Account Data Compromise Event Management Best Practices

26 February 2019

Summary of Changes, 26 February 2019

This section reflects the most recent changes made in this document since 29 September 2015.

The contents of this document are not Standards, as such term is defined in the Definitions portion of the *Mastercard Rules*. In the event of a discrepancy between information set forth in this document and the Standards, the Standards shall in all respects exclusively govern and the conflicting information set forth herein shall be of no effect. Mastercard disclaims any and all warranties of any kind and disclaims any and all liability of any nature relating to or arising in connection with the use of or reliance on any information set forth herein. Any person that uses or otherwise relies in any manner on any information set forth herein does so at his or her sole risk.

Description of Change	**Where to Look**
Old Mastercard logo replaced with the new one.	Throughout
MasterCard replaced with Mastercard.	Throughout
Updated the following section: • Introduction	Introduction
Removed the following section: • Acquirer Responsibilities in Connection with an ADC Event or Potential ADC Event	
Updated the following section: • Reporting an ADC Event or Potential ADC Event	Reporting an ADC Event or Potential ADC Event
Updated the following section: • ADC Incident Response	ADC Incident Response
Updated the following section: • ADC Incident Response Reporting Guidelines	ADC Incident Response Reporting Guidelines
Updated the following section: • ADC Incident Response for Small Businesses	ADC Incident Response for Small Businesses
Updated the following section: • Threat Indicators	Threat Indicators

Description of Change	Where to Look
Updated the following section: • Common Attack Vectors	Common Attack Vectors
Removed the following section: • Social Engineering	Common Attack Vectors
Updated the following section: • Entity Containment Best Practices	Entity Containment Best Practices
Section title from Event Prevention changed to: • Event Mitigation	Event Mitigation
Updated the following section: • Issuer Guidelines	Issuer Guidelines
Updated the following section: • Issuer ADC Event Management Framework	Issuer ADC Event Management Framework
Updated the following section: • Issuer Risk Mitigation	Issuer Risk Mitigation
Removed the following section: • Cardholder Notification Considerations for Entities Impacted by an ADC Event	
Updated the following section: • Education and Awareness	Education and Awareness
Removed the following chapter: • Appendices	

Contents

Chapter 1 Proactive Reporting Guidelines

This section provides acquiring financial institutions with their responsibilities connected to the identification of an Account Data Compromise (ADC) event or potential ADC event.

Purpose of This Document

The *Account Data Compromise Event Management Best Practices Guide* was created to assist customers and other stakeholders in implementing both proactive and reactive response strategies to address payment card data compromise events.

NOTE: This guide is intended for use by Mastercard acquiring and issuing customers to enable them to manage and mitigate actual and potential risk associated with Account Data Compromise (ADC) Events. Mastercard disclaims all responsibility and liability with respect to the information contained herein and any such information is used at the sole risk of the user.

Section 10.2 of the *Security Rules and Procedures* guide defines an ADC Event as an occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Mastercard account data. That section defines a Potential ADC Event as an occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of Mastercard account data.

Mastercard Standards pertaining particularly to ADC Events and Potential ADC Events are in section 10.2 of the *Security Rules and Procedures*. For more information pertaining to ADCs, see the Mastercard *Account Data Compromise User Guide*.

Introduction

The number of ADC events varies from year to year, but it only takes a single event to impact a large number of card accounts and negatively affect an organization's security posture.

It is critical that acquirers and issuers do everything they can to prevent these events from happening and to minimize their impact if they do occur by both proactively working with their customers, cardholders, and vendors. To act quickly if an event does occur.

In the event of an ADC event or potential ADC event, the customer, the breached or potentially breached entity (typically a merchant or processor), and third parties that support the customer's activities need to be able to act quickly and effectively. As stated in section 10.2 of the *Security Rules and Procedures*, "A customer must notify Mastercard immediately when the customer becomes aware of an ADC Event or Potential ADC Event in or affecting any system or environment of the customer or its Agent."

Further, having a pre-established Incident Response Plan (IRP) is critical to prevent further data loss and provide support for management. An IRP is required by the Payment Card Industry Data Security Standard (PCI DSS). A comprehensive IRP plan will enable decisive action and continued operation in response to an ADC Event. The IRP should be distributed throughout the management structure in order to ensure full awareness in the event of a compromise.

Reporting an ADC Event or Potential ADC Event

A customer must report an ADC Event or Potential ADC Event by using the ADC Reporting Form (ARF) located within the Manage My Fraud and Risk Programs application on Mastercard Connect™.

