of time.

This type of attack is likely due to criminals constantly seeking authorizations on randomly-generated BIN ranges in an effort to obtain a positive authorization for valid account numbers, which can then be used for fraudulent transactions.

Criminal probing-type activities that lead to BIN attacks can occur during all stages of a BIN's lifecycle and are not necessarily associated with a specific BIN status change. Therefore, constant vigilance is required, because if no authorization controls are in place, inactive or low-activity BINs can present a fraud risk to issuers whereby transaction losses may quickly occur.

BIN Attack Prevention Measures

Issuers should closely and continuously monitor transaction activity on both active and inactive BINs to detect potential fraud patterns. Issuers also should initiate the following security measures to help mitigate BIN attacks.

Review and customize Stand-In parameters to align with cardholder portfolios. This action helps to ensure that valid accounts are approved. Issuers should also leverage Negative Listings to help ensure that invalid (e.g., lost, stolen, and closed) accounts are declined.

Check Stand-In transaction logs for suspicious activity. When transactions are in Stand-In, logs are created to help identify and record suspicious activity. When operating in or immediately following Stand-In processing, issuers should review these logs to determine whether transaction patterns are out of the ordinary.

Choose BIN range blocking to protect account ranges. Selecting this offering can help prevent fraud from occurring on accounts that are inactive or not yet issued to cardholders.

Issuers should closely and continuously monitor transaction activity on both active and inactive BINs to detect potential fraud patterns.

Stand-In Service Fraud Management Services

MasterCard offers a Stand-In Service to help enhance the integrity and reliability of our issuing customers by ensuring an authorization response when an issuer cannot respond because of unexpected outages, data communication errors, or planned maintenance interruptions to their systems.

Since events that trigger Stand-In processing are quite often outside of the control of the issuer, the following services offered by MasterCard can help ensure that issuers protect inactive BIN ranges—including newly licensed BIN ranges not yet issued to cardholders and existing BIN ranges in an inactive state of low or no cardholder activity.

Stand-In Range Blocking Service

This offering blocks authorization requests in Stand-In to assist issuers in managing risk on inactive accounts or accounts not yet issued. Issuers are able to block an entire BIN range or a segment of a BIN range, defined up to 11 digits.

Transaction Blocking Service for Inactive BINs

This feature helps issuers avoid large-scale fraud attacks by providing preventive, backup authorization controls that deny unauthorized use of non-issued or inactive BIN ranges. The service blocks transactions on specified card ranges when transactions are processed online. It also blocks authorization requests for an entire BIN range or a segment of a BIN range, defined up to 11 digits.

Magnetic Stripe Validation Service

This service provides additional testing of the magnetic stripe, or card validation code 1 (CVC 1) data, using a Data Encryption Standard (DES) algorithm to validate the legitimacy of the card and the authenticity of the point-of-sale (POS) or ATM transaction.

Stand-In Investigation Service (SIS)

MasterCard also has developed the Stand-In Investigation Service (SIS) as an enhancement to its Stand-In processing services for detecting suspicious authorization requests processed by Stand-In through MasterCard's Expert Monitoring Solutions. This service incorporates a proprietary analytical tool that notifies MasterCard personnel when an authorization request processed by Stand-In indicates certain risk factors. It also allows MasterCard to help detect and advise issuers about suspicious authorization requests of this nature.

SIS comprises the following three categories of available services:

SIS Attack

The MasterCard Fraud Investigations team will work with the affected issuer to verify and help eliminate any identified vulnerabilities related to suspicious authorization requests. If MasterCard considers the suspicious activity high-risk after its investigation, MasterCard will provide critical information to the affected issuer and then follow the issuer's instructions to help resolve the situation.

SIS Warning

This service occurs when MasterCard monitors Stand-In authorization requests for early warning signs (testing or probing) of fraudulent activity typically associated with Card-Not-Present (CNP) authorizations at suspicious merchants. Based on these warning signs, MasterCard can then work with the affected issuer to verify and help eliminate any identified vulnerabilities.

SIS Monitoring

This optional service allows issuers to request short-term or recurring monitoring of their Stand-In transactions by MasterCard using customized transaction monitoring parameters. ■

PREVENTING CVC 1 BRUTE FORCE AND INVALID SERVICE CODE ATTACKS

Phishing scams present a variety of fraud management challenges for issuers when it comes to exploiting payment card data. Because any unsuspecting cardholder can fall victim to an official-looking online or social media phishing ploy, fraudsters can quickly gain access to a number of valid primary account numbers (PANs), expiry dates, and PINs, as well as specific personally identifiable information (PII). By leveraging this information, criminals can engage in a wide range of fraudulent activities, including card validation code 1 (CVC 1) brute force and invalid service code attacks. This article provides an overview of the attack methodologies and offers fraud mitigation techniques related to these two fraud schemes.

BRUTE FORCE ATTACKS TARGETING CVC 1 VALUES

In this type of attack, criminals use high-speed computer programs and stolen merchant IDs to test phished payment card data in association with multiple combinations of possible CVC 1 values. After valid authorizations are received, fraudsters engage in test transactions of small dollar authorization amounts, typically less than a dollar, which are run through a compromised merchant ID in order to identify a valid CVC 1 value. These brute force attacks may occur in a short timeframe and usually involve repeated attempts on a single PAN to identify the valid CVC 1 value. Once a valid CVC 1 value has been identified, criminals can use the other phished cardholder payment card information to counterfeit a card and commit additional fraudulent transactions, usually at ATMs.

To address this type of brute force attack, issuers should continue to raise awareness among their cardholders regarding the various forms of phishing scams currently occurring in the marketplace. It is important that cardholders safeguard their payment card data from scams, such as traditional phishing (phone or e-mail messages), smishing (text messages), and fraudulent social media requests asking for personal information.

Issuers also need to make sure that they have dynamic authorization and fraud control strategies in place to address this risk and avoid financial losses associated with this attack methodology. These strategies should ensure that they identify the attack, decline the associated transactions, and status the impacted accounts without loss. Specifically, issuers also should review the authorization and fraud velocity controls for PANs and merchant IDs and establish alerts when limits or parameters are exceeded. If issuers need additional assistance in mitigating this type of fraud, MasterCard will gladly work with them to create specific fraud rules and strategies to identify this type of attack. Such support may involve assigning a reason code to a rule(s) that will be inserted into the Authorization Request/0100 message. The reason code then can be used to define authorization and queue management strategies on an issuer's authorization system.

INVALID SERVICE CODE ATTACKS

000

Another potential fraud attack vector that hackers have been able to exploit through phishing scams involves using an invalid service code value of 000 for the CVC 1 entry. The service code, a three-digit numeric value, is encoded in the Track 1 and Track 2 data of a card and indicates to a magnetic stripe-reading terminal the transaction acceptance parameters of the card.

The presence of the invalid service code 000 in magnetic stripe transaction authorizations is a likely indicator that counterfeit fraud is occurring. In this scenario, criminals take the phished cardholder data—such as the PAN and expiry date—to produce counterfeit magnetic stripe cards encoded with the service code of 000 and with the phished CVC 2 value in place of the CVC 1 value in the track data. When issuers use the same cryptographic Data Encryption Standard (DES) key to verify the CVC 1 and CVC 2 values, criminals are able to commit ATM fraud with the phished PIN, so that the transactions are able to pass the CVC 1 check and be authorized by issuers.

Based on this attack vector, issuers are strongly recommended to promptly implement system edits that will result in the decline of authorization requests containing 000 service codes. Issuers also should set their authorization system parameters to recognize 000 as an invalid service code when verifying the CVC 1 value encoded on Track 1 or Track 2. Additionally, they should decline such magnetic stripe transactions as a fraud prevention measure. This recommendation applies to both magnetic stripe-only cards and EMV cards used in magnetic stripe environments. ■

Helping Cardholders Avoid the Phishing Hook

Cardholders must safeguard their payment card data from scams such as:

- Traditional phishing (phone or e-mail messages)
- Smishing (text messages)
- Fraudulent social media requests asking for personal information

Protecting Prepaid Cards Against Fraud

The ever-increasing growth of prepaid cards represents a sizable business opportunity for many issuers. In addition to becoming the ubiquitous gift-giving option, consumers also greatly appreciate the benefits that these cards provide as an alternative to carrying cash or travelers checks. Organizations also see the benefits of using prepaid cards to support payroll and benefit payments, while their employees have learned to value the increased flexibility and security that these cards offer in contrast to paper checks.

However, with these opportunities, come potential risks. Broader distribution channels also mean that issuers are offering prepaid cards with all of the utility and risk associated with universally-accepted payment cards. Consumers who may not have passed a typical issuer screening process or have no direct business relationship with the issuer are now able to take advantage of the prepaid card program benefits.

These prepaid card dynamics, combined with many of the same fraud attack vectors used against credit and debit cards, represent a different channel for criminals to commit fraud. Therefore, issuers must be able to manage potential prepaid card program risk in the same manner that they manage credit and debit card risk.

