Account Data Compromise User Guide

5 October 2017

ADC

Summary of Changes, 5 October 2017

This document pertains to ADC Events in which the first ADC Alert is published on or after 1 January 2017. For ADC Events in which the first ADC Alert is published prior to 1 January 2017, the 04 February 2016, and the 15 January 2014 publications of this manual will apply and are available upon request. For a copy of the previous publications of this manual, email the Mastercard Account Data Compromise team at account_data_compromise@mastercard.com. To locate these changes online, click the hyperlinks in the following table.

Description of Change	Where to Look
Updated the following section: • Purpose of the Account Data Compromise User Guide	Purpose of the Account Data Compromise User Guide
All section 10.2 and 10.2.2 instances changed to: • Chapter 10	Throughout
Replaced Member ID with: • Customer ID	Throughout
Replaced MIM with: • Member Information Online	Throughout
Updated the following section: • ADC Reporting Form	ADC Reporting Form
Updated the following section: • Attachments—General Instructions	Attachments—General Instructions
Updated the following section: • ADC Event Reporting without the Use of Manage My Fraud and Risk Programs	ADC Event Reporting without the Use of Manage My Fraud and Risk Programs
Updated the following section: • Secure Upload	Secure Upload
Updated the following section: • ADC Investigation Process	ADC Investigation Process

Description of Change	Where to Look
Updated the following section: • Engaging a PCI Forensic Investigator	Engaging a PCI Forensic Investigator
Updated the following section: • Financial Responsibility	Financial Responsibility
Updated the following section: • Manage My Fraud and Risk Programs—View Mastercard ADC Alerts Application	Manage My Fraud and Risk Programs—View Mastercard ADC Alerts Application
Updated the following section: • Overview of the Use of Manage My Fraud and Risk Programs for an ADC Event or Potential ADC Event	Overview of the Use of Manage My Fraud and Risk Programs for an ADC Event or Potential ADC Event
Updated the following section: • Notification of Compromised Accounts Using Manage My Fraud and Risk Programs Application	Notification of Compromised Accounts Using Manage My Fraud and Risk Programs Application
Updated the following section: • View Mastercard Account Data Compromise (ADC) Alerts	View Mastercard Account Data Compromise (ADC) Alerts
Updated the following section: • Manage My Fraud and Risk Programs Quarterly Fees	Manage My Fraud and Risk Programs Quarterly Fees
Updated the following section: • Updating a Manage My Fraud and Risk Programs User Profile	Updating a Manage My Fraud and Risk Programs User Profile
Updated the following section: • Manage My Fraud and Risk Programs—Noncompliance Assessments	Manage My Fraud and Risk Programs—Noncompliance Assessments
Updated the following section: • Requesting a Manage My Fraud and Risk Programs Application License	Requesting a Manage My Fraud and Risk Programs Application License
Updated the following section title: • System to Avoid Fraud Effectively (SAFE)	System to Avoid Fraud Effectively (SAFE) Reporting

Description of Change	Where to Look
Updated the following section: • Overview of SAFE Reporting	Overview of SAFE Reporting
Updated the following section: • Known At-Risk Time Frame	Known At-Risk Time Frame
Updated the following section: • Unknown At-Risk Time Frame	Unknown At-Risk Time Frame
Updated the following section: • ADC Case Eligibility for OR/FR	ADC Case Eligibility for OR/FR
Updated the following section: • Estimate of Potential Financial Liability	Estimate of Potential Financial Liability
Updated the following section: • ADC Operational Reimbursement	ADC Operational Reimbursement
Updated the following section: • ADC Operational Reimbursement Factors	ADC Operational Reimbursement Factors
Updated the following section: • ADC Operational Reimbursement—BIN Reports	ADC Operational Reimbursement—BIN Reports
Updated the following section and title: • ADC Operational Reimbursement—Acquirers and Issuers	ADC Operational Reimbursement—Acquirers and Issuers
Updated the following section: • ADC Operational Reimbursement—Customer Responsibility Cap	ADC Operational Reimbursement—Customer Responsibility Cap
Updated the following section: • ADC Fraud Recovery	ADC Fraud Recovery
Updated the following section: • ADC Fraud Recovery—BIN Reports	ADC Fraud Recovery—BIN Reports
Updated the following section: • ADC Fraud Recovery—Notification	ADC Fraud Recovery—Notification

Description of Change	Where to Look
Updated the following section: • ADC Fraud Recovery—Acquirer Responsibility Cap	ADC Fraud Recovery—Acquirer Responsibility Cap
Updated the following section: • ADC Fraud Recovery Factors	ADC Fraud Recovery Factors
Updating section title from Fraud Recovery—Responsible Member Responsibility to: • Fraud Recovery	Fraud Recovery
Operational Reimbursement Billing Event Codes updated to: • Operational Reimbursement Billing Event Codes for Acquirers	Operational Reimbursement Billing Event Codes for Acquirers
Updated the following section: • Fraud Recovery Billing Event Codes for Acquirers	Fraud Recovery Billing Event Codes for Acquirers
Updated the following section: • Operational Reimbursement Notification	Operational Reimbursement Notification
Updated the following section: • Fraud Recovery—Reimbursement Notification	Fraud Recovery—Reimbursement Notification
Updated the following section: • Annual Fees	Annual Fees
Updated the following section: • Billing Events	Billing Events
Updated the following section • ADC Event Responsibility Estimate Letter	ADC Event Responsibility Estimate Letter
Updated the following section: • ADC Event Final Responsibility Letter	ADC Event Final Responsibility Letter
Updated the following section: • Issuer Credit Letter	Issuer Credit Letter

Description of Change	Where to Look
Updated the following section: • Applications of SAFE to an ADC Event	Applications of SAFE to an ADC Event
Updated the following section: • Applications of Mastercard Connect to an ADC Event	Applications of Mastercard Connect to an ADC Event
Updated the following section: • Applications of Manage My Fraud and Risk Programs to an ADC Event	Applications of Manage My Fraud and Risk Programs to an ADC Event
Added the following section: • Manage My Fraud and Risk Programs and ADC Reporting Form Field Definitions	Manage My Fraud and Risk Programs and ADC Reporting Form Field Definitions
Added the following section: • ADC Reporting Form (ARF)—Issuer View—Field Descriptions	ADC Reporting Form—Issuer View—Field Descriptions
Added the following section: • ADC Reporting Form (ARF)—Acquirer View—Field Descriptions	ADC Reporting Form—Acquirer View—Field Descriptions
Updated the section title Applications of the MIM to an ADC Event to: • Applications of the Member Information Online to an ADC Event	Applications of the Member Information Online to an ADC Event

Contents

Chapter 1 Introduction to Account Data Compromise (ADC) User Guide

This chapter explains the purpose of this user guide, describes the Account Data Compromise (ADC) Event time line, and provides contact information for various regional offices of the Mastercard Global Customer Service team.

Preface to the Account Data Compromise User Guide

In the event of a conflict between any of the information set forth in this *Account Data Compromise User Guide* and any of the Standards (as such term is defined in the definitions portion of the *Mastercard Rules* manual), the Standards shall be afforded precedence and the conflicting information set forth in this *Account Data Compromise User Guide* shall be deemed deleted and of no effect.

All pricing set forth herein is subject to change at the discretion of Mastercard.

Although this *Account Data Compromise User Guide* generally provides that Mastercard notifies a customer by email, Mastercard may use an alternative or additional means of notification.

Purpose of the Account Data Compromise User Guide

The Mastercard *Account Data Compromise User Guide* provides instructions for Mastercard customers and their merchants and agents, including customer service providers and data storage entities, regarding the administration of the Mastercard Account Data Compromise (ADC) program.