For more information regarding the reporting of Events through this product, refer to the Mastercard *Account Data Compromise User Guide* located under the Library within the Publications product of Mastercard Connect.

If a customer does not have access to or requires immediate response regarding an ADC Event or Potential ADC Event, all inquiries may be sent to the account_data_compromise@mastercard.com inbox.

When an ADC Event or Potential ADC Event is identified, it is very important to secure and safeguard all potential evidence in the physical and virtual environment. A forensic investigation is compromised if changes are made to the affected systems. Further information regarding the preservation and containment of potential evidence can be found in section 2.5 of this document.

When reporting an ADC Event or Potential ADC Event to Mastercard, responses to the following questions prove useful in assisting the Account Data Compromise team to investigate:

- What was the first known date of compromise?
- Did the event involve multiple locations?
- Can the window of exposure, or at-risk time frame in which legitimate accounts used at the entity which led to subsequent fraud be determined?
- What was the initial attack vector?
- If systemic in nature, can it be confirmed that data was being harvested and exfiltrated from the environment?
- Were significant security vulnerabilities identified?
- If a physical compromise has occurred, how was the data captured during the event?
- Is a PCI Forensic Investigator (PFI) engaged? If so, provide the PFI company and contact for the investigation.
- Has external counsel been engaged? If so, who?
- Is a security firm engaged (non-PFI) to perform services? If so, which company and when were they engaged?
- Have any remedial actions been taken to contain the event?

Chapter 2 Account Data Compromise Incident Response

This section describes the process in which customers should prepare in response to an ADC Event to help mitigate and remediate as quickly as possible.

ADC Incident Response

An ADC event can have significant impacts on a business of any size. The implementation of an account data compromise incident response plan can aid in reacting quickly to prevent further fraud losses, potential liability and customer backlash.

An effective incident response starts with the establishment of an Incident Response Team (IRT)—a cross-functional core team of experienced personnel. This team should have the decision-making authority to act quickly without hindering containment, preservation, and recovery efforts. Based on the size of an organization, a member of the IRT may be responsible for more than one function on the team or may be an outsourced individual who performs services for the organization. Special consideration should be given to ensure that the appropriate team members have prearranged relationships with a security vendor, one or more PFIs, a payment card brand contact, and an appropriate law enforcement representative to support a rapid investigation response. Below is a listing of the key stakeholders that should be considered for inclusion on an IRT:

- Executive Sponsorship
- Team Leader
- Information Security
- Customer Support
- Communications
- Audit
- Risk Management/Security
- Legal
- Compliance
- Finance
- Human Resources
- Investor Relations (if applicable)
- Regulators

The way an organization responds to an ADC Event is vital to minimize the impact of a data compromise. The *Payment Card Industry Data Security Standards* (PCI DSS) requires entities that store, process, transmit, or impact the security posture of transmit cardholder data to have an ADC event response process in place. Refer to PCI DSS Requirement 12 for more information.

At a high level, an incident response plan should address the following:

- Preparation
- Detection and Analysis
- Containment/Eradication/Recovery
- Post-Incident Activity

Maintaining such a plan is critical to helping prevent further data loss and providing support for management of the event.

Preparation

A financial institution should establish an incident response capability so that it is ready to respond by ensuring that systems, networks, and applications are sufficiently secure. In the preparation stage, employees within your organization who are responsible for handling incidents should be identified. For example, organizations need contact information, escalation procedures (including executive management), secure storage facilities to secure evidence, software/hardware used for forensic acquisition/analysis, and access to clean images for recovery/purposes. Regular exercises should be carried out to test readiness of the plan and demonstrate its effectiveness or vulnerabilities.

Detection/Analysis

Financial institutions should be prepared to handle any breach incident and should focus particularly on being prepared to handle incidents that use common attack vectors. Different types of incidents merit different response strategies. In order to determine malicious activity on financial institutions' network, first the environment must be understand (such as differentiating between normal versus abnormal behavior). Enable logging on financial institutions' systems. Ensure all steps taken during an event are documented. Specialized technical knowledge and experience are necessary for proper and efficient analysis of incident-related data.

Containment/Eradication/Recovery

Containment is important before an incident can overwhelm resources or increase damages. An essential part of containment is decision-making. To fully contain an incident, an organization must first understand the attack vectors or cause of compromise. If this information is unknown, there is a high possibility that the compromise will happen again. While it is important to remove the components of the incident impacting the affected systems such as malware, it is imperative to preserve evidence using industry best practices.

Post-Incident Activity

Intelligence derived from the investigation should be applied to improve the security posture of the organization. In addition, the process can be improved as needed.