INCORPORATING RISK MANAGEMENT CONTROLS AS PART OF DAILY OPERATIONS

Issuers should include a variety of risk controls in their daily operations to help reduce their exposure to prepaid card fraud. They also must set minimum risk criteria for both current and new customers and establish the appropriate level of screening for portfolios. Additionally, limits must be established for the initial value load or stored value of an account, as well as the reload value depending on the type of product and characteristics of the prepaid program.

Authorizations

Setting reasonable daily limits for both ATM and point-of-interaction (POI) transactions is the first line of defense for any kind of potential loss. Issuers should create checks and balances to ensure that all authorization systems are working from similar balance information. Issuers also need to have authorization monitoring and loss-control programs in place to track velocity and spending limits on individual accounts on a single-day and multiple-day basis. MasterCard also recommends that issuers have the capability to respond in real-time when the fraud and risk controls are triggered during the authorization process. Having documented policies and procedures around these authorization controls is vital to keeping a prepaid portfolio current and accurate.

Posting Transactions

Prepaid card transactions, just like debit card transactions, should be posted to an account as soon as a valid authorization is provided. This process ensures that funds are available for transactions that may take time to settle and post against the account. Issuers should consider instituting a policy to hold available funds that can match the clearing transactions. A separate policy should be implemented for transactions with no matching authorization record. Issuers should also consider implementing a process to hold credits and force-posted authorizations until such records can be matched to off-setting debits or approved authorizations. *Note: Transactions clear on average within two or three days, so the hold period should accommodate for the clearing transaction, but not be longer depending on the market.* ›

$100
choosing your own gift:
priceless
a $100 gift card just for you

FRAUD CATEGORIES

The following overview describes the top fraud categories and provides recommended practices for issuers to help control losses resulting from these types of fraud as they relate to prepaid cards.

Lost/Stolen Card Fraud

Fraudulent activity commonly occurs as the result of a lost or stolen card, which fraudsters use to post transactions to the account. Issuers should consider the following risk management tools to help control lost and stolen card fraud:

- Daily reviews of exception and velocity monitoring reports can help identify potential problems with accounts. The following categories should be reviewed:
  - Transaction amounts in a rolling 24- to 48-hour period
  - Dollar amounts in a rolling 24- to 48-hour period
  - Expiration date mismatch
  - Multiple mismatched card validation code 1 (CVC 1) decline reason codes
  - Daily decline reason code
  - High-risk merchant category codes (MCCs) and country codes
  - Non-monetary changes to accounts
- Mail or ship inactive prepaid cards that require cardholder activation

The ability to monitor exceptions in these categories allows the issuer to better control risk and enable more proactive customer service when identifying potential fraud on cardholder accounts.

Card-Not-Present Fraud

Card-Not-Present (CNP) fraud involves non–face-to-face transactions where fraudsters obtain account numbers and fraudulently use them to make purchases via phone, through the mail, or on the Internet. Computer-savvy criminals can generate or extrapolate valid card numbers using bank identification number (BIN) listings or existing numbers from various Internet programs. A number of approaches can help prevent losses associated with CNP fraud, regardless of how the criminals obtain the account numbers, including:

- Address Verification Service (AVS)
- Mismatch expiration date programs
- CVC 2
- Daily reporting for MCCs and country codes
- Daily reporting for merchant authorization denial/fraud advisory codes
- POI entry mode
- MasterCard® SecureCode™

Counterfeit Cards

Counterfeiting has become much more sophisticated as criminals have developed new ways to obtain genuine cardholder account information. This obtainment allows the fraudsters to create embossed, printed, or re-encoded cards bearing trademarked and branded icons. Issuers should consider implementing the following security controls to help mitigate counterfeit fraud:

- Validate the expiration date in all authorization requests
- Use neural network fraud detection technology with a prepaid or debit behavior model to monitor authorizations for unusual activity
- Perform CVC 1 verification on all authorization requests (ATMs included), as well as CVC 2 verification on all non–face-to-face transactions
- Establish expiration dates on the CVC and change periodically to avoid potential compromise
- Review authorization exception reports for patterns of key-entered transactions
- Implement strategies to monitor authorizations from high-risk MCCs and country codes
- Review clearing data for transactions under the floor limit for non-issued account numbers
- Monitor for authorization attempts on consecutive account numbers
- Monitor for CVC 1 mismatch decline velocity
- Monitor for exceeds PIN-entry attempts
- Implement a card reissue decision matrix and special authorization monitoring for accounts that have been part of past data breaches
- Monitor for unusual settlement activity such as credits or force-posted authorizations without matching authorizations
- Randomly issue account numbers and vary the expiration dates

ANTI-MONEY LAUNDERING CONSIDERATIONS

Consideration should also be given to the unique anti-money laundering (AML) risks that prepaid cards may pose. In doing so, there will likely be a clear need to incorporate risk-based controls, such as load and velocity limits on the different delivery channels. Issuers should consult with their legal and compliance departments to ensure that appropriate AML policy, procedures, and risk controls are in place for their prepaid card portfolio. Prepaid programs must meet local regulatory requirements and network standards for AML. The program, at a minimum, should include:

- Customer identification procedures
- Suspicious activity monitoring and reporting
- Record keeping
- Independent control validation and refining
- Sanction screening

> *Issuers must be able to manage potential prepaid card program risk in the same manner that they manage credit and debit card risk.*

In addition to the previously described practices, issuers should also implement the following practices to help control prepaid card fraud:

- **Linking prepaid cards**—Issuing prepaid cards when there is an ongoing credit or debit account relationship
- **Knowing your business**—Ensuring that all parties are known by the issuer and that each party has an understanding of its role. This effort should include:
  - Third-party service providers
  - Processors
  - Program managers
  - Co-brand partners
  - Other program partners that might have a role in the distribution of payroll or incentive-type cards to employees

WHAT TO DO IF FRAUD OCCURS

The recommended monitoring of suspicious transactions helps issuers detect fraudulent patterns quickly, helping to mitigate the impact on their portfolios. In contrast, waiting for the legitimate cardholder to discover and report the fraud can cause significant brand damage as well as strain the issuer and cardholder relationship.

In the case where the cardholder information cannot be authenticated, such as with certain prepaid gift cards, the issuer should contact the consumer who purchased the gift card in an attempt to ascertain the identity of the actual cardholder. If possible, the issuer should attempt to verify whether the person who received the gift card was responsible for the transaction in question. The issuer should use a cardholder authentication process with personalized cardholder-selected questions to verify the identity of the cardholder. If the information obtained from these cardholder contacts confirms the suspicious activity, the issuer should block the card immediately to prevent further fraudulent activity. Even if the true cardholder has the card in his or her possession, an unauthorized purchase could indicate CNP fraud in which the fraudster used only the account number and not the actual card or possible counterfeit activity.

If an issuer identifies fraud on numerous prepaid accounts, the issuer should take the following important actions:

- Pull statements for the reported timeframes to determine a specific fraud trend or suspicious pattern. This action may help isolate a merchant that obtained account numbers of legitimate cardholders for fraudulent purposes as a potential account data compromise (ADC) event.
- Contact the card processor to obtain full authorization logs. An issuer's daily reports may not contain all of the detailed transaction information that is vital in identifying fraudulent activity. The logs provide critical information needed to analyze the fraud type and pattern of suspect transactions. The logs also contain other useful information, such as:
  - Merchant information (e.g., street addresses and terminal IDs)
  - Transaction amount details to help determine whether the sales were lower than the floor limits
  - Sequential account numbers used in fraudulent transactions ■

Understanding Website Navigation Layer Vulnerabilities

Since the commercialization of the Internet, there has been an evolution in how cyber criminals are conducting malicious activities on websites. They are finding an ever-increasing number of ways to steal information, commit fraud, game website logic, and impact business operations. Central to the explosion of cyber crime in recent years is the continued evolution of rich Internet applications and exposure of critical business operations to the worldwide web.

By Jesse McKenna
Fraud Analyst
Silver Tail Systems

The more that business operations (both internal and external-facing) move to web-enabled platforms in 2012, the more opportunities present themselves for criminals to find loopholes, mine for valuable data, and exploit legitimate website functionality.

Cyber criminals are becoming more creative and automating their way of exploiting vulnerabilities and business logic flaws at the Navigation Layer, which includes all behavior on a website and may be referred to as a "clickstream."

In 2012, the industry will begin to recognize a new classification of attacks executed through the Navigation Layer. This insight will begin to give organizations leverage as they start to look at web-born threats in a new way.

THE NAVIGATION LAYER

Basically, the Navigation Layer is how users of web services access and interact with various resources and functionality of websites. Purchasing a digital camera on an e-commerce site, balancing your checkbook using online banking, and interacting with project plans on a company's intranet are all examples of activities that take place in the Navigation Layer.