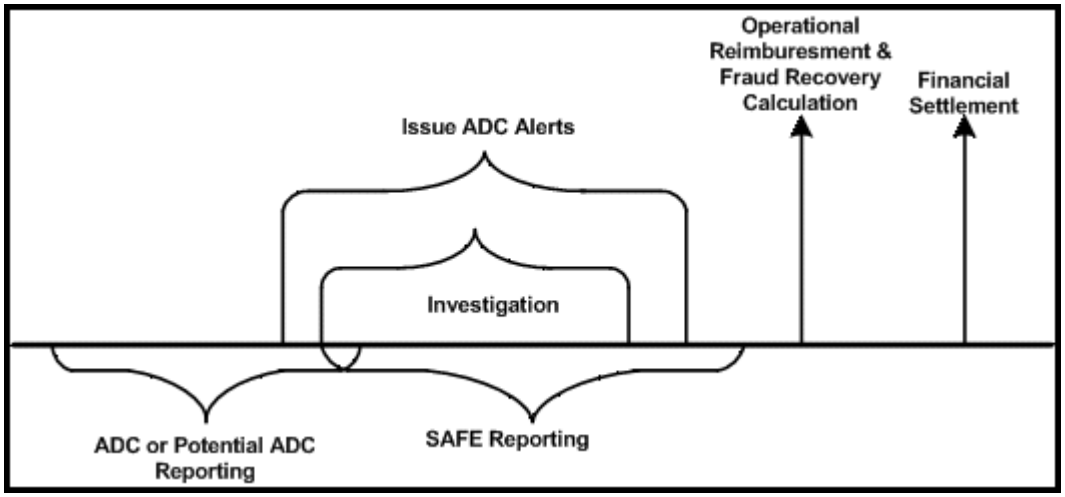
The Mastercard Standards relating to ADC Events or Potential ADC Events are set forth in Chapter 10, Account Data Compromise Events of the *Security Rules and Procedures* manual.

As defined in the Mastercard *Security Rules and Procedures* Chapter 10, Account Data Compromise Event or ADC Event means an occurrence that results, directly or indirectly, in the unauthorized access to or disclosure of Mastercard account data. A Potential Account Data Compromise Event or Potential ADC Event means an occurrence that could result, directly or indirectly, in the unauthorized access to or disclosure of Mastercard account data.

ADC Event Time Line

The ADC Event time line as follows depicts the life cycle of an ADC Event or Potential ADC Event. This guide depicts each of the steps associated with the administration of a typical ADC Event or Potential ADC Event.

Given the nature and complexity of an ADC Event and Potential ADC Event, it is important to note that this guide is not intended to set forth every ADC Event or Potential ADC Event. Mastercard retains the discretion to act (or not act) other than in accordance with this user guide.



Account Data Compromise User Guide Contact Information

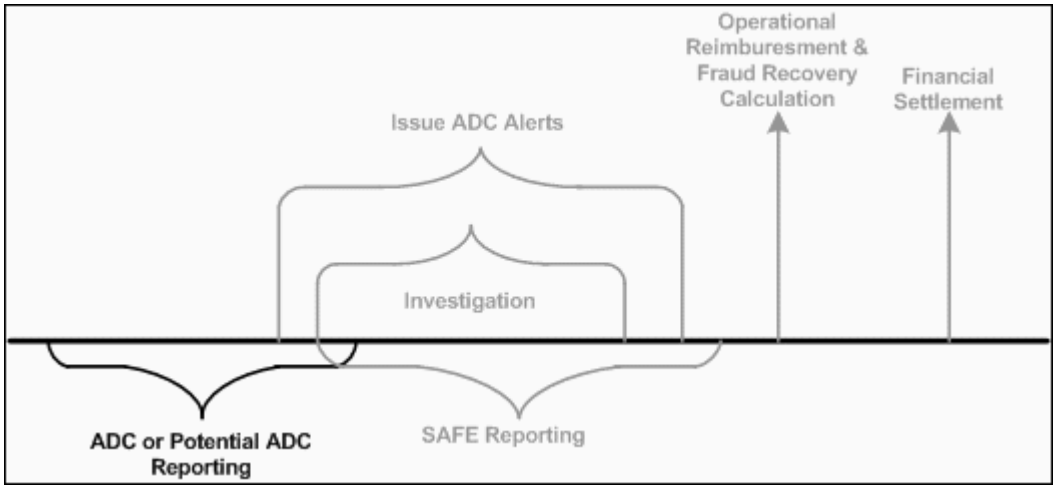
For contact information, refer to the Information Available Online section of the Notices page of this document.

Chapter 2 Reporting an ADC Event or Potential ADC Event

This chapter describes the process by which an acquirer or issuer must report an ADC Event or Potential ADC Event to Mastercard.

Overview of the Reporting of an ADC Event or Potential ADC Event

The following depicts where the reporting of an ADC Event or Potential ADC Event to Mastercard falls in the life cycle of an ADC Event.



A security vulnerability in a payment processing environment may not immediately be known; however, there may be indicators of a security breach, unauthorized activity, or possible signs of misuse within the payment environment that may indicate an ADC Event or Potential ADC Event. Indicators of an ADC Event may include, but are not limited to the following:

- Internet connections originating from non–business-related IP addresses[3]; inbound Internet connections originating from countries without a business relationship to the potentially compromised entity; outbound Internet connections to non–business-related IP addresses; countries, or both
- Log-in activity from unknown or inactive user IDs, or excessive or unusual login activity from user IDs
- Multiple instances of remote access tools present on systems in an "always on" mode
- Presence (in network systems or environments) of malware, suspicious files, or executables and programs, or presence of unusual activity or volume in same.
- SQL injection or other suspicious activity on Web-facing systems
- POS terminals and ATM devices showing signs of tampering
- Key-logger found
- Card-skimming devices found
- Lost, stolen, or misplaced sales receipt
- Lost, stolen, or misplaced payment card data

[3] An IP address that is not recognized by the entity in question as being an IP address that would need access to the entity's network.

- Lost, stolen, or misplaced computers, laptops, hard drives, or other devices that contain Mastercard payment card data
- Files containing Mastercard account data mistakenly transmitted to an unauthorized party
- Suspicious e-mail or File Transfer Protocol (FTP) activity occurring on network systems.

To comply with Chapter 10, Mastercard *Security Rules and Procedures*, the customer must contact Mastercard immediately when they become aware of a Potential ADC Event or an ADC Event.

ADC Event Reporting Using Manage My Fraud and Risk Programs

A customer must report an ADC Event or Potential ADC Event through the Manage My Fraud and Risk Programs application.

For information about the required customer roles, responsibilities, and associated time frames in response to an ADC Event or Potential ADC Event, refer to Chapter 10, Mastercard *Security Rules and Procedures*.

To report an ADC Event or Potential ADC Event to Mastercard, a customer must use the ADC Reporting Form (ARF) located within the Manage My Fraud and Risk Programs application on Mastercard Connect™. Events include, but are not limited to, the following:

- A customer (acquirer or issuer) or any of its agents becoming aware of an ADC Event or Potential ADC Event in or affecting any system or environment of the customer or its agents
- An issuer experiencing elevated fraud or otherwise suspecting an ADC Event or Potential ADC Event impacting their payment processing.
- A responsible customer must report an ADC Event immediately and no later than twenty four (24) hours of becoming aware of the Event or Potential Event, and on an ongoing basis thereafter to Mastercard all known and or suspected facts concerning the ADC Event or potential ADC Event.

To obtain access to the Manage My Fraud and Risk Programs application, refer to section Manage My Fraud and Risk Programs - View Mastercard ADC Alerts Application of this manual. To report an ADC Event without access to Manage My Fraud and Risk Programs, refer to section ADC Event Reporting without the Use of Manage My Fraud and Risk Programs below.

ADC Reporting Form

A customer must use the ARF within the Manage My Fraud and Risk Programs application to report and provide information about an ADC Event or Potential ADC Event. The use of this form is important as it provides a central location for all ADC Event or Potential ADC Events and is monitored daily by Mastercard.