ADC Incident Response Reporting Guidelines

Once an ADC event or potential ADC event has been identified, the IRT must convene quickly and perform a risk assessment to determine whether an event occurred and the nature and scope of the event.

IRPs should include the following items:

- Reporting any event or potential event to Mastercard promptly (within 24 hours) and in accordance with the *Account Data Compromise User Guide* requirements
- In determining the severity of an ADC event, there are a number of elements and risk factors associated with a specific ADC event to consider:

  - The number of accounts at-risk
  - The type of data that was compromised (for example, Track 1, Track 2, Full Magnetic Stripe, card validation code 1 [CVC 1], CVC 2, primary account numbers [PANs], expiry dates, PINs, chip information and cardholder name), tokens, and Track Equivalent data
  - If applicable, the type of Personally Identifiable Information (PII) data elements that may have been exposed (for example, cardholder name, address, Social Security Number [SSN], e-mail address, birth date and maiden name)
  - The method by which the merchant or entity has expressed the nature, scope, or scale of the compromise publicly to its cardholders or the media
  - If applicable, the merchant PCI level and whether the merchant or entity and their service providers were *Payment Card Industry Data Security Standard* (PCI DSS) compliant
  - The critical systems that were impacted or compromised during the event

Acquirers may support Mastercard ADC investigations by facilitating communications with the affected party (for example, merchant, Service Provider, agent, or a third party contracted to the merchant). This support may involve:

- Working with the impacted party throughout all phases of the event
- Providing clear communication regarding the entity's obligations under *Mastercard Rules* to promptly cooperate, and if necessary, the consequences for failure to comply
- Centralizing communications to an incident lead within the acquirer's internal data security compliance team and with the compromised entity
- For compromising events involving PCI Level 1 or Level 2 merchants, engaging an internal merchant relationship manager or account management staff to expedite communication and investigation requirements
- Establishing clear communications with compromised entities via regular status update conference calls and written documentation for initial investigation information, any ongoing forensic investigation findings, and any possible compliance assessments and validation
- Ensuring that the entity promptly engages a PFI to investigate the ADC event or potential ADC event within the Mastercard required timeframes as set forth in Chapter 10 of the *Security Rules and Procedures* manual and the *Account Data Compromise User Guide* if required, or voluntarily chosen
- Ensuring that Mastercard requests for account data fulfilled according to the Mastercard requirements as set forth in the *Account Data Compromise User Guide*
- Building capacity to recover older or archived Mastercard payment account data sets at an acquirer ICA or merchant ID level (if it is not available from the affected merchant or processor)
- Assisting the impacted party to engage proper law enforcement agencies to report the breach
- Remediating the compromise and providing an unedited forensic report to Mastercard according to Mastercard requirements

- Ensuring that the affected entity becomes and maintains *Payment Card Industry Data Security Standard* (PCI DSS) compliance following the event according to Mastercard requirements
- Determining ongoing PCI DSS compliance training for any compromised entity

NOTE: If a financial institution is both an acquirer and issuer, it should advise its card issuing management group regarding the details of the ADC event.

ADC Incident Response for Small Businesses

Level 4 merchants can minimize the impact of security threats through the creation of a basic incident response plan.

While the plan may be less complex than those for larger volume merchants, the plan, at a minimum, should contain the following guidelines:

- Specify contacts who should be notified in the event of an account data compromise
- Explanation of employee functions and basic mode of business operation
- During an ADC event, necessary procedures necessary procedures for appropriate, timely notification to the acquiring bank(s)
- A list of readily available resources that can be found on the Internet (such as State data compromise requirements for notifying customers, data compromise response guides and plan toolkits)

By developing a thorough incident response plan, a small business can effectively respond to an ADC event, safeguard their customer data and position their business for a safer and thriving environment.

Chapter 3 Anatomy of an Account Data Compromise Event

This section explains those characteristics that are commonly observed during a suspected or confirmed ADC Event.

Threat Indicators

Acquirers and merchants should become familiar with potential threat indicators that an ADC Event has occurred or is occurring, and report these occurrences as soon as possible to Mastercard in accordance with Chapter 10 of the *Security Rules and Procedures* manual and the *Account Data Compromise User Guide*.