The reason that the Navigation Layer is such an attractive target for criminals is that the functionality that enables their criminal activities, in large part, has to be made available to legitimate users. As long as there are websites, criminals will be looking for ways to take advantage of the data and functionality made available through those sites. Although certainly not an exhaustive list, a significant portion of online criminal activity can be seen in the categories of:

- Business Logic Abuse,
- Data Scraping, and
- Architecture Probing.

TRADITIONAL SECURITY STRUGGLES TO PROTECT THE NAVIGATION LAYER

The cyber security challenge facing businesses and organizations is that it is notoriously difficult to detect and defend against Business Logic Abuse, Data Scraping, Architecture Probing, and other types of attacks executed through the Navigation Layer.

Traditional approaches that leverage deep-authentication of users, transaction risk-modeling, link analysis, and event correlation are still critical to have in place, but are rendered largely ineffective when confronted with "low-and-slow" processes scraping site data or with attacks carried out by networks of hundreds of personal computers (PCs)

infected with criminal-controlled malware. Moreover, criminals are continually changing their attack strategies and developing new methods of exploiting website functionality. Keeping detection systems up-to-date with the latest attack vectors is incredibly challenging.

DEFENDING AGAINST NAVIGATION LAYER ATTACKS

All of this may seem overwhelming and rightfully so. However, there are a few aspects of this type of criminal activity that begin to level the playing field.

First, these attacks all take place through the Navigation Layer and website owners control this layer. Although the functionality exploited by criminals typically is required for the use of legitimate users, businesses and organizations can have visibility into every aspect of the traffic going through the Navigation Layer. The ability to monitor this wealth of traffic is invaluable for detecting attacks coming through the website and for performing forensic investigations of past events to better inform detection and mitigation decisions in the future.

The other area where businesses and organizations have an advantage is that criminals, in order to execute their attacks, need to behave differently than normal users of a website. Normal users do not try to log in using tens, hundreds, or thousands of different passwords. Nor do they crawl entire product catalogs on e-commerce sites or submit nonsensical chunks of data to web applications in the hopes that they will break. By leveraging full visibility into the Navigation Layer, it is possible to perform behavioral analytics on every click on the website and rapidly identify the outliers—those web sessions that are not behaving like everyone else using the website.

As web applications and web-enabled devices continue to rapidly evolve, the attacks on the Navigation Layer will continue to keep pace—using the latest functionality for something other than what it was intended for. However, by maintaining full visibility into the Navigation Layer and on every click occurring on the website, these evolving threats can be detected and mitigated in near real-time, thereby preventing the often dramatic impacts of attacks that have gone unnoticed until the damage has been realized. ■

As long as there are websites, criminals will be looking for ways to take advantage of the data and functionality made available through those sites.

A Friend Request from ZeuS

Julie Conroy McNelley, *Research Director*
jmcnelley@aitegroup.com

Cyber crime is constantly evolving to stay one step ahead of the most recently deployed fraud mitigation technologies.

Cyber criminals are actively targeting the payment value chain, and financial institutions (FIs) are feeling the pain. Many of the organized syndicates responsible for these attacks span multiple countries, thereby complicating the efforts of law enforcement agencies to coordinate and stop them. Because cyber crime is such a lucrative business with few adverse consequences, the intensity of cyber attacks is rapidly increasing.

The fraudsters don’t need a business case to justify creating new ways to perpetrate crime, and their pace of innovation around cyber crime is escalating. Cyber crime is constantly evolving to stay one step ahead of the most recently deployed fraud mitigation technologies. Criminals leverage the coding efforts of their peers and continually “improve” upon the base model of a malware strain in an effort to avoid detection. A high-profile example of this evolution is a variant of the credential-capturing ZeuS Trojan that was first released a few years ago. Criminals deploying ZeuS realized that their efforts were often being thwarted when a business logged into its online banking site, detected an unauthorized transaction, and called its bank to stop payment. In response, cyber criminals developed a derivative strain of the malware to mask the unauthorized transaction in the online banking interface, so that the commercial customer would not identify the activity until it was too late.

FRAUD: COMING SOON TO A MOBILE PHONE NEAR YOU

In the mobile channel, most FIs are currently experiencing few mobile-fraud losses, largely because customer adoption of this technology is still in its early stages, and a low number of high-risk transactions have been processed via the mobile channel. However, this scenario is rapidly changing, as most risk management executives with whom Aite Group has spoken believe that mobile will be the next big area of exposure for financial services

Financial services innovation in the mobile channel is progressing rapidly, but there is an unfortunate paradigm in financial services that security often lags behind innovation. While transactional capability has been fairly low-risk to date, customer demand and the need for FIs to find new revenue sources are driving higher-risk transactional capability to consumer and business mobile-banking applications. A Q4 2011 Aite Group survey of global financial services risk executives found that while one in four respondents expects to increase security in the mobile channel, respondents are currently waiting to see how the risk environment will evolve.

Cyber criminals are well aware that the mobile platform is an increasingly attractive target for financial fraud, and they are deploying an increasing variety of attacks. The Android™ operating system (OS) is the favorite target of cyber criminals, but no mobile OS is immune. While there are far fewer strains of mobile malware than their online malware counterparts, mobile malware is growing at a faster rate, with 41 percent more unique malware strains detected in the first three-quarters of 2011 than in a comparable time period in 2010.[2]

Many mobile attacks emulate the malware directed against the computer, seeking to steal credentials, contacts, and other valuable data. The mobile platform also has unique characteristics that provide cyber criminals with interesting new opportunities.

The Trojan SpyEye has successfully intercepted and forwarded Short Message Service (SMS) messages used for out-of-band authentication, thereby enabling cross-channel fraud across the mobile and online channels. Two forms of malware have been detected on the Android platform that record voice conversations and forward the recorded calls to a hacker, who can then use the data for further social engineering. The mobile phone's geolocation data is susceptible to similar types of attack.

IN SEARCH OF THE SILVER BULLET

In light of the elevated risk environment, FIs are investing in a variety of fraud prevention technologies to protect themselves and their customers. Effective protection requires the combination of multiple technologies deployed to protect the endpoint, the online session, and the transaction itself. The U.S. Federal Financial Institutions Examination Council (FFIEC), recognizing that there is no silver bullet against the sophisticated and varied threats in the current environment, mandated a layered approach with its supplemental guidance.

The layered approach needs to be commensurate with the risk of the transaction; therefore, a higher degree of protection is expected for commercial customers than is required in the retail business. The risk-layered approach also needs to effectively balance effectiveness with the level of intrusiveness on the user experience. While some level of user participation is generally required—and even desirable in certain cases—the total user experience must not become so difficult that customers abandon remote channels altogether.

If the criminal is successful in one of 100 attempts, he or she will potentially profit with a sizable sum. Financial institutions, on the other hand, need to be perfect in their attempts to protect themselves and their customers.

The figure below provides a mapping of common remote channel fraud mitigation solutions. Based on interviews with 32 North American FIs, including 19 of the top 35, the figure maps the solution's perceived effectiveness and intrusiveness on the user experience.[3]

CONCLUSION

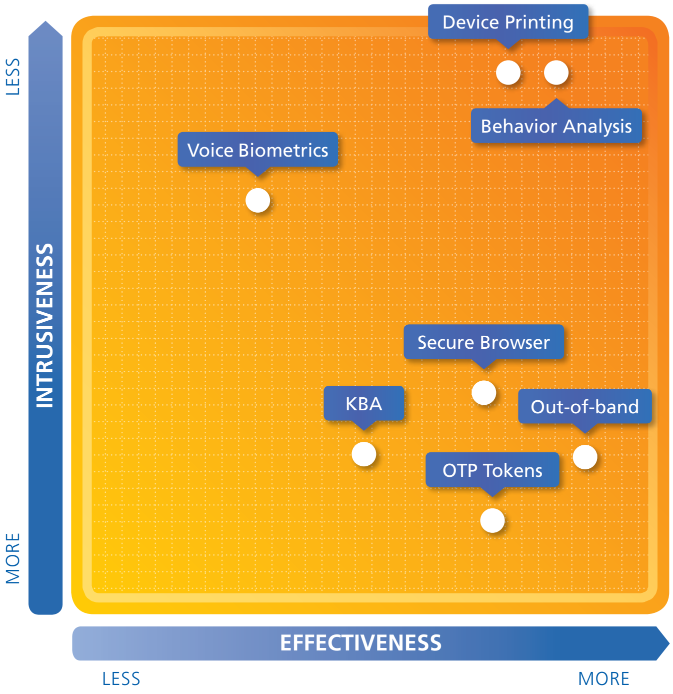
It is much easier to be successful at committing crimes than thwarting them; if the criminal is successful in one of 100 attempts, he or she will potentially profit with a sizable sum. FIs, on the other hand, need to be perfect in their attempts to protect themselves and their customers. While there are many tools at the FIs' disposal, the effort to secure remote channels against cyber crime will be more about the journey than the destination—as with all things related to fraud, cyber crime will remain an ongoing battle between the forces of good and evil. ■

[1] Aite Group, *Mobile Fraud: The Next Frontier*, November 2011.