A registered user may access the ADC Reporting Form by following these steps:

1. Go to www.mastercardconnect.com.
2. Log on using your **User ID** and **Password**.
3. From the top of the Mastercard Connect™ home page, click **My Apps**, and then click **ADC or FR MTF**.
4. Under **Manage My Fraud and Risk Programs**, click **Report a Potential Account Data Compromise (ADC)** at the left of the screen.
5. Read the Terms and Conditions, click **Accept** to accept the terms, and click **Save and Continue**.
6. The Customer ID will be automatically populated on the Welcome screen. Customers will see their institution name, along with provisioned selections for their Customer ID/ICA number and institution type from a drop-down box. Once selections are made, click **Save and Continue** to progress to the reporting form.

Customers will have access to their submitted forms via the Manage My Fraud and Risk Programs application, along with the ability to provide additional information at the request of Mastercard. For ADC Reporting Form field definitions, refer to Appendix E.

General Instructions

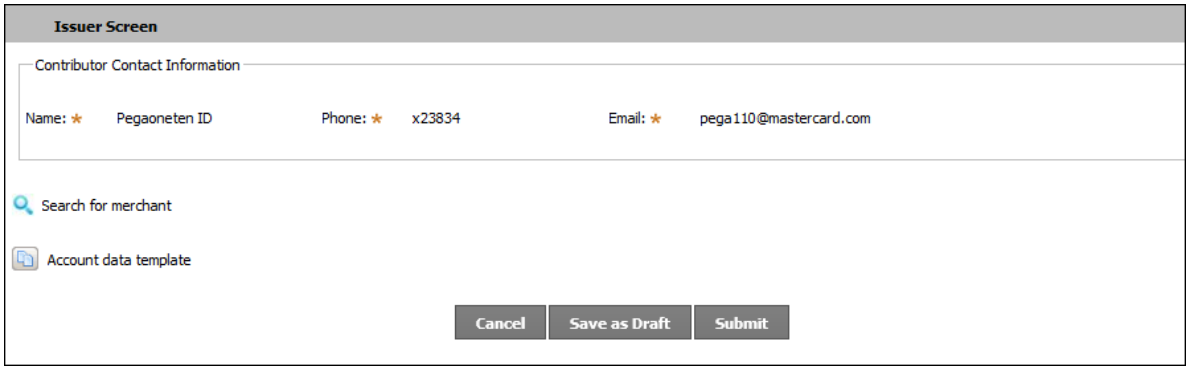
The user must complete all required fields in the ADC Reporting Form. All required fields marked with an asterisk must be completed to advance the *ADC Reporting Form*.

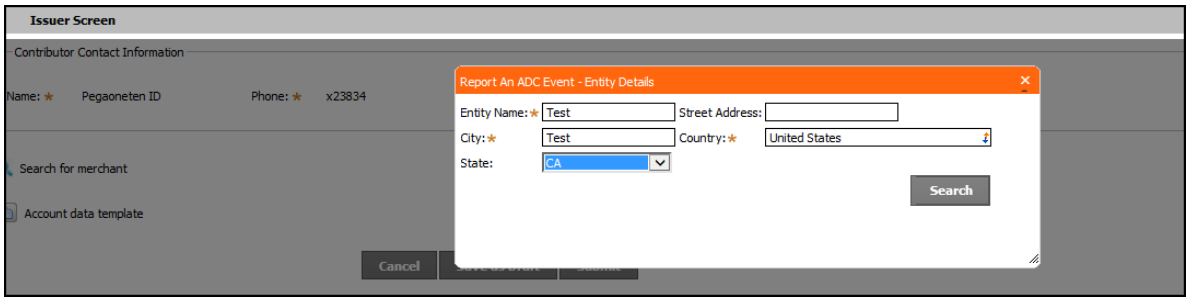
If the information is unknown, and not a required field, it may be left blank. If a required integer value is unknown, enter the number zero. If the required data element or date is unknown about the ADC Event being reported, select (none) or enter today's date by default. Required text fields that are unknown may be filled with N/A. Omitting fields may delay the investigation or the applicable next steps of the event.

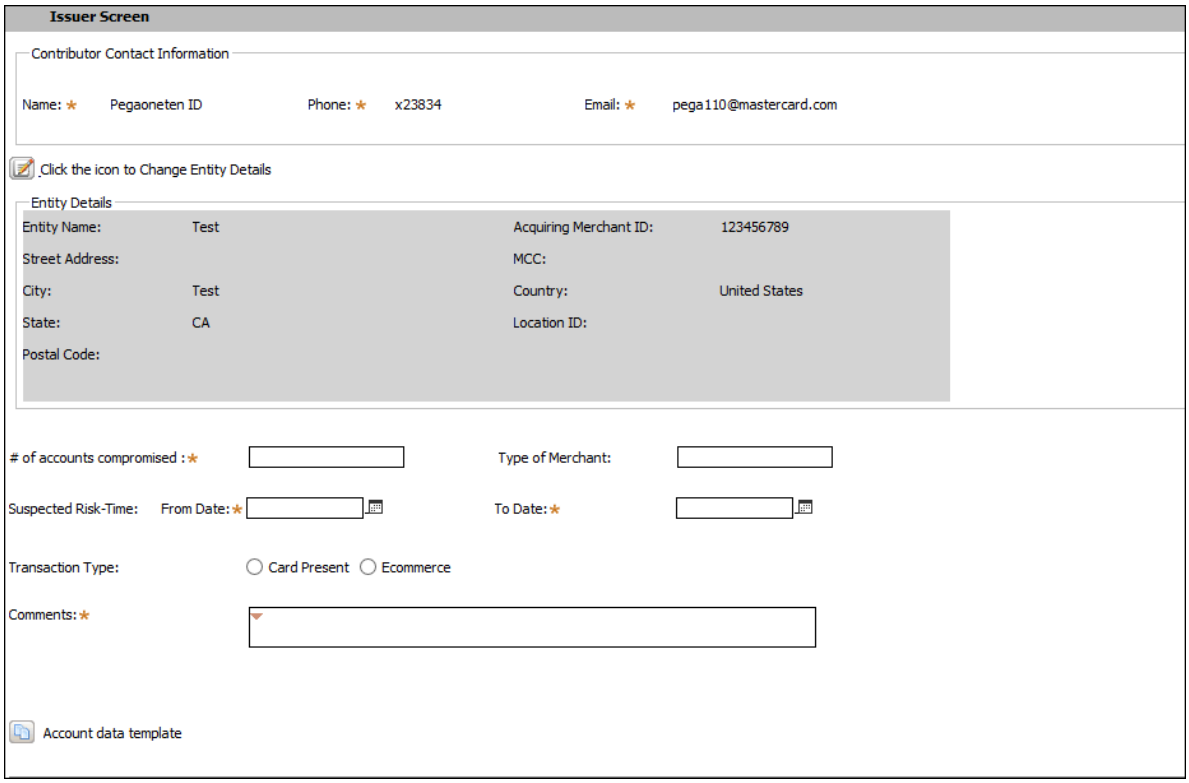
The following are illustrations of the ADC Reporting Form for both an Issuer and Acquirer view within the Manage My Fraud and Risk Programs application.