Examples of Account Data Compromise threat indicators may include the following:

- Unauthorized systems accessed or unauthorized privileges obtained
- Alerts and alarms that tripped an Intrusion Detection System (IDS), Intrusion Prevention System (IPS), firewall rules, system logs alerts, or an anti-virus solution
- The identification of unknown users or commands found in IDS logs
- The presence of suspicious files on network systems (encrypted files, files **hidden** in directories where they should not belong, such as Windows 32, deleted files, and so on)
- Multiple remote access tools present on the systems which are in an **always on** mode
- Authentication that includes single factor (user ID and password) allowing brute force attempts or lack of complex passwords
- Machines in the cardholder data environment having unrestricted access to the Internet
- Inconsistent activity logged on audit trails
- The identification of a packet sniffer, key logger, memory scraper, or other suspicious program that is capturing or has captured payment card account data
- Repetitive, unsuccessful logon attempts in a short timeframe
- Web logs showing numerous attempts at performing Structured Query Language (SQL) injections against a database
- Unapproved or unknown user accounts
- Denial of Service (DoS) attacks or disruptions to Web-based services
- System crashes due to unidentified causes
- Unusual or off-hour login activity or login activity that does not coincide with a user’s history
- Unexplained additions or modifications to files that include new or modified file names, changes to system files or attempts to modify, or the deletion of data
- The presence of unidentified and possibly encrypted compressed files, such as .zip, .rar, .7z containing payment card data
- Network connections (inbound or outbound) to Internet Protocol (IP) addresses for which it is not normal for the merchant or processor to be connected
- Unidentified applications that appear to launch automatically when the system reboots
- E-mail or file transmissions (inbound or outbound) that are not normal business traffic
- A notification from issuers or cardholders related to cardholder complaints and chargebacks
- Attempts to exploit known vulnerabilities to commonly used platforms

Common Attack Vectors

Acquiring financial institutions and the merchants, service providers, or agents they work with need to understand that data security compromises can occur in many different ways and can involve more than one attack methodology.

However, there are generally four key common characteristics that are found in most ADC events:

- Access to the payment processing environment
- Ability to access payment card data
- Ability to exfiltrate data out of the network
- Access to source code or code that supports the payment mechanisms, that is, Javascript)

Detecting the path or method in which malicious activity can enter a system can be challenging, but a goal of entities that process store, transmit, or impact the security of payment card data should strive to minimize the risk to the payment card data they encounter. This is accomplished by implementing such security layers as P2PE (Point to Point Encryption), EMV chip card terminals, or tokenizing the data. It is critical that acquiring customers educate their clients on threats that may expose payment card data to risk of unauthorized use occurring from, but not limited to:

Electronic

Breach (an unauthorized network intrusion by an externally or internally sourced person[s]). Breach attack methods can be highly varied, including:

- Exploitation of insecure third party remote access software
- Downloading of malicious software tools (malware)
- Lack of 2FA (2 Factor Authentication)/MFA (Multifactor Authentication) can lead to:
  - Password cracking as a result of weak or default passwords through various methods, including brute-force attacks
  - Keylogger malware in which keystrokes and screen shots are captured to an encrypted log file that can contain sensitive data including PINs, passwords, credit card information, social security numbers, and so on
- Password cracking as a result of weak or default passwords through various methods, including brute-force attacks:
- Manipulation of shared network access
- Insecure wireless networks and the use of wireless encryption protocols that are vulnerable to known exploits
- The exploit of known vulnerabilities in software coding such as Structured Query Language (SQL) injection attacks and Cross Site Scripting (XSS)

Physical

Theft of, or tampering with physical equipment containing payment account data such as cardholder receipts, files, personal computers, PIN entry devices and POS terminals.

Skimming

The compromise of PIN, magnetic stripe, and/or EMV data at an ATM using a skimming device combined with a PIN pad overlay or camera to capture the PIN. The subsequent data can be utilized for creation of both credit and debit cards.

Entity Containment Best Practices

Upon suspicion of compromise, entities must act quickly to mitigate further exposure of sensitive data by performing an investigation of their network and immediately notifying Mastercard within 24 hours of the potential data compromise event. Also, contacting the appropriate internal incident response team can aid in the mitigation efforts. Equally important is the entities diligence to maintain evidence.

NOTE: For more details, see the *Mastercard Rules* guide.

Actions of containment performed by a PFI should include the following:

- Image all impacted systems to ensure preservation of evidence
- Disconnect compromised systems from the Internet
- Ensure any malware artifacts or log data is preserved in accordance with industry standards
- Refrain from taking any actions that could eliminate or destroy information that could potentially provide evidence of an ADC Event or Potential ADC Event
- Document all incident response actions
- Configure the entity’s firewall to block suspicious IPs from ingress and egress traffic
- Continue to monitor all traffic on systems within the payment processing environment
- Alert all associated financial entities along with an internal incident response team
- Patch all software identified as being vulnerable to attack

Event Mitigation

In addition to understanding the various ways that criminals can illegally access payment account data, acquiring financial institutions also need to understand how to address potential physical and network vulnerabilities and support their merchants’ efforts to mitigate these risks.