[2] McAfee® Labs™, "McAfee Threats Report: Third Quarter 2011," http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf.

[3] Aite Group, *Online Fraud Mitigation: Tools of the Trade*, October 2011.

Remote Channel Fraud Technology Mapping: Effectiveness vs. Intrusiveness[3]



SUMMARY OF TECHNOLOGY TYPES

Behavior Analysis Detects fraud by monitoring the user session to detect anomalous behavior patterns using a combination of rules and analytics.

Device Printing Uses a combination of hardware and software attributes associated with a computer or mobile device to create a unique "fingerprint". This technology can be used to recognize devices associated with fraudulent activity, as well as identify devices with trusted reputations.

Knowledge-Based Authentication (KBA) Leverages demographic and credit data in third-party databases to dynamically create questions that the end user must accurately answer.

One-Time Password (OTP) Tokens Supply an expiring password, which changes on either an event- or time-driven basis.

Out-of-band Authentication uses a communication mechanism not directly associated with the device being used to access the banking site in order to facilitate a second mode of communication. The most common example of this mechanism is the transmission of a text message or voice call to a mobile device to authenticate a session or transaction that is taking place on a computer.

Secure Browser Uses client software or hardware to create a browser environment that is shielded from other applications and potential malware on a computer.

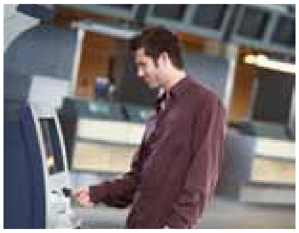
Voice Biometrics Use the end user's voice print to authenticate remote channel activity.

Preventing ATM Fraud

Automated teller machine (ATM) attacks and the resulting fraud continue to be significant concerns for issuers and acquirers around the world.

When it comes to ATM-based fraud, criminals are taking advantage of the proliferation of cash machines at less secure non-banking locations, which make these machines an appealing target for adding skimming devices to capture cardholder data. Criminals are also targeting small- to medium-sized financial institutions that may not have adequate security controls in place. Because these institutions have not traditionally been targeted, many of them do not have adequate protection measures in place. For example, they may not monitor their ATM terminals or be able to afford the sophisticated fraud detection technology necessary to identify patterns indicative of skimming and counterfeiting during card transactions.

The recommendations and best practices presented in this article are specific to the physical, logical, and procedural security requirements of the ATM. This article also provides guidance for cardholder considerations when they are conducting transactions at ATMs.



Cash machines at less secure non-banking locations make an appealing target for adding skimming devices to capture cardholder data.

ISSUER ATM FRAUD CONTROL PARAMETERS

In an effort to help mitigate the possibility of ATM-based fraud threats, issuers should consider implementing the following recommendations:

☑ Where applicable, issue EMV-capable chip cards, because these cards can be authenticated during each chip transaction at the ATM.

☑ Implement a strategic process for mailing ATM cards and their corresponding personal identification numbers (PINs), such as:
– Mail the PIN code and the ATM card separately.
– Send the separate mailings at least 24 hours apart.
– Disguise the envelopes containing the cards and PINs, so that they do not attract attention and alert non-recipients to their contents.

☑ Use a card activation process.

☑ Confirm cardholder address changes for both debit and credit accounts.

☑ Use card-based PIN offsets and validate offsets in the authorization process.

☑ Validate the card validation code 1 (CVC 1) value during authorization for PIN transactions and monitor CVC 1 mismatch activity.

☑ Review both the value and volume of ATM withdrawals.

☑ Monitor velocity checks on failed PIN transactions.

☑ Use neural network fraud detection systems.

☑ Consider lowering daily cash withdrawal limits to minimize exposure to risk.

☑ Report and track unauthorized card usage.

☑ Limit PIN usage to ATM/point-of-sale (POS) terminal access only, and use different authentication methods for customer service and online banking.

Issuer PIN Security Considerations

ATM PINs can either be generated by an issuer or selected by the cardholder. **If the PIN is generated by the issuer,** it should:

- Be derived from card data using cryptographic means. The cryptographic means must be secure, so that even if a hacker knows the number of inputs or outputs to the algorithm, it would be nearly impossible to deduce any further outputs. Additionally, the primary account number (PAN) must be included in the input.
- Be generated using a random or secure pseudo-random process compliant with International Organization for Standardization (ISO) 9564.
- Not contain the letters Q or Z.

If the PIN is selected by the cardholder, the cardholder should be advised that the PIN should not have a value that is:

- Readily associated with the cardholder (e.g., phone number, address, birth date, or other personal information).
- Part of data imprinted on the card.
- Consisting of the same digits or a sequence of consecutive digits.
- Identical to the cardholder’s previously selected PIN.
- Less than four digits in length.
- Using the letters Q or Z.

ACQUIRER ATM FRAUD CONTROL PARAMETERS

Acquirers need to maintain an accurate record of all of the ATMs within their inventory and ensure that the machines are monitored, inspected, and serviced regularly to ensure that non-authorized devices are not being used to capture sensitive card data and PINs. To support those efforts, acquirers should consider:

☑ Ensuring that bank branch staff understands how to detect overlays and internal capture devices.

☑ Training ATM service technicians to ensure that they conduct a detailed evaluation of key ATM components at each visit to ensure that there has been no tampering or modifications to the ATM.

☑ Performing due diligence on non-bank-owned ATMs by having access to current and accurate names and addresses of every ATM location participating in their program.

☑ Monitoring ATM terminal activity for:
- Card reader and dispense errors.
- PIN entry timeouts.
- Changes in transaction patterns at the machine, such as multiple balance inquiries, increases in "invalid PIN" messages and/or transaction velocity, and unusual transaction activity periods.

Physical ATM Security Considerations

Whether an ATM is located at a bank branch or remote location, it is critical that the physical security of the machine be closely monitored using a combination of electronic and physical inspections. The following tips and techniques should be implemented to make sure that ATM owners can be alerted quickly if a skimming or tampering attack does occur:

- **Video surveillance** – Cameras can be easily integrated with ATM machines, and stronger security can be achieved by installing additional site cameras on and around the premises. Not only is continuous surveillance a critical security issue, but remote sites offer particular challenges with regard to maintenance, which can be addressed by video monitoring.
- **Remote diagnostic services** – These services track and manage events at the ATM and can route information to a centralized resource capable of quickly responding to issues that may arise. For example, the continual notification via a remote diagnostic service of an incident regarding a card reader failure or a drastic decline in transactions at an otherwise high-traffic ATM location may be an indication of tampering.
- **Machine-based security features** – ATMs can be designed to prohibit or deter common attack vectors targeted against them. Card readers and cash dispense devices can be altered to reduce data capture devices and cash retract schemes. Machines can also be designed to reduce shoulder surfing and provide cardholders with greater comfort via rear-view mirrors or panic buttons.

Educate ATM users on practices such as shielding the PIN pad when entering their PIN.