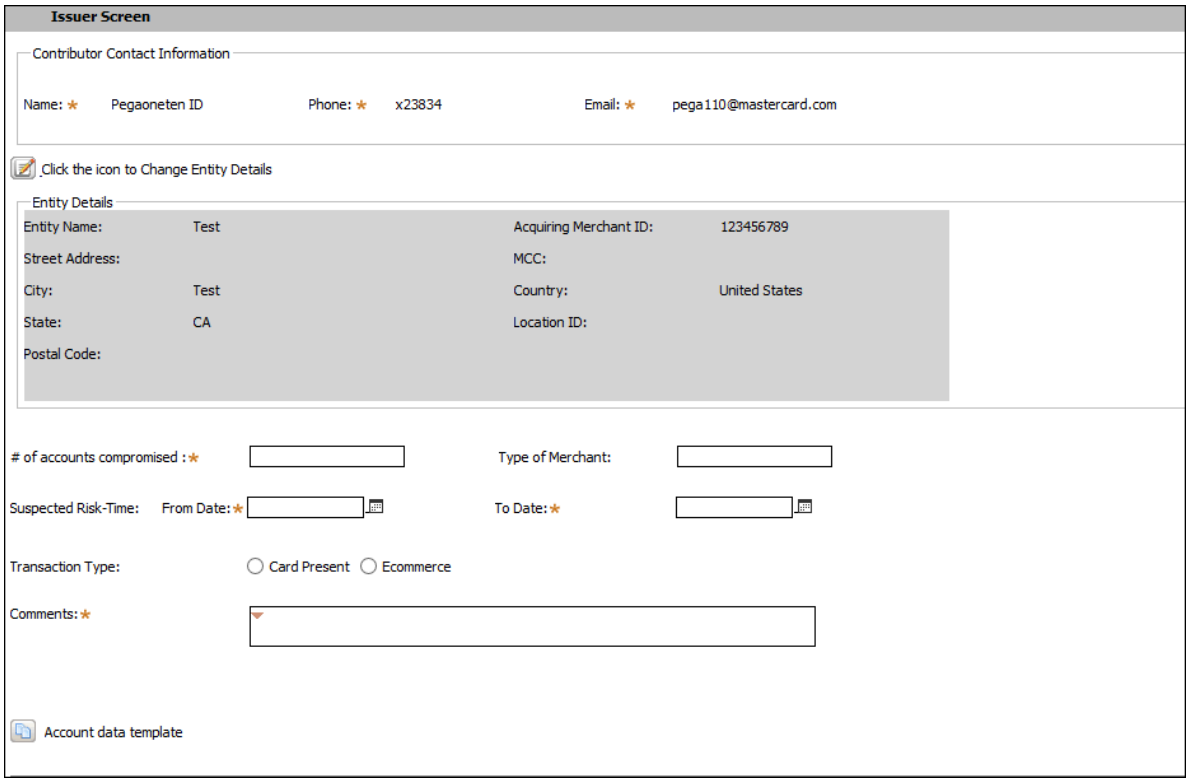
NOTE: Issuers are required to report actual fraudulent transactions to the System to Avoid Fraud Effectively (SAFE).

ADC Reporting Form





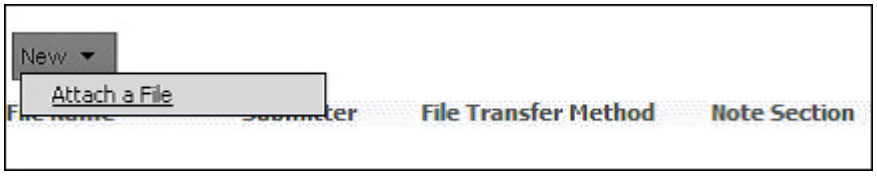




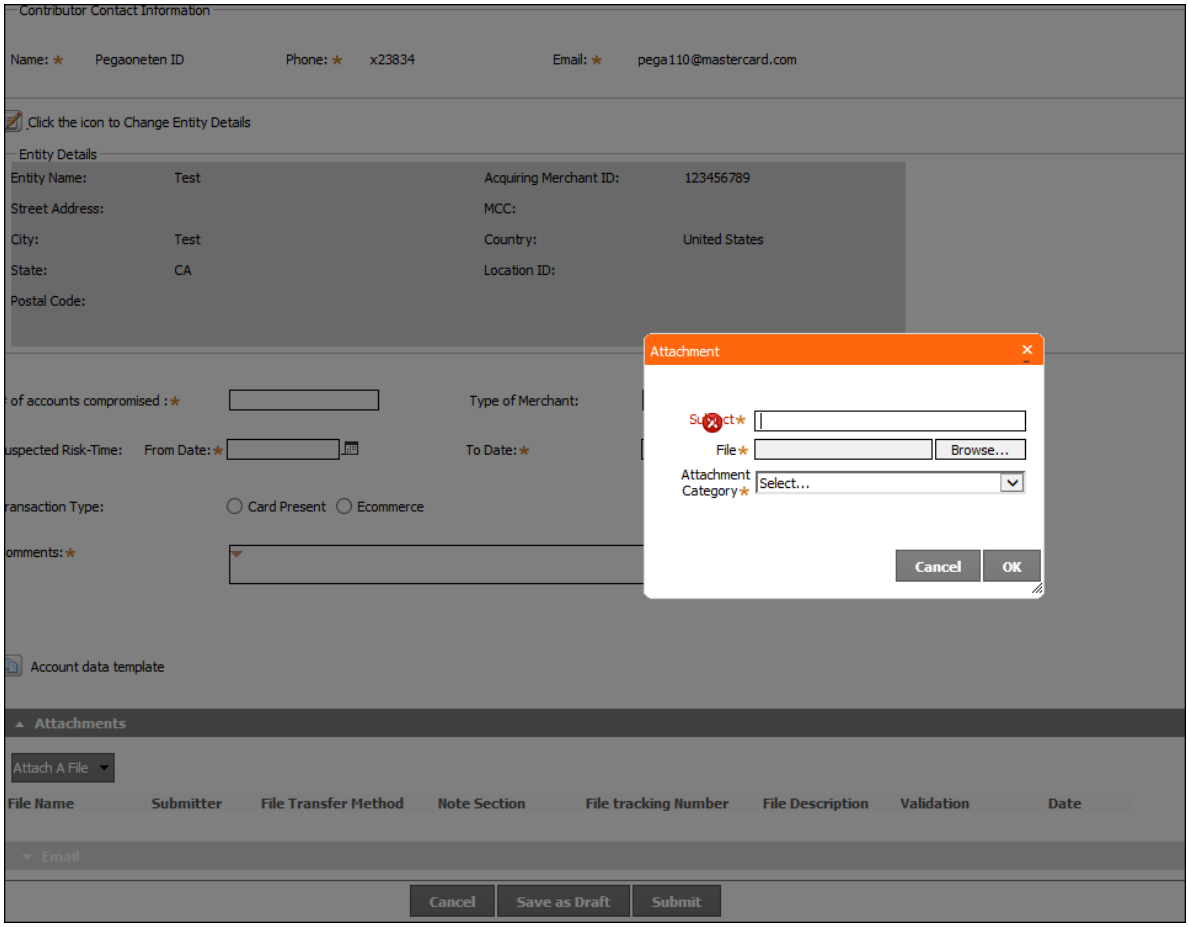
Attachments—General Instructions

The following is a representation of the Account Data Compromise Form Attachments Tab in both the issuer and acquirer view:

Click **Attach a File** below the Attachments section to attach documents to the *ADC Reporting Form*.



Customer View



Follow the instructions on the **Attachment** screen. Enter a valid subject line pertaining to the file that will be chosen directly from the computer after clicking **Browse**. Select a specific file attachment category type, and then click **OK**.

Repeat this process for additional files. Click **Submit** to upload the files. Once the files have been uploaded, a file tracking number and validation message will be displayed. The files are also available under **Attachments** in the specific *ADC Reporting Form* which is assigned an ARF number that appears in the **Active Projects and My Work** tabs of the Manage My Fraud and Risk Programs application.

When submitting account numbers to Mastercard, issuers will select the Attachment Category Compromised Acts while the term At Risk Accounts will be used by an acquirer. An issuer at a minimum must provide "10 unique accounts" that have had subsequent fraud or fraud attempts after use at the suspected compromised entity. If the at-risk account numbers are readily available by the acquirer when reporting a potential ADC event, create a file of all at-risk Mastercard or Maestro account numbers. This obligation applies regardless of how or why such account numbers were received, processed, or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature- or PIN-based)

proprietary, or any other kind of payment transaction, incentive, or reward program. The required BIN ranges start with **222100**-**272099**, **510000** to **559999**, and **670000** to **679999**.

If the at-risk account numbers are not readily available, they may be submitted at a later date using the *ADC Reporting Form* via the Manage My Fraud and Risk Programs application, Secure Upload product, or by using PGP encryption file. ARF forms with less than 10 valid accounts may be closed.

Customers will receive an email confirmation of submittal indicating a file was received for a specific case.

The *ADC Reporting Form* can be saved in draft form in the Manage My Fraud and Risk Programs application before it is electronically submitted to Mastercard.