Changes to application, network, and data environments are inevitable as users change accounts, applications are added, and systems become upgraded.

In order to proactively mitigate such risks, key areas of focus may include the following:

- The use of Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), anti-virus solutions, and regular review of audit logs (firewall, security event, anti-virus, IDSs, and IPSs)
- An established process on how to respond to and manage events in which equipment (computers, laptops, computer tapes, files, or archives, and so on) containing or having access to payment account data that may have been stolen or is missing equipment that may expose payment account data to compromise
- Internal procedures to report unauthorized or suspicious network activity
- Awareness that system crashes and repeated cardholder concerns regarding fraudulent transactions on payment cards could indicate possible intrusion attempts
- Proper due diligence involving system administrative access controls, authentication, and data storage after system enhancements or new system releases are implemented
- An established process on how to work together with Mastercard and law enforcement authorities to address possible events that may have exposed payment account data to compromise
- The sharing of information concerning known vulnerabilities in software and hardware products that support POS terminals and PIN entry devices (PEDs) that may affect merchants or others beyond the compromised entity
- Help ensure that merchants and processors comply with *Payment Application Data Security Standard* (PA-DSS) rules mandating the retirement of obsolete or outdated POS equipment
- Routine testing of network security vulnerabilities (penetration testing) by a Qualified Security Assessor (QSA)
- Help ensure that the PIN-capable terminals (POS and ATM) are *PCI PIN Transaction Security* (PTS) compliant
- The implementation of anti-skimming strategies at ATMs such as, but not limited to, equipment that detects and alerts the acquirer in the event that attempts are made to install skimming devices or the installation of electronic countermeasures to render the illegal skimming devices ineffective (for example, electromagnetic scramblers or other technologies).
- Help ensure that the *Payment Application Data Security Standard* (PA-DSS) devices are installed by a QIR to ensure PCI compliance and the highest level of security.
- Detailed logging to assist with rebuilding the path(s) of an unauthorized intruder(s)
- Timely patching and a program to monitor and help ensure that the systems are patched in accordance with the risk level associated with the patch provided.
- Establish a risk assessment program for all engaged third parties to understand what data elements are shared with these entities and how they secure the same data

Further prevention techniques can be implemented based upon the type of environment being monitored:

Electronic

Protecting against the compromise of system or network environments that process payment card data

- Firewalls should be properly configured to restrict inbound and outbound traffic to only trusted and business necessary locations
- The payment processing environment should be segmented from public networks such as the Internet to reduce the number of systems in the PCI DSS scope
- Avoid use of systems connected to the payment processing environment for browsing the Internet, as the Internet is considered an untrusted network
- Avoid the use of default usernames or passwords, ensuring passwords are properly complex
- Regularly update or patch hardware devices, operating systems, anti-virus software, and payment processing applications
- Use multi-factor authentication for any remote connections
- Limit all remote access for Third-Party vendors on a needed basis

Social Engineering

Protecting against Social Engineering

- Review company policies regarding the posting of internal information on public social media sites
- Educate employees and test phishing awareness on potential misuse of information by hackers to send targeted malware and malicious URLs via email communications
- Ensure email gateways contain multiple antivirus engines for broadest range of virus definitions (that is, antivirus engine at the email gateway and alternative engine for the endpoint systems)
- Set up checks for third party vendors to ensure changes are validated

Physical

Monitor and track ownership of physical technology

- Monitor employees utilizing POS terminals with a clear understanding of their infrastructural restrictions
- Review self-service checkout lanes and monitor for unusual purchase activity
- Install cameras and record footage near check-out lanes where POS terminals are present
- Track ownership of physical assets (that is, credit card receipts, hardcopies of documentation containing sensitive data)
- Define procedures to maintain logs of visitors and recorded footage to areas containing sensitive data
- Physically lock down devices
- Assign asset tags to desktops/laptops/cell phones/wireless devices and POS devices that stores, transmits, or processes cardholder data
- Physically lock down equipment and ensure servers/data centers are locked in separate rooms only accessible to proper personnel
- Lock sensitive documentation in file cabinets or lock boxes
- Enable remote wipe capabilities for cell phones/wireless devices to protect against loss or theft

Skimming

Monitor and check POS equipment and employees

- Regularly inspect POS equipment for skimming devices or evidence of tampering
- Monitor employees who manually process credit cards away from the cardholder
- Understand vulnerabilities associated with POS terminals and PIN-pad devices used by contacting POS reseller/vendor.