ATM USER FRAUD PREVENTION EDUCATION RECOMMENDATIONS

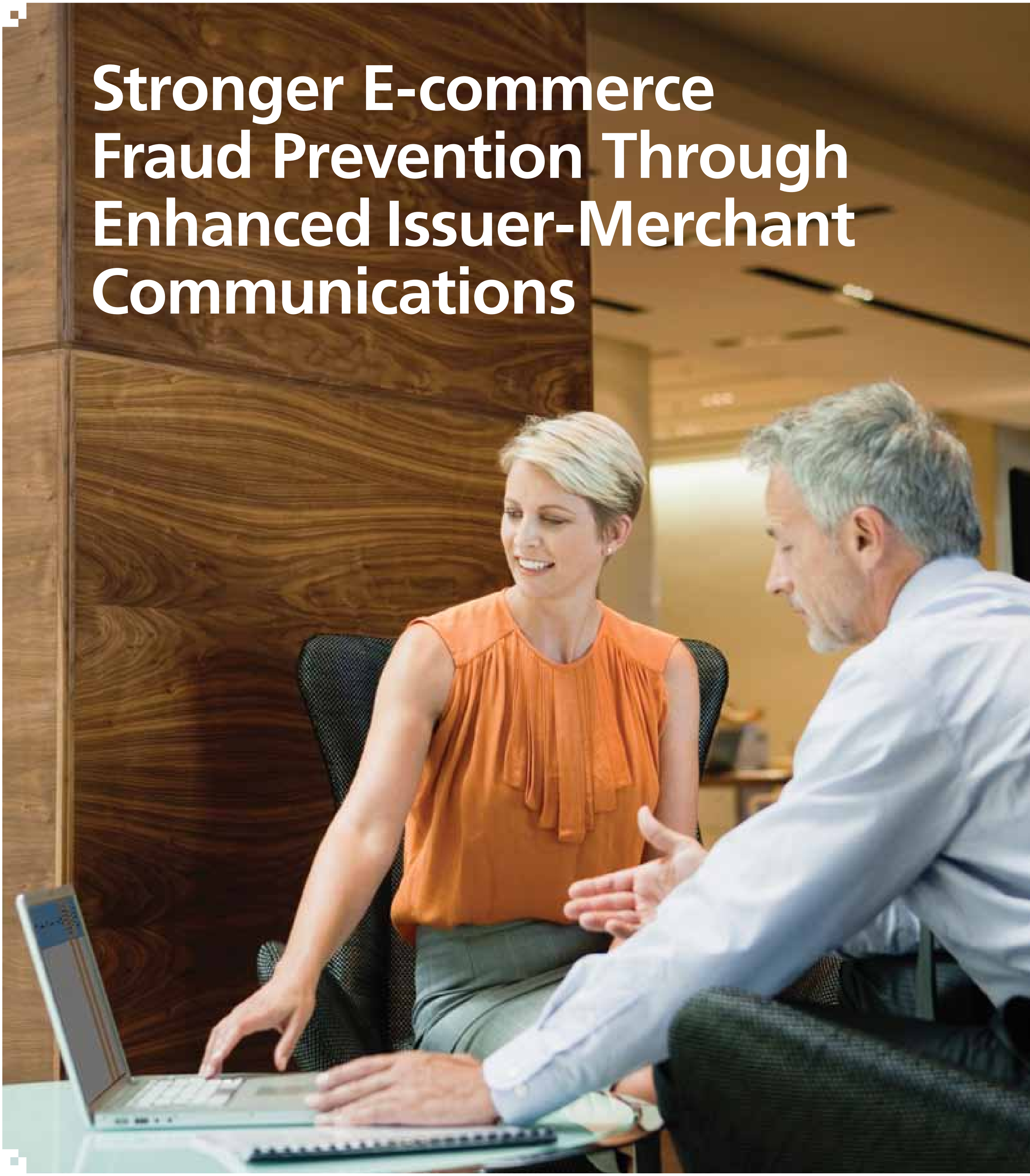
Financial institutions should emphasize the importance of awareness at the ATM to their cardholders and promote vigilance in reporting any irregularities in the appearance and operation of an ATM. Financial institutions should instruct consumers to contact their financial institution if they suspect ATM tampering. In addition to leveraging cardholders to report suspicious ATM occurrences or interactions, financial institutions also should:

☑ Educate ATM users on practices such as shielding the PIN pad when entering their PIN.

☑ Advise them to immediately notify their bank regarding an unauthorized ATM or debit card transaction on their account.

☑ Remind their customers to carefully review their monthly account statements or to use Internet banking to monitor for any suspicious activity on their account. ■

Stronger E-commerce Fraud Prevention Through Enhanced Issuer-Merchant Communications



Online shopping gives consumers immediate access to a wide world of commerce, from exotic vacations, to favorite books, to special gifts. But as merchants capitalize on this marketplace, with electronic commerce (e-commerce) transactions reaching record levels[1] and online Card-Not-Present (CNP) payments rising, the threat of online fraud is ever-present.

E-commerce merchants, who are the first line of defense against online fraud, feel perhaps the worst impact from fraudulent CNP transactions. Such transactions can lead to financial losses that include decreased direct revenue, as well as increased costs and chargeback rates. However, merchants are not the only stakeholders who feel the negative effects. Issuers themselves sustain fees to process chargebacks. In addition, customer satisfaction suffers as well.

Global CNP transactions are also growing significantly, as e-commerce crosses borders for merchants to sell their products and increase revenue. However, this opportunity presents authentication challenges as well. International CNP transactions are declined at a higher rate than domestic CNP transactions. Fraud-screening is more challenging, and standard validation tools may not be readily available or may be costly to implement. Because of an issuer's reluctance to approve cross-border transactions, merchants may not be able to fully capitalize on this new revenue stream, and thereby could risk losing both money and merchandise if an issuer declines a transaction after the merchant has already shipped an order.

A VIEW INTO ONLINE SECURITY THREATS

Fraudsters are increasingly targeting the Navigation Layer of websites where transactions take place. As such, e-commerce merchants may have little to no visibility into what is attacking them. And with fraud schemes evolving so rapidly, merchants may not even be aware of the many types of online threats that exist. Greater levels of communication about trends and detection methods between the merchant and the issuer could help reveal criminal activity sooner. Some of the common attack vectors that perpetrators are using to commit online fraud are malware, Botnets, and Web Logic Abuse *(see sidebars)*.

Malware

Malware is any software or code developed for the purpose of extracting information from a computer database or network without the owner's consent. This prominent threat in payment card data breaches runs silently on payment systems, capturing data and feeding a continuous flow of card information back to criminals. As malware becomes fully automated, it becomes more difficult to detect. In fact, 63 percent of malware in data breach cases cannot be recognized by traditional defenses as it involves specialized code.[2]

Botnets

Botnets are groups of malware-infected computers under the control of cyber criminals. Malicious software applications (contained within e-mail attachments or links to websites) turn a computer into a "bot" (or zombie), so that it will perform automated tasks via the Internet without the user even knowing it. Under a hidden identity, the bot can steal passwords, log keystrokes, and send out spam messages.

Web Logic Abuse

Web logic abuse uses legitimate pages and page flows of a website to conduct fraud. Attacks may take days or weeks to identify and manifest themselves in different forms:

- A *man-in-the-middle attack*, in which the merchant website is compromised, causes the cardholder to be unknowingly redirected to a malicious site at the time of checkout.
- A *man-in-the-browser attack* installs a piece of malware on the user's computer and establishes a background session utilizing the user's account and browser session to conduct malicious activity (such as transferring funds out of bank accounts or buying items).
- *Screen scraping* occurs when an attacker takes all of the information that a person has posted on his or her website or social networking page and uses that information to break into the user's account and commit identity theft.

Other common attacks include password guessing, phishing, and account takeover, all of which are designed to commit identity theft. There is also HTML injection, whereby an attacker introduces code into a computer program to change the course of execution.

The projected growth in these types of online crime is daunting:

- 25 million new strains of malware have been released in 2011, with expected growth to 87 million by the end of 2015.[3]
- Botnet infections enabling fraudster control of consumer computers are growing at about 200,000 per day.[4]

STRENGTHENING LINKS IN THE PAYMENT VALUE CHAIN

Fraudulent transactions have the potential to be as damaging as they are innovative. Issuers have been implementing systems to detect fraud on their side, while merchant investment in advanced fraud analytics technologies has increased significantly. Although issuers and merchants have become more sophisticated and more diligent in fighting fraud, criminals are just as focused on making it more challenging to detect.

It can be difficult to distinguish between legitimate consumers and criminals, as fraudulent orders are looking increasingly like real orders. E-commerce merchants need to gain greater visibility and insight into browsing behavior on their websites pre-checkout, before receiving orders from cardholders. This information is critical in determining whether a transaction is normal or unusual for a merchant's website—and it may only require the data that an issuer already possesses.

But while issuers and merchants would benefit from enhanced communication and information sharing, until recently, communication has been limited. Issuers do not notify impacted merchants when their research determines that a transaction is fraudulent and is therefore denied. Merchants, who may detect a fraudulent transaction on their end, have not had a clear channel for sharing such information with the impacted issuer.

ADDRESSING CHALLENGES, COMBATING THE THREAT

MasterCard is committed to closing the existing communication gap between issuers and merchants to lower fraud and increase approval of genuine transactions. One way that MasterCard has assisted in bridging these gaps is by enabling e-commerce merchants to decline CNP transactions approved by issuers but indicated as high-risk by merchant fraud detection solutions. To provide greater visibility for the issuer into acquirer and merchant fraud prevention practices, MasterCard has made sure that reason codes are required in the authorization reversal request message. In this way, MasterCard is helping participants in the payments industry fight back against fraud by improving detection methods and opening the communication channels.

In addition, MasterCard has established the CNP Advisory Group to address the specific challenges and opportunities for CNP transactions. This group represents merchants, acquirers, merchant service providers, and issuers, and focuses on three key objectives:

- Ensuring a positive CNP experience for customers and cardholders transacting within the remote payment environment.
- Enabling secure and safe remote payments.
- Creating an environment that fosters innovation and addresses issuer and merchant pain points related to CNP.

It can be difficult to distinguish between legitimate consumers and criminals, as fraudulent orders are looking increasingly like real orders.

25 mil
malware strains in 2011
87 mil
malware strains in 2015

Twenty-five million new strains of malware have been released in 2011, with expected growth to 87 million by the end of 2015.

MasterCard has also developed a number of online tools that help combat fraud and enhance communication between merchants and issuers.

E-commerce Fraud Alerts For Issuers
These alerts notify the issuer when an authorized CNP transaction has been refused by a merchant due to suspected fraud. Enhanced communication between merchants and issuers benefits all parties in the value chain by reducing chargeback losses as well as increasing cardholder confidence. Proactively alerting the issuer to suspicious activity gives the issuer the opportunity to communicate with its cardholders sooner, which ultimately results in an improved cardholder experience and strengthened cardholder relationship.