The *ADC Reporting Form* entry must be submitted before Mastercard can process the report. This is done by clicking **Submit** at the bottom of the form. No information will be saved if **Cancel** is clicked.

ADC Event Reporting without the Use of Manage My Fraud and Risk Programs

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

If a customer does not have access to the Manage My Frauds and Risk Programs application, at-risk account data and the ADC Reporting form may be submitted to Mastercard using one of the following methods.

- Secure Upload
- PGP Encrypted File
- Mastercard OnMail

When at-risk account numbers are available, submit them in separate files, along with the Incident Report, to Mastercard, using Secure Upload.

Account data should never be sent without being encrypted before transmission. Each method of transport described in this guide offers a method of securely transferring account data.

All files containing compromised or potentially compromised account data must be submitted in the file format defined in this guide.

Secure Upload

The Secure Upload product allows for the secure file transfer of compromise information through a secure Mastercard website.

This feature expedites the receipt and delivery of at-risk account information. A brief description characterizing the provided data is required along with the account data.

NOTE: Secure Upload is used only for data and information pertaining to an ADC Event or Potential ADC Events.

Consider the following when uploading data using Secure Upload:

- The file size is limited to 50 megabytes (MB).
- Mastercard prefers text (*.txt) and Excel® (*.xlsx) file formats for at-risk accounts. Portable Document Format (*.pdf) is not acceptable for account files.
- Mastercard prefers text (*.txt), Excel (*.xlsx), PDF (*.pdf), or Word® (*.docx) documents for communications related to investigations.

Secure Upload is available through Mastercard Connect™ for Mastercard customers.

PGP Encrypted File

A customer that cannot submit files using Secure Upload must send files encrypted using PGP to help ensure that the account data is secure while in transit.

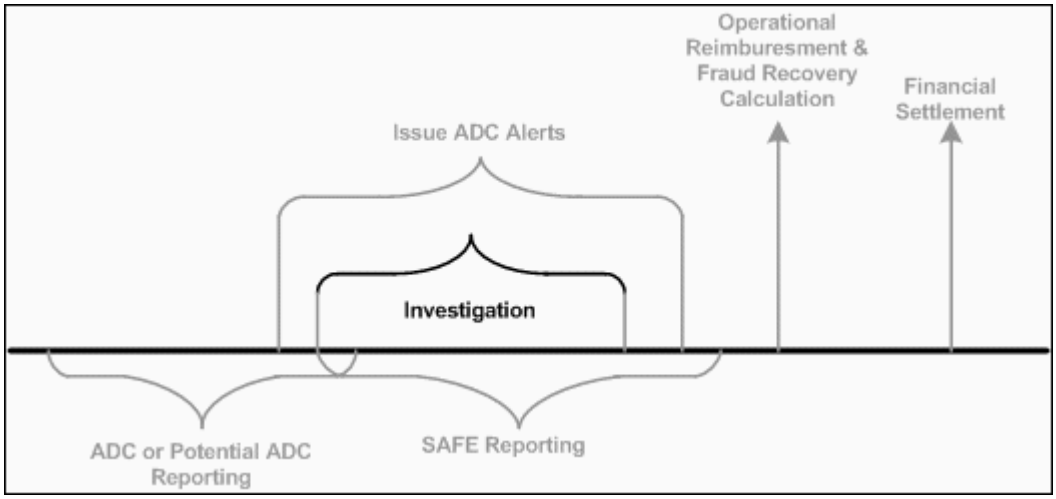
Send all encrypted files to account_data_compromise@mastercard.com.

Chapter 3 Investigation of an ADC Event or a Potential ADC Event

This chapter describes the processes pertaining to the investigation of an ADC Event or a Potential ADC Event.

Overview of the Investigation of an ADC Event or Potential ADC Event

The following graphic depicts where the investigation of an ADC Event or Potential ADC Event falls in the life cycle of an ADC Event.



Each responsible customer must comply with the obligations set forth in Chapter 10 in Mastercard *Security Rules and Procedures* manual. The responsible customer must satisfy these obligations to the satisfaction of Mastercard. Each ICA must have at least two users register for use of the application.

A customer must ensure that any non-customer entity authorized by the customer to access Manage My Fraud and Risk Programs on behalf of the customer is registered with Mastercard as a service provider of the customer and has access to the Manage My Fraud and Risk Programs application.

ADC Investigation Process

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 through Mastercard Connect™.

Once the ADC Reporting Form is submitted, the customer will note in their Active Projects tab that the event was submitted to Mastercard for review.

NOTE: Submission of an investigation request using the ADC Reporting Form does not mean that Mastercard has or will commence an investigation.

If Mastercard receives a report of a Potential ADC Event or an ADC Event, Mastercard may attempt to validate the information set forth in the report.

Mastercard may notify the Security Contact, Principal Contact, and/or the ADC Compliance and/or ADC Investigation Contact for the applicable ICA that a Potential ADC Event is pending additional investigation details in the Manage My Fraud and Risk Programs.

Engaging a PCI Forensic Investigator

The customer responsible for an ADC Event or Potential ADC Event may required to engage a PCI Forensic Investigator (PFI) if requested by Mastercard as outlined in Chapter 10, Mastercard *Security Rules and Procedures* manual.

Chapter 10 in Mastercard *Security Rules and Procedures* manual states, "Prior to the commencement of such PFI's investigation, the customer must notify Mastercard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by Mastercard or, if such preliminary approval is not obtained, of a modified proposal acceptable to Mastercard."

The documentation relating to the scope should be attached to the ADC Reporting Form in the Manage My Fraud and Risk Programs application for Mastercard review and approval.

Financial Responsibility

As a courtesy to a Responsible Customer, Mastercard may calculate possible preliminary ADC Recovery responsibility prior to the completion of the investigation.

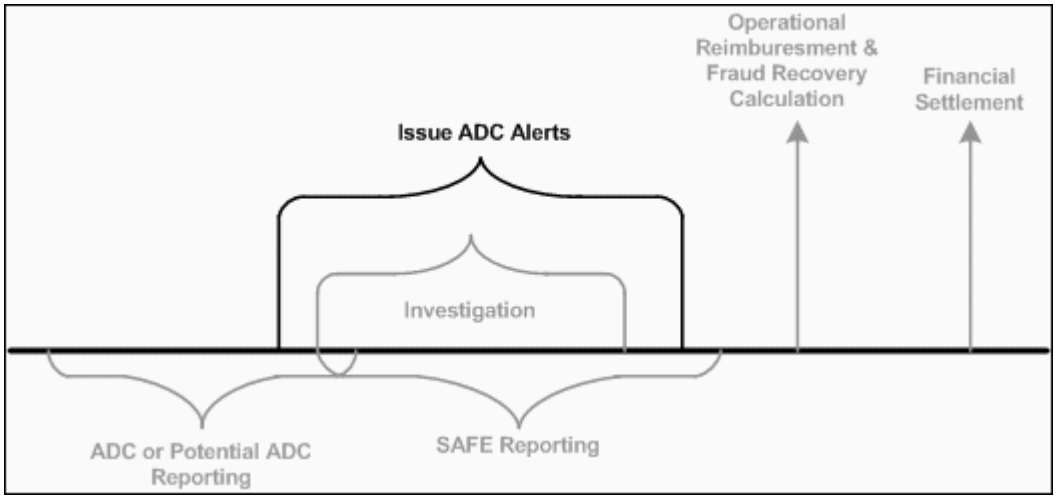
The calculation will utilize the published at-risk accounts that are available at the time of the calculation. Therefore, the amounts that appear on the final liability report may change from the originally communicated pre-estimate report.

Chapter 4 Manage My Fraud and Risk Programs—View Mastercard ADC Alerts Application

This chapter describes how to view Mastercard ADC Alerts via Manage My Fraud and Risk Programs application.

Overview of the Use of Manage My Fraud and Risk Programs for an ADC Event or Potential ADC Event

The following depicts where the publication of an ADC Alert falls in the life cycle of an ADC Event.



Each customer must be licensed to use the Manage My Fraud and Risk Programs application with at least two registered users.