Third-Party Vendors

Also, it is important to be aware and gather as much information as possible about a third party vendors. Many compromised entities are not even aware that a particular third party vendor provided remote support and are surprised to hear that this entity was the weak link that resulted in the attack. It is important to ask questions and look at the security policies and practices of third party vendors. Understanding a third party vendor's method of remote connectivity, whether or not they utilize multi-factor authentication, or have connections that are always enabled are factors that can determine the risk level of an Account Data Compromise event.

Chapter 4 Issuer Guidelines

This section explains guidelines for issuers notifying customers and reporting ADC events.

Issuer ADC Event Management Framework

An enterprise-wide ADC management approach needs to involve key security, operations, customer service, legal, communications, as well as product level management teams.

If the financial institution has both an issuing and acquiring presence, it is important to set up a similar enterprise-wide approach for cross-bank notifications. Similar to other entities impacted by an actual or potential ADC event, issuers also need to establish an operational plan to manage an incident where payment card data may be at risk.

An issuer ADC event operational plan should:

- Manage the account distributions from Mastercard and other payment brands
- Determine cross-departmental product impacts and capabilities of each of the issuer's functional units concerning these accounts
- Leverage internal ADC event competencies within an issuer's organization regardless of product ownership
- Ensure proper allocations of internal resources
- Manage internal and external partnerships, because affected accounts could involve co-branded relationships with other institutions
- Sufficient EMV card plastic stock for potential large volume reissuance

Issuer Risk Mitigation

A key decision that an issuer faces in connection with an ADC event is whether to monitor or reissue affected accounts, or a combination of both.

An effective risk management framework can help guide the decision-making process by serving as a standardized approach for issuers to evaluate their initial and ongoing risks from an ADC event. The following paragraphs provide details regarding specific elements of a risk management framework to support issuers in determining whether they need to monitor or reissue accounts associated with an ADC event.

For in depth assistance and expertise, reach out to the local/regional fraud support teams. The following important factors must be taken into account when determining reissuance and monitoring strategies:

Type of Data Compromised

An issuer should understand the type of data at risk from a given ADC event to determine the level of severity and its risk tolerance. If more sensitive data (such as magnetic stripe information, CVC 2 data, or PINs) is compromised, an issuer may apply different monitoring and reissuance strategies as opposed to a PAN and expiry date compromise. Chip issuers may also apply different monitoring and reissuance strategies for ADC events in which the track data compromised is actually the chip equivalent track data and where the CVC 1 is different from the Chip CVC.

Account(s) Involved in One or More Compromises

An issuer should have a thorough screening process in place to determine whether accounts put at-risk of unauthorized use due to an ADC event were also put at-risk in a prior event. It is essential to review the dates of transactions or PANs with expiry dates in past ADC events in order to prioritize an approach and manage high risk accounts that need to be addressed.

Fraud Impact on ADC Accounts

Assessing the impact of fraud on at-risk accounts will enable an issuer to take appropriate actions to protect cardholders and mitigate losses. Key actions can include both maintaining a normal run rate and tracking specific ADC event fraud run rates.

Normalized Account Fraud Run Rates within Bank Identification Number (BIN) or Product Lines vs. Accounts Received in an ADC Event

An issuer should maintain a normal fraud run rate on each account or product/BIN range within their portfolio. An issuer's internal database should maintain good versus bad spend levels for both domestic and cross-border geographic spending and fraud patterns, and be able to differentiate accounts with elevated levels of fraud risk. In addition, accounts impacted by ADC events and not reissued must be flagged in the issuer's system for ongoing monitoring to determine whether risk levels are escalated and additional decision-making methodology is necessary.

Percentage of Accounts in the ADC Event Impacted by Fraud

Not all accounts exposed in an ADC event will incur fraud. It is critical that an issuer track the specific ADC event fraud run rates on accounts. For each event, issuers should calculate the percentage of accounts exposed in a given event that had fraud activity for benchmarking and analysis to understand the actual ADC event risk to their cardholders.

Establishing Fraud Loss Ratios

An issuer should identify fraud loss rates on accounts affected by an ADC event because each issuer's loss rates will vary based on portfolio size and risk tolerance. Issuers should establish account fraud ratios based on the actual percentage of accounts exposed in an ADC event and also apply fraud value ratios to these events based on total fraud dollar amounts on the accounts. The issuer can track the number of accounts exposed in each event as well as the total fraud loss for each account.