Merchant Fraud Scoring
Developed specifically for e-commerce merchants, this fraud scoring system expands these merchants' insights into cardholder behavior beyond their shopping cart. By delivering a highly predictive merchant fraud score, it more accurately describes online cardholder behavior, beyond the information that merchants received only from their website.

Web Session Behavior Monitoring
This system maps normal web flows, then monitors every click on the e-commerce website and computes threat scores based on abnormal traffic and flows. With a focus on the entire website interaction, rather than simply the transaction, it diverts sophisticated attacks on e-commerce sites using real-time web session intelligence, thereby stopping cyber criminals before they commit fraud.

MasterCard is continually working to develop greater functionality through infrastructure, service, and research and development initiatives to connect merchants, acquirers, and issuers. Better modeling, rules management, fraud reporting, web monitoring, transaction blocking, and open communication are some of our best defenses in combating growing e-commerce fraud attacks.

BETTER COMMUNICATION FOR MORE SECURE E-COMMERCE

The increased availability of more robust information about potential online fraud helps issuers and merchants in being more proactive and making better decisions about future transactions involving a cardholder's account. By working together as partners to manage the complexities of online transactions and share information, issuers and merchants can improve their fraud detection practices, reduce associated costs, and strengthen customer satisfaction. As a central touch point for both issuers and merchants, MasterCard is helping to open the lines of communication and make it easier for merchants and issuers to connect with this vital information. ■

[1] comScore, *U.S. Retail E-Commerce Sales Estimate*, Q4 2011 (spending reached a record $161.5 billion, a 13 percent increase from 2010)
[2] Verizon Business, *2011 Data Breach Investigations Report*
[3] Aité Group
[4] McAfee Corp, *A Good Decade for Cybercrime*

Small-Merchant Payment Application Installation and Integration Best Practices

Small merchants are being targeted at an escalating rate by criminals who are taking advantage of vulnerabilities in a merchant's system as a result of inadequate payment application implementations. The primary issue is that the payment applications themselves are not presenting an actual vulnerability, but rather it is the improper implementation of these applications that is allowing a data breach to occur.

Hackers scan the Internet looking for open remote access connections. They find active remote access sessions with little to no authentication enabled, which allows them direct access to the merchant's system. Once inside the system, criminals exploit any weak passwords, default vendor IDs, and stored cardholder data that exist within the merchant's environment neglected by vendors who the merchant relied upon for their technical expertise to properly set up the system.

The vast majority of small merchants do not have a large technology footprint, so in most cases their only areas of responsibility for maintaining PCI DSS compliance are the POS terminal and the payment application.

THIRD PARTY INTEGRATORS/RESELLERS

Merchants typically do not install or manage their own payment applications. They rely upon third party integrators or resellers to properly install and manage their payment systems. The vast majority of small merchants do not have a large technology footprint, so in most cases their only areas of responsibility for maintaining *Payment Card Industry Data Security Standard* (PCI DSS) compliance are the point-of-sale (POS) terminal and the payment application that they use to accept credit and debit card transactions. When it comes to data security and PCI DSS requirements, small merchants tend to place all of their trust in their vendors and implementers of their payment application to address any required security controls.

PCI DSS compliance is about reducing the risks associated with compromising cardholder data, and merchants have a responsibility to understand the risks to their business as they relate to the customer data that they store, process, and transmit. Merchants that take the time to understand their role in maintaining compliance with PCI DSS and data security requirements can greatly reduce their risk of compromising their customers' data. Therefore, it is important for acquirers to ensure that their small merchants become more educated about the levels of enforcement that can help those merchants realize that compliance with the PCI DSS requirements is just as much their responsibility as it is their third party integrators or vendors that support the merchants' payment applications.

MERCHANT RESPONSIBILITIES: TRUST BUT VERIFY

Purchasing and the ongoing management of firewall, anti-virus, wireless, and data storage systems are examples of responsibilities that completely belong to the merchant. An improper payment application implementation by a third party can undo any security that the merchant worked hard to establish. There is a practice in information security and audit called "trust but verify," which means simply don't completely trust anyone's assurance. For example, merchants should ask vendors and third party integrators to guide them through the product installations and learn the risks involved as well as the controls in place to prevent those risks.

The following examples highlight some of the most common vulnerabilities in payment application implementations that can lead to an account data compromise (ADC) event. Acquirers should stay informed about these vulnerabilities and work with their merchants to identify and remediate them.

Generic User IDs and Passwords

Payment applications with a generic username and password that are not changed following an installation are extremely vulnerable to compromise.

- Payment applications use a generic ID and password to initiate implementations across many different merchants. In many merchant breaches, the hacker was able to use the generic login account and generic password (e.g., vendorname123, 123456, password) to access the system, just as the merchant or vendor would.
- The merchant should validate that all generic accounts were deleted by the vendor after a unique ID and strong password are set up for the merchant.

Remote Access

Remote access solutions are considered incorrectly installed according to the PCI DSS, if they contain weak passwords or no password at all. Examples of weak passwords include device default passwords or actual passwords such as: password, 123456, vendor name, merchant name.

- Such remote access passwords are by far the most common vulnerability and most attractive target for hackers. The PCI DSS requires two-factor authentication for any remote access to payment applications.
- POS implementations install a remote access tool, even though there is already one present. Many investigations of merchants that have been hacked reveal that two or more different remote tools were installed and active on the merchant's system at the time of the compromise.

- Remote access should only be activated when needed and should be deactivated after maintenance and support work has been completed.
- Third parties should not control remote access. Merchant management and their employees should be present to monitor vendor updates and ensure that access is enabled and disabled correctly.

Stored PCI Data

Payment applications may be storing cardholder data and full track data without the merchant's knowledge.

- Most hackers want to access full payment card track data. Certain functions within a payment application allow for the storage of data on an "as needed" basis, such as troubleshooting or testing application updates. These functions are often used during installation to validate whether the application is working. However, if these remain active, track data can be stored from that point on without the merchant knowing it, thereby providing hackers with the prized data that they seek.
- Merchants should ensure that integrators deactivate all data storage functions within the payment application. If the merchant chooses to store primary account numbers (PANs), the merchant must ensure that the payment application is encrypting this data.

No Firewalls

Payment applications should not be installed without firewall protection.

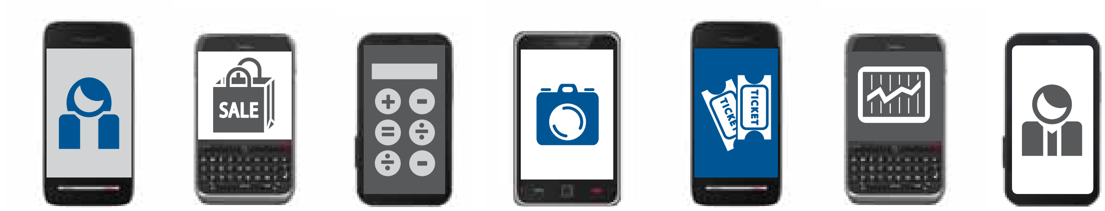
- Data can be exposed if POS terminals and payment applications are installed on the merchant's network where the firewall does not provide the intended adequate level of protection. This vulnerability exposes the merchant's system and possibly customer data directly to the Internet.
- Merchants should validate with integrators that their payment application is not exposed directly to the Internet and is protected by a firewall.

Weak Wireless Networks

A payment application that is installed using an insecure wireless access point is highly vulnerable to attacks.

- Merchant data breaches are often due to poorly configured wireless access points that do not enable basic security controls that other newer wireless routers provide. Hackers sometimes sit in parking lots or nearby retail outlets and scan for weak wireless networks to access.

- Merchants should ensure that vendors do not remove security settings on wireless networks or install an insecure wireless access point to support payment application functions. ■



Security Considerations for Mobile Point-of-Sale Acceptance

Smartphones and tablets are providing users with an ever-expanding set of capabilities including: music, videos, gaming, photography, global positioning systems, social networking, Internet browsing, and instant messaging. But what does this mean for security?

For many users, these devices have become their primary vehicle for interconnectedness and entertainment. According to some estimates, global sales of smartphones could rise to 982 million by 2015.

Not surprisingly, mobile devices are widely expected to have a significant impact on the electronic payment industry on both the issuing and acquiring sides of the business. Some issuers have already provisioned card credentials to mobile phone wallets, which ultimately may prove to replace the traditional payment card form factor.

For merchants, Mobile Point-of-Sale (MPOS) acceptance solutions represent a new opportunity for accepting card payments. MPOS solutions are being adopted by small businesses that have operated on a cash- and invoice-only basis and have never accepted payment cards. The use of MPOS solutions may very well become prevalent at yard sales, flea markets, and in other mobile door-to-door sales situations. Additionally, due to the sophisticated nature of smartphone applications, there are broader possibilities for enhancing the traditional payment experience that makes MPOS attractive to small retailers and even large retail chains. Also, there is a tremendous opportunity for expanding acceptance in undeveloped markets where traditional landline and Internet connectivity has posed a challenge for payment card penetration.