A customer must ensure that any non-customer entity authorized to access Manage My Fraud and Risk Programs on behalf of the customer is registered with Mastercard as a service provider of the customer and has access to the Manage My Fraud and Risk Programs application.

Notification of Compromised Accounts Using Manage My Fraud and Risk Programs Application

If Mastercard determines that account data may be at risk as the result of an ADC Event or Potential ADC Event, Mastercard may publish an ADC Alert to notify issuers of accounts that may be at risk.

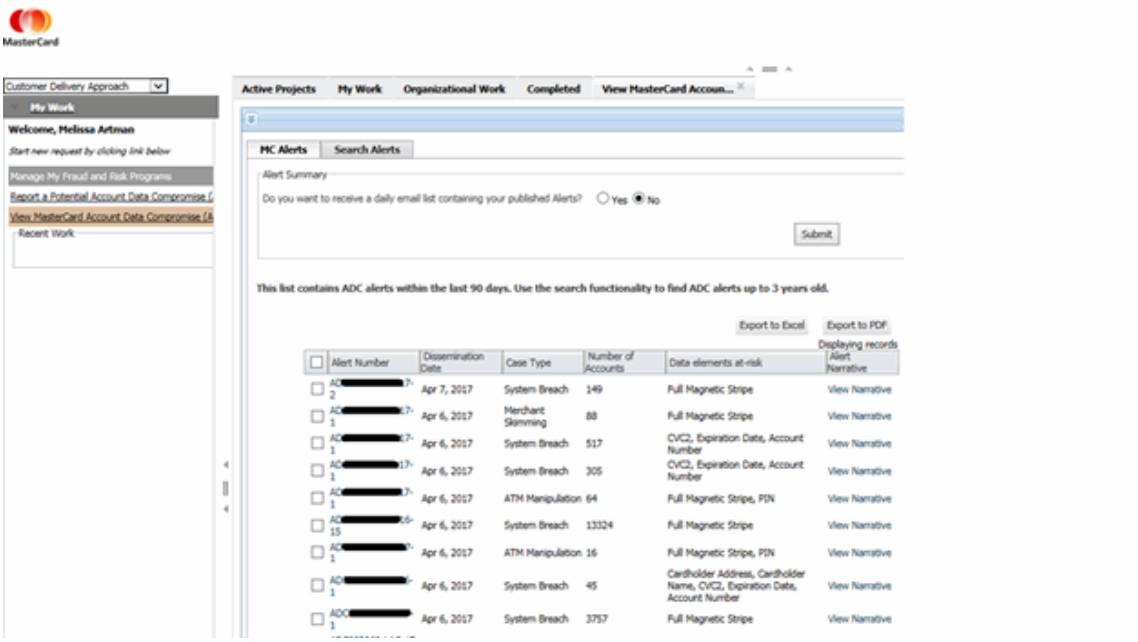
Mastercard may also notify by email or otherwise of an ADC Alert. The notification instructs the issuer to log into Manage My Fraud and Risk Programs Application to obtain a list of at-risk accounts and may include information about the ADC Event or Potential ADC Event.

NOTE: A Manage My Fraud and Risk email notification for an ADC Alert is sent to the email address located in the user's Mastercard Connect™ user profile. To change an email address, a customer may contact Customer Support at customer_support@mastercard.com.

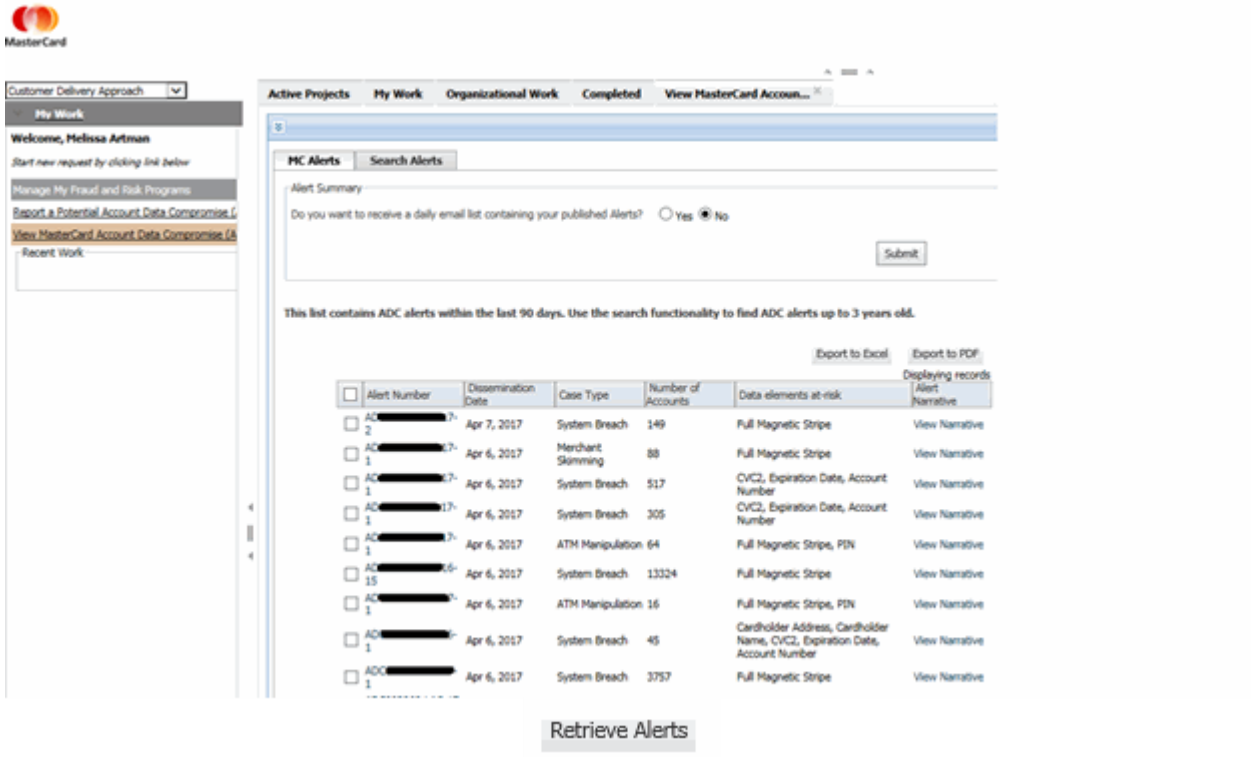
View Mastercard Account Data Compromise (ADC) Alerts

Customers must use View Mastercard Account Data Compromise (ADC) Alerts to review and download at-risk accounts.

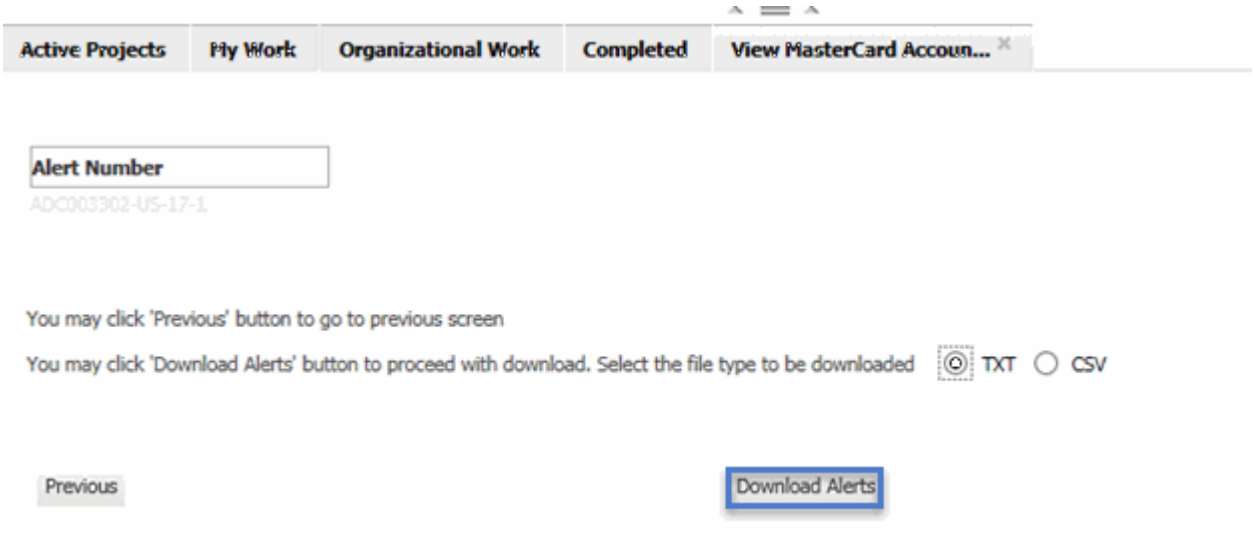
1. Go to www.mastercardconnect.com.
2. Log on using your Mastercard **User ID** and **Password**.
3. From the top of the Mastercard Connect homepage, click **My Apps**, and then click **Manage My Fraud and Risk Programs**.
4. Under Manage My Fraud and Risk Programs, click **View Mastercard Account Data Compromise (ADC) Alerts** located on the left side of the screen.
   - Customers will see their provisioned alerts for download, with columns for Alert Number, Dissemination Date, Case Type, Number of Accounts, Data Elements At-Risk, and Alert Narrative.
   - Customers can select one or more Alert Numbers to view in either .txt or .csv format by checking the box and select Retrieve Alerts.