Each issuer's risk tolerance levels will vary based on its portfolio size and fraud loss ratios. An issue's risk management framework should apply a score based on core aspects of the case concerning the data at-risk as well as the fraud run rates on affected accounts. Once an issuer has categorized the event's severity levels, it can follow predetermined escalation and response protocols.

Issuer Risk Mitigation Guidelines

Following are examples of escalation levels and action steps that an issuer may consider once it has carefully examined an ADC event's core aspects and fraud impacts and determined its own severity level for a specific event.

The reporting of fraud on compromised accounts using the proper fraud status codes in the Mastercard System to Avoid Fraud Effectively (SAFE) database within proper timeframes are critical to the investigation and remediation of account data compromise events. Also, errors in fraud reporting can affect an issuer's ability to receive fraud recovery relating to a given ADC event.

Severity Level 1—Extreme

- Block cards after prompt cardholder contact or immediately before reaching out to cardholders
- Ensure that all account details and relevant ADC event information are loaded into an issuer's card system
- Prioritize cardholder communications based on a portfolio segmentation approach (such as VIP high credit lines, commercial, debit, standard) and begin contacting cardholders
- Advise call center representatives of ADC messaging, establish cardholder scripting for inbound and outbound calls (when applicable), and develop cardholder letters and statement inserts along with website messaging
- Establish authorization strategies for each impacted account based on cardblocking procedures

Severity Level 2—High

- Based on prior ADC events, determine the time it takes for full reissuance of each compromised account (that is, plastics inventory, vendor management, total cost, and other aspects involved in reissuance)
- Prior to establishing a reissue strategy, segment cardholder portfolio levels
- Segment impacted accounts flagged for reissuance based on expiration date in sequential order (cards scheduled to expire in 30, 60, 90 days)
- Monitor account activity until the new account is activated by the cardholder
- Establish reissue cycles (90-, 60-, 30-, 15-, 10-day reissue cycles), record the expiration date of each account, and determine whether reissuing is necessary
- Establish account closure cycles based on cardholders not activating new accounts (that is, soft blocks or hard declines)
- Ensure that new accounts are blocked until activated by cardholders
- During reissue periods, determine whether credit lines should be adjusted for both active and new accounts until activation occurs
- Consider posting ADC event response messaging on the issuer's website
- Distribute letters to cardholders and statement inserts or proactively call cardholders

  - Attempt additional outbound calls, and if no contact is made by cardholders, then set a predetermined timeframe and block the account
- Ensure that authorization systems are aligned with call centers that have the ability to authorize and decline accounts

Severity Level 3—Moderate

- Distribute letters to customers or contact them proactively
- Attempt additional active outbound calls, and if no cardholder contact is made, then:
  - Set a predetermined timeframe to block the account
  - Ensure that authorization systems are aligned with call center call strategies.

Severity Level 4—Low

- Continue to analyze and monitor account fraud levels daily and weekly, review old and new Mastercard alerts, fraud rates, potential ADC events, and regional and global fraud trending based on the potential ADC event's location
- Maintain a database on fraud dollar amount losses for each account (that is, flag each account with higher fraud losses for reissuance)
- Administer velocity checks on flagged accounts during monitoring and have analytics in place to specify transaction geography changes within 24/48/72-hour periods
- Review internal databases to identify active and inactive accounts to determine processing and monitoring strategies for inactive accounts, soft declines, call referrals, and cardholder notification
- Ensure that open BIN ranges not currently being used for issuing are in acquiring-only status to limit risk and exposure
- Maintain data storage capabilities to track high-risk card acceptor business codes (MCCs), merchant IDs, and potential ADC events
- Possess the ability to initiate real-time declines on transactions at the point of sale if a sudden run rate of fraud appears on a flagged account
- Determine general account fraud run rates on counts and amounts that will assist in determining whether account behavior is within normal parameters or indicating elevated levels of risk
- Continually track loss rates on open compromised accounts to determine whether a prioritization strategy should be modified at a BIN or ICA level
- Establish priority status levels using an alphanumeric scoring system with different actions warranted within the priority level

Building an Internal ADC Identification Process

Building a thorough process for detecting the common points of origination of a possible ADC event, commonly referred to in the industry as a Common Point of Purchase (CPP), is an important aspect of an issuer ADC event risk management protocol.