When it comes to security, the mobile phone architecture is still in an evolving state. Issuers are making use of the Secure Element within the device for the secure provisioning and storage of cardholder credentials. The Secure Element is typically a stand-alone, tamper-resistant hardware component that provides a high degree of confidentiality and data integrity.

For merchants and MPOS solution providers, the security of the mobile device is critically important, especially in light of the card brand requirements for *Payment Card Industry Data Security Standard* (PCI DSS) compliance as well as various local/regional laws and regulations that hold merchants accountable for the security of cardholder data. However, the challenge is that the typical mobile device was built with consumer ease-of-use in mind, and not necessarily business-grade data security. For example, smartphones and tablets have completely open architectures that allow users to download various applications on an on-demand basis. Mobile devices also provide for unmitigated connectivity. Most devices upon power-up immediately establish multiple connections via General Packet Radio Service (GPRS), Wi-Fi, and Bluetooth. Plus, mobile devices actively log and record keystrokes to instantly recall previous user entries on the keypad. While these features provide a pleasant consumer user experience, they also provide some serious challenges from a data security perspective.

Given all of these challenges, many merchants and their acquirers are wondering how they can comply with the PCI DSS and use payment applications that comply with the *Payment Application Data Security Standard* (PA-DSS). Traditional compliance with these standards is especially challenging, since merchants do not have the ability to change mobile device configurations and provide additional levels of security.

To compensate for these challenges, many MPOS solution providers are making use of point-to-point encryption, whereby transaction data is encrypted within the MPOS accessory device that is plugged into the mobile device via the audio jack, universal serial bus (USB) connector, or other multi-pin connector format. The entire set of transaction data is then transmitted enciphered via the mobile device to the MPOS solution provider's backend systems. As a result, for merchants that use this type of solution, the risk of data compromise via the mobile device is greatly minimized.

The use of point-to-point encryption in electronic payments is a relatively new concept, and in October 2011, the PCI Security Standards Council (SSC) issued a new standard for building point-to-point encryption solutions. With this new standard, MPOS solution providers have an industry-recognized and consistent framework to utilize.

The challenge is that the typical mobile device was built with consumer ease-of-use in mind, and not necessarily business-grade data security.

Yet point-to-point encryption does not solve all of the security challenges presented by mobile devices. For example, the keypad on mobile phones is not capable of complying with the PCI PIN Transaction Security (PTS) standard and as a result, cardholder PINs must never be entered onto the merchant's mobile device. Key-entered primary account numbers (PANs) also remain a challenge, due to the insecure nature of the keypad itself and the susceptibility of mobile devices to key logging. The eventual use of mobile devices as contactless readers will also present future challenges.

Even though these challenges currently exist, there are a new generation of technologies and advancements on the horizon which promise to greatly improve mobile phone security. As these capabilities become available, MasterCard will be there to guide the industry to continually preserve and enhance payment system integrity across the ecosystem. ■

Increasing the Odds Against Online Gambling Fraud

Online gambling has become a widely accepted and enjoyed form of entertainment around the world, with online poker leading in popularity over casino games and bingo. In fact, by 2014, online gambling worldwide is projected to be worth a staggering USD 40 billion.[1] This trend presents an enormous opportunity for online gambling merchants to expand their markets. But varying rules and regulations by country and non-standardized identity verification tools make this space especially vulnerable to cyber crime and fraud.

Technology used in Internet gambling has become more sophisticated, and fraudsters have kept pace. From card and identity theft to misrepresentation, online gambling merchants have had to adapt the way that they manage their businesses, their customer identification procedures, and the fraud prevention tools they employ. One of the most effective ways that merchants can fight fraud is to institute a series of best practices that will help protect their customers and businesses, and ensure a secure gambling experience.

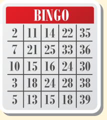
[1] PokerPages.com, *Online Gambling Industry Grows by 12 Percent in 2011*

UNDERSTANDING THE RISKS

In exploring fraud prevention in this space, this article looks at three business types—multiplayer poker, casinos, and bingo. One merchant could provide one or all of these on a gambling site.

Multiplayer Poker (e.g., Texas Holdem, Omaha) is the highest fraud risk for a merchant. Money is transferred over an open network with players from many different gambling sites playing against each other. Merchants cannot always see where the money is coming from. Fraud here can involve two players opening multiple accounts and "chip dumping"—one player using a stolen payment card and purposely losing the money to the other player who cashes out.

Casino Games (e.g., slots, roulette, blackjack) hold a high risk of fraud and involve a single participant playing against the house. In this case, a fraudster can use a stolen payment card to deposit money in the casino account then cash out via a different payment method (e.g., electronic wallet).



Bingo presents the least amount of risk. It is played either against the house or other players on a website and involves small purchases.

DISTINCT CHALLENGES FACING GAMBLING MERCHANTS

Gambling online moves just as quickly as playing inside a casino. Online gambling merchants have a very short time to determine whether a transaction is genuine or fraudulent. If cyber criminals discover a gap in security, fraud can manifest in a very short period of time. Risk rules can be deployed, but within hours fraudsters will change their behaviors. Real-time crediting of casino accounts means that rule sets need to be regularly adjusted to meet the ever-changing fraud trends.

Further challenging to online gambling merchants is that they are highly reliant on previous transactional history in determining whether a customer or transaction is legitimate.

By not identifying fraudulent accounts in time, merchants face tremendous negative impacts on revenue, expenses, operational effectiveness, and their online brand reputation. An online gambling provider suffering from high rates of fraudulent activities will find it difficult to earn new business with both customers and advertisers. To prevent such negative impacts, gambling merchants have had to invest in a wide range of fraud detection tools and increase their manual review processes.

The growing popularity of mobile gambling platforms also presents a challenge, particularly with respect to customer identification. In the mobile space, the Internet Protocol (IP) address sent by the merchant for risk-screening does not reveal the true location of the customer. This is a limitation of the mobile casino software. In addition to this challenge, no presence of a device ID creates further constraints by hampering the ability to determine whether multiple accounts have been created using the same mobile device. With the total sum wagered on mobile casino games expected to surpass USD 48 billion by 2015[2], keeping this platform secure will become more complicated and critical.

BEST PRACTICES FOR REDUCING GAMBLING FRAUD

When considering the changing trends in the online gambling industry, it's apparent that performing various types of analyses (such as chargebacks, demographics, payment methods, risk rules, etc.) can be helpful in combating fraud and protecting revenue. DataCash (a MasterCard company) has established—and continues to improve upon—a number of rules, processes, and best practices to support merchants in this industry. Often these are used in tandem, layering authentication and screening tools to manage Card-Not-Present (CNP) fraud.

The following suggested best practices are stopgaps that online gambling merchants can leverage to help reduce and prevent fraud.

Authentication and Verification

- **Ensure consistent customer details**—making sure that information such as name, phone number, and e-mail address match across accounts. If merchants are unsure about a player, they can request a DataCash review to check that customer globally against the client-merchant database.

- **Match card and account holder names**—ensuring that the name on the card and the casino account holder name are the same. If not, the merchant can cancel the transaction and deny additional purchases.

- **Match IP and BIN**—comparing the IP (country) and the bank identification number (BIN) for each transaction and reviewing flagged mismatches. Certain mismatches may be acceptable, but there is a high likelihood that the transaction is fraudulent when such a mismatch occurs on new accounts.

- **Compare currency and country**—checking that the currency being played with is from the originating country of the transaction and reviewing any flagged mismatches.

- **Check telephone number country code against BIN country**—validating mobile customers for whom there is no device ID.

[2] Juniper Research, *Mobile Gambling Wagers to Surpass $48 Billion by 2015*, September 2010

- **Know your customer (KYC)**—requesting a customer to complete an information verification document. These types of documents must be returned within a certain timeframe or the account will be closed and the player will not be able to cash out.

Payment Type

- **Follow source-to-source payment rules**—paying money during cash out first to the original payment method. Only after the initial expense is covered can the balance be paid to a different source. This reduces a fraudster's profit if a stolen card is used for the upfront purchase. Payment disputes and customer "denial" cases are also reduced.

- **Review global negative cards list**—checking the list for "hot" (lost/stolen) card numbers as provided by multiple processors. Transactions involving these cards should be denied.

- **Check for 1:1 payment methods**—accepting payment methods such as PayPal™ and Check and Buy where the player can hold only one gambling account.

Payment Behavior

- **Leverage the Central Negative Database (CND)**—using the DataCash database that contains player details uploaded upon merchant request and based on criteria such as excessive chargebacks, gambling problems, and known fraudsters. Adhering to the e-Commerce and Online Gambling Regulation and Assurance (eCogra) association's rules for fair and responsible gambling, this system is valuable in protecting customers with gambling issues—once entered into the database, they are blocked from gambling for six months. Regardless of whether the customer or merchant identifies the issue, it is the merchant's responsibility to notify the CND.