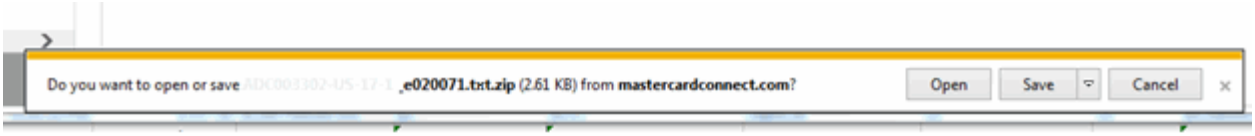
5. On the Alerts tab in Mastercard Connect, select one or more Alert Numbers to view by checking the box, and then click **Retrieve Alerts** at the bottom of the page.



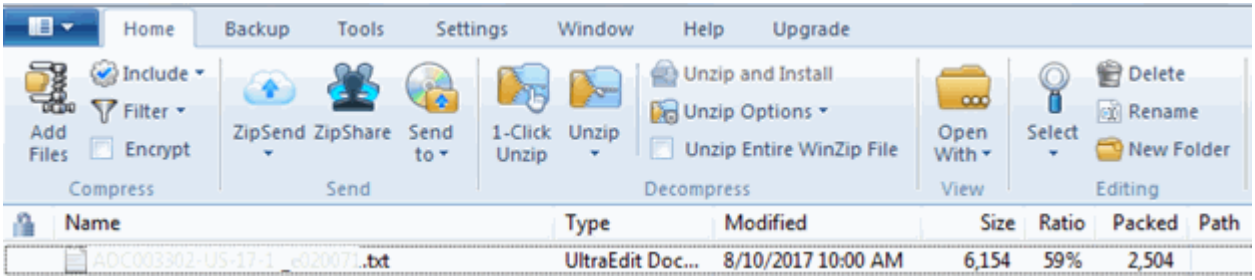
6. Select if you would like to download file as a .txt or .csv, and then click **Download Alerts**.
   - .txt format will only display PANs.
   - .csv format will display Alert dissemination information.
     - If more than one Alert is selected for download, you may have to wait up to two minutes for the file to be processed.



7. If a .txt file is selected, click **Open** or **Save** to save the file.

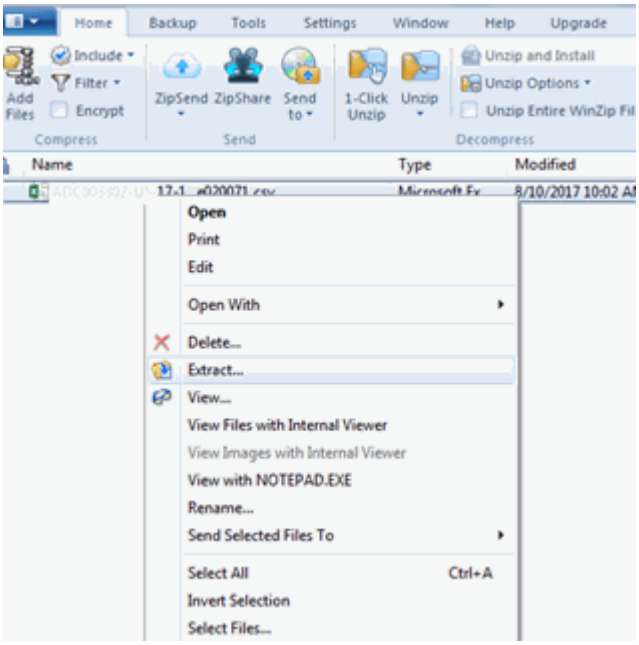


8. If a zip file opens, double-click on the file name. The file opens displaying PAN data.

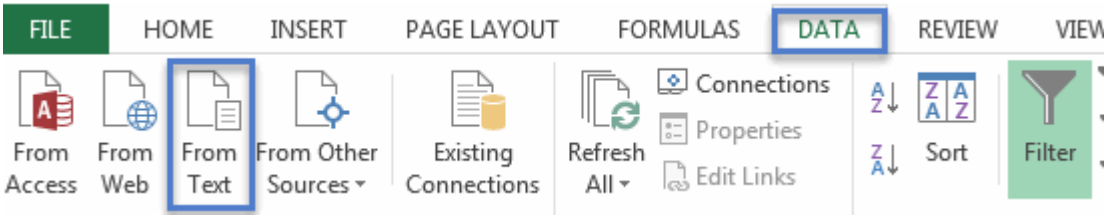


9. To open a .csv file click **Open** from the **File Download** menu.

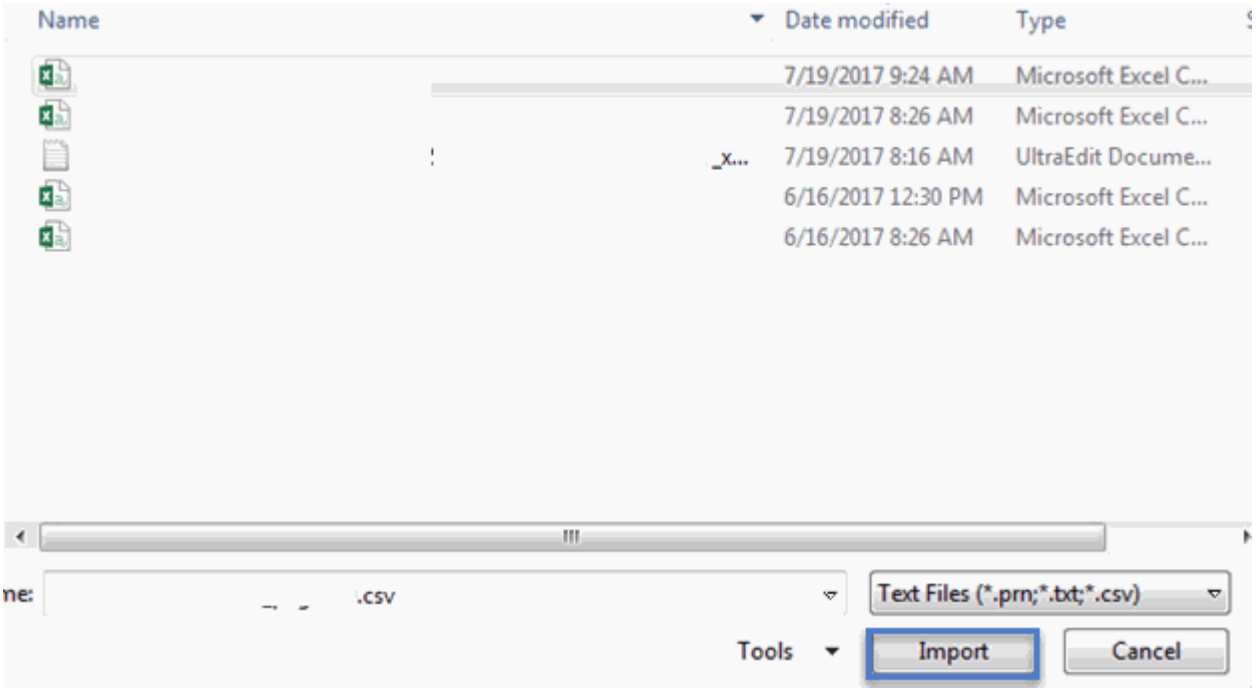
10. Right click on the file, select **Extract**, and then save the file on your computer.