The establishment of this type of process can help identify potential ADC events based on fraud notifications by issuers. Reporting this information to Mastercard in a timely manner along with expedited reporting to SAFE, plays a critical part in assisting Mastercard fraud investigation personnel with ADC events. The following considerations can assist issuers in building an effective ADC identification process:

- Report potential Common Points of Purchase (CPPs) with at least 10 unique Mastercard accounts experiencing subsequent fraud through the ADC Reporting Form located within the Manage My Fraud and Risk Programs application on Mastercard Connect™
- Properly status and correctly report POS 90 swiped counterfeit accounts to Mastercard via the SAFE database reporting process
- Use transaction data mining tools to review transaction velocity on accounts
- Establish a potential vulnerability time period for accounts that were used at a suspected ADC origination point
- Determine the number of accounts used at a suspected ADC origination point that involved swiped counterfeit data and establish at-risk dates or date ranges
- Use test account patterns, even if the account did not incur fraud, to determine the actual ADC origination point
- Establish separate velocity monitoring and reporting for transactions (fraud probes/tests) for smaller dollar amounts and on non-reissued inactive accounts

Cardholder Notification Considerations for Issuers

At some point during or following an ADC event, an issuer may need to reissue cards and notify cardholders as to why they are receiving new ones.

When notifying cardholders, issuers may want to consider the following messaging recommendations:

- Include contact information and necessary steps for replacement card activation.
- Instruct cardholders on actions they need to take to avoid possible service interruptions when transitioning to their new replacement card. These instructions can include:
  - Informing authorized users that the account number is no longer valid
  - Notifying any recurring billing merchants associated with the prior account number
  - Updating automatic bill payment services with the new account number.
- Express regret for the inconvenience and remind cardholders of the issuer's commitment to fraud prevention and data security.

Issuers may also want to consider including notification information in multiple languages based on the geography or preferences of affected cardholders.

Chapter 5 Education and Awareness

This section provides education and awareness regarding ADC events.

Education and Awareness

Both issuing and acquiring financial institutions should dedicate resources to assist in the education and reinforcement of appropriate data security practices to their customers, including cardholders, merchants, Third-Party Agents, Service Providers.

For issuers, they should focus on cardholder education:

- Encourage cardholders to regularly review their payment account statements for accuracy
- Encourage cardholders to report suspected ADC events to the issuing bank
- Publish literature and provide educational information about current fraud trends, such as phishing and skimming
- Promote the use of online security tools, such as anti-virus, anti-spyware, and firewall software
- Provide easy to access information on what to do if customers believe they are the victim of an ADC or identity theft event
- Encourage the use of strong passwords for online banking

Acquirers also need to ensure that they are protecting the integrity of payment card account data, including:

- Educate value chain partners such as merchants, processors and POS vendors about what types of sensitive payment card data can and cannot be stored
- Establish an effective Payment Card Industry Data Security Standard (PCI DSS) program to drive merchant compliance.
- Share information through the publication of literature on known security vulnerabilities of software and payment devices that have led to past data compromises

Chapter 6 Conclusions

This section provides the conclusion and resources.

Conclusions

All stakeholders in the payment value chain need to be committed to the ongoing process of payment card data security. A key concept of data security protection is sustained vigilance and monitoring.

While achieving data security compliance is a necessary accomplishment, it is not the final step since any change to a system or lack of adherence to a specific data security policy can quickly shift an organization from compliant to non-compliant, thereby creating opportunities for criminals. Therefore, data security compliance efforts must be a continuous process of assessment and remediation to ensure the safety of cardholder data. By presenting the enclosed best practices and recommendations, Mastercard is encouraging its issuing and acquiring customers to apply these techniques to help mitigate the chances of an ADC event from occurring and effectively respond and communicate to key stakeholders if an incident does occur.

For More Information

For more information related to the Mastercard ADC process, see the resources listed below.

Resources

- *Security Rules and Procedures Manual*
- *Account Data Compromise User Guide*
- Mastercard Security and Fraud Management website
- Mastercard PCI 360 Education Program
- National Institutes of Standards & Technology (NIST)
- United States Computer Emergency Readiness Team (US-CERT)

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to Mastercard International Incorporated, one or more of its affiliated entities (collectively "Mastercard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of Mastercard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of Mastercard trademarks in the United States. Please consult with the Global Customer Service team or the Mastercard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any Mastercard manual, bulletin, release, or other Mastercard document into a language other than English is intended solely as a convenience to Mastercard customers. Mastercard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall Mastercard be liable for any damages resulting from reliance on any translated document. The English version of any Mastercard document will take precedence over any translated version in any legal proceeding.

Information Available Online

Mastercard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on Mastercard Connect™. Go to Publications Support for centralized information.