- **Block excessive chargebacks**—adding customers to the CND to be blocked because of excessive chargebacks. The customer can also be blocked globally across all MasterCard merchants.

- **Ensure consistent player behavior**—requesting that MasterCard review customers across multiple operators, as well as evaluating existing customers to ensure that purchases match behavior from the last few days or months. New customers are checked for other casino accounts, and behavior consistency with those accounts is reviewed. Alerts are generated if spending suddenly increases or if multiple purchases are made in a short timeframe using different payment methods.

- **Set spend limits**—putting spending limits on customers, and flagging purchases if the limit is exceeded.

- **Conduct manual checks by fraud specialists**—enlisting fraud specialists to flag cases based on risk alerts, customer tip-offs, and unusual gambling and wagering behavior. These alerts are typically pre-defined rules based on business knowledge and past experiences. Manual checks are especially important in open network, multiplayer poker to determine whether one player is winning or losing unusual amounts of money, to monitor a chat facility to determine whether cards are being exposed, or to review hands for abnormal play.

Velocity Checks

- **Counter-Based Constant Velocity**—determines whether an account, consumer, product line, or card has been used more times than the threshold allows within a specific timeframe.

- **Value Based Velocity**—establishes whether the total purchases of a consumer exceed the specified threshold over a specified time period.

- **Counter-Based Change Detection Velocity**—detects and evaluates changes and frequency of changes to data fields, such as card names or billing address, against an account.

Recognizing that fraud tactics are continually changing, DataCash is developing more tools to better analyze customer website behavior and detect compromised cards and payment methods more rapidly. For example, a plug-in can be provided that alerts analysts to illicit activity in real-time, trapping funds before they are fraudulently lost. Additionally, a Rules Management Interface is being developed to simplify and automate the risk rule creation and simulation process. This offering allows rules administrators and merchant experts to create and simulate the impact of rules in real-time, rating transaction risk and taking positive action.

DataCash is also investigating tools that will intelligently identify anomalies in transactional behavior. By applying machine learning and predictive modeling to detect fraud, we can allow for significant pre-analysis. In this way, we can greatly reduce the investigative effort on the part of the risk analysis team and provide them with the tools to perform the advanced analysis that is currently so time consuming.

CONCLUSION

Due to improved best practices and rules, online gambling fraud rates have not increased, even as the industry grows. Through continued use of best practices, online merchants can reduce their risk of fraud, remain profitable, and ensure that customers enjoy a safe and entertaining online gambling experience. ■

NEW AND NOTEWORTHY GLOBAL SECURITY BULLETINS

TITLE	APPLIES TO	EFFECTIVE DATE	BULLETIN DATE
Revised Standards to Support the U.S. Region Point-of-Interaction Roadmap	Issuers, Acquirers, Processors	Multiple effective dates (See bulletin)	Global Security Bulletin No. 4 – 13 April 2012
	Summary: MasterCard announced revised Standards to support the MasterCard U.S. Region Point-of-Interaction (POI) Roadmap, including: - U.S. region issuer and acquirer requirements for chip and PIN support; - U.S. region chip and chip/PIN liability shifts for domestic MasterCard® and Maestro® Point-of-Sale (POS) transactions; - The inclusion of the U.S. region in the Global Chip Liability Shift Program for interregional MasterCard and Maestro POS transactions; and - U.S. region-specific enhancements to the Account Data Compromise (ADC) program Operational Reimbursement (OR) and Fraud Recovery (FR) calculations and the *Payment Card Industry Data Security Standard* (PCI DSS) compliance validation requirements for Level 1 and Level 2 merchants.		
Revised Standards for the Maestro Chip Liability Shift	Issuers, Acquirers, Processors	19 April 2013 (31 December 2015 in Australia and New Zealand)	Global Operations Bulletin No. 9 – 1 September 2011
	Summary: MasterCard announced the participation of the U.S. and Asia/Pacific (A/P) regions in the Global Chip Liability Shift Program for interregional Maestro ATM transactions.		
Enhancements to the MasterCard PCI DSS Risk-based Approach and Revised Standards	Acquirers and Processors	15 September 2011	Global Security Bulletin No. 9 – 15 September 2011
	Summary: MasterCard revised its Site Data Protection (SDP) Program Standards to enhance the MasterCard PCI DSS Risk-based Approach framework in recognition of the counterfeit fraud prevention potential of EMV chip transactions.		
New Account Data Compromise Event Management Best Practices Guide Now Available on MasterCard OnLine	Issuers, Acquirers, Processors	Guide published 28 October 2011	Global Security Bulletin No. 12 – 15 December 2011
	Summary: MasterCard announced the availability of the new *Account Data Compromise Event Management Best Practices Guide* to assist its customers in addressing payment card account data security issues.		

TITLE	APPLIES TO	EFFECTIVE DATE	BULLETIN DATE
Revised Standards for Chip CVC Data	Issuers, Acquirers, Processors	12 October 2012 in Brazil 18 October 2013 elsewhere	Global Security Bulletin No. 11 – 15 November 2011
	Summary: MasterCard will revise its Standards to require all MasterCard, Maestro, and Cirrus chip card issuers to use different values for Card Validation Code 1 (CVC 1) and Chip CVC for all new and reissued cards. This requirement will include issuers using the Chip-to-Magnetic Stripe Conversion Service, as well as magnetic stripe grade issuers that do not use the Chip-to-Magnetic Stripe Conversion Service.		
Expert Monitoring Real-time Fraud Scoring Service for Merchants	Acquirers and Processors	1 April 2012	Global Security Bulletin No. 9 – 15 September 2011
	Summary: MasterCard introduced the Expert Monitoring Real-time Fraud Scoring Service for Merchants to acquirers for all Card-Not-Present (CNP) transactions originating from a card issued in the U.S. region.		
Offline Card Authentication for Chip Transactions	Issuers	15 December 2011	Global Security Bulletin No. 12 – 15 December 2011
	Summary: MasterCard explained the vulnerabilities associated with offline Static Data Authentication (SDA) of EMV chip cards and recommended that issuers migrate to the more secure dynamic Card Authentication Methods (CAMs).		
New Additions to the Business Risk Assessment and Mitigation Program	Acquirers and Processors	15 February 2012	Global Security Bulletin No. 2 – 15 February 2012
	Summary: MasterCard raised awareness regarding certain products identified as illegal or brand-damaging under the Business Risk Assessment and Mitigation (BRAM) compliance program.		
MasterCard SDP Program PCI PA-DSS Compliance Requirements—Reminder	Acquirers and Processors	1 July 2012	Global Security Bulletin No. 2 – 15 February 2012
	Summary: MasterCard reminded acquirers that all of their merchants and Service Providers that use third party-provided payment applications must only use those applications that are compliant with the *PCI Payment Application Data Security Standard (PA-DSS)*, as applicable. In addition, MasterCard clarified the PA-DSS compliance validation requirements for Level 1, Level 2, and Level 3 merchants and Level 1 and Level 2 Service Providers.		

CONTACT INFORMATION

For information on MasterCard Payment System Integrity (PSI) solutions, programs, or services, please contact the appropriate leader of the Customer Security & Risk Services regional team:

Asia/Pacific
Barry_Wong@mastercard.com

Canada
Rick_Rennie@mastercard.com

Europe
Richard_Smith@mastercard.com

South Asia/Middle East/Africa
Ian_Potgieter@mastercard.com

United States
John_Brady@mastercard.com

General Inquiries
PSI@mastercard.com

Latin America & the Caribbean
Guillermo_Maniaux@mastercard.com
(GeoNorth: Mexico and Central America)

Jack_Sinnott@mastercard.com
(GeoCentral: Colombia, Ecuador, Venezuela, and the Caribbean)

Luis_Camera@mastercard.com
(GeoSouth: Brazil and Southern South America)

Peter_Goldenberg@mastercard.com
(Fraud Management Program)

USEFUL URLs

www.mastercardworldwide.com
MasterCard continues to build on its history of innovation to develop and deliver new security initiatives that strengthen fraud prevention.

www.mastercard.com/arm
The Academy of Risk Management provides best-in-class knowledge and expertise to customers to help improve their risk management capabilities as a value-driver for their business.

www.mastercard.com/sdp
The MasterCard Site Data Protection (SDP) program is designed to help acquirers, merchants, and service providers achieve compliance with the *Payment Card Industry Data Security Standard* (PCI DSS).

www.mastercard.com/pci360
The MasterCard PCI 360 Education program is a complimentary initiative offered by MasterCard to raise awareness and promote the adoption of PCI.

FUTURE ARTICLE SUGGESTIONS

If you would like to see a particular topic included in next year's *Security Matters* magazine, please send your suggestions to datasecurity@mastercard.com.

MasterCard Fraud Management Solutions

Payment System Integrity

Expert Monitoring Solutions™

- Higher detection rates in real time
- Custom modeling
- Event management

For more information, e-mail us at risksolutions@mastercard.com.

MasterCard
Worldwide