11. Open a new Excel workbook. On the **Data** menu, click **From Text**.



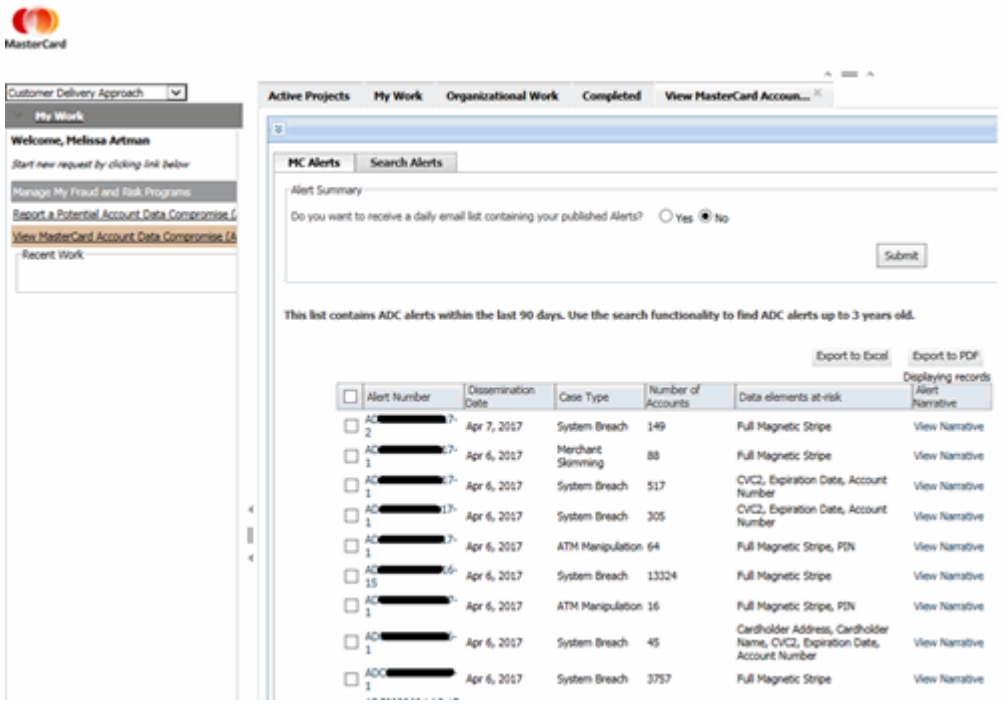
12. Select the file you saved and click **Import**.



13. Step 5 of 7 in Import Wizard – Click **Next**.
14. Step 6 of 7 in Import Wizard – Check the Comma box and click **Next**.
15. Step 7 of 7 in Import Wizard – Uncheck General then check **Text** and click **Finish**.
16. At the Import Data box, click **OK**.
    - Excel file will not have the Alert Dissemination Information.
    - Reference Appendix D for Mastercard ADC dissemination text file format.

Issuer—How to View Alert Narrative

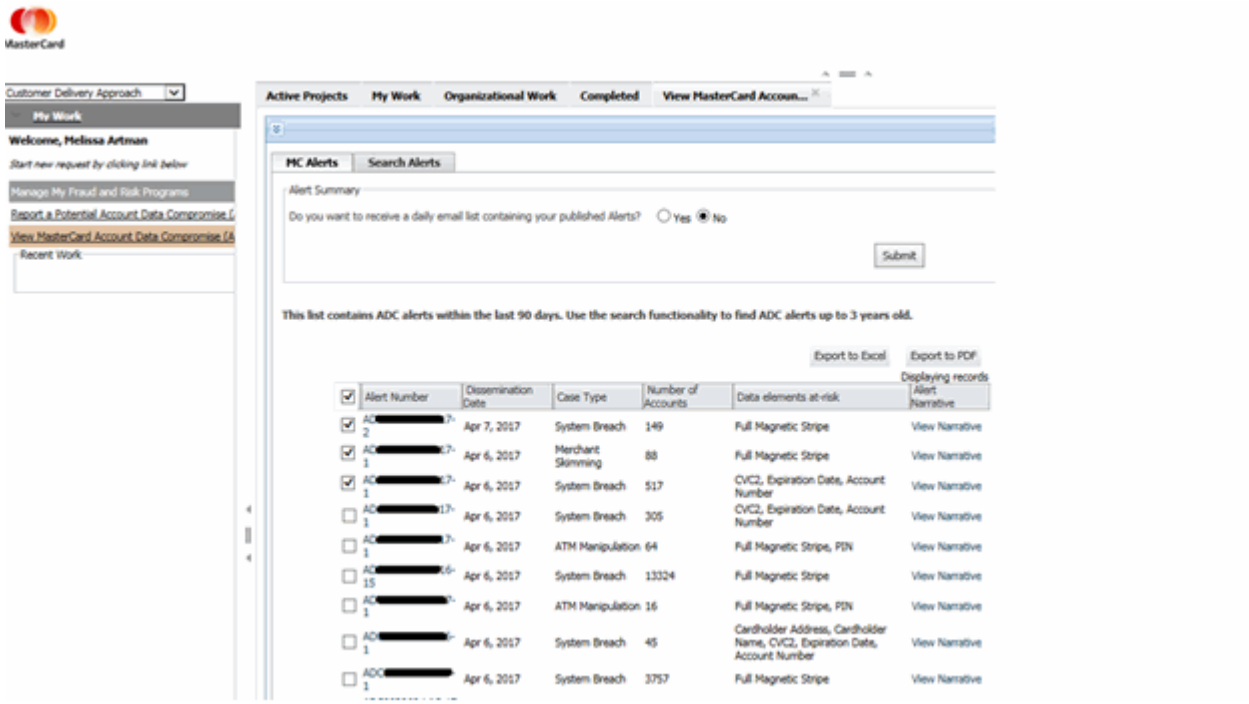
1. From the **View Mastercard Account Data Compromise (ADC) Alert** window, click **View Narrative**. A popup window displays with the narrative.



Issuer—How to Export Alert Narrative Details

1. From the **View Mastercard Account Data Compromise (ADC) Alert** window, click the check box of the narratives you want to view.

2. Click **Export to Excel** or **Export to PDF**.



Manage My Fraud and Risk Programs Quarterly Fees

Mastercard assesses a quarterly license fee at the (Marketing Parent) customer ID/ICA number level through Mastercard Consolidated Billing System (MCBS) for access to Manage My Fraud and Risk Program application. An affiliate without its own ICA must obtain information from its sponsoring principal (or that principal's service provider).

Fees are calculated based on the total number of accounts (including both open and blocked accounts) reported by each customer in the Quarterly Mastercard Report (QMR) for the prior quarter.

NOTE: If no accounts are reported to the QMR, the customer will be assessed Tier 3 fees.

The following table contains the fee structure in regions other than the Europe region and Brazil region.

Tier	Total Accounts	Quarterly Fee
1	More than 2,000,000	USD 5,000
2	400,000–2,000,000	USD 2,000
3	Fewer than 400,000	USD 300

The following table contains the fee structure in the Europe region.

Tier	Total Accounts	Quarterly Fee
1	More than 2,000,000	EUR 5,000
2	400,000–2,000,000	EUR 2,000
3	Fewer than 400,000	EUR 300

The following table contains the fee structure in Brazil.

Tier	Total Accounts	Quarterly Fee
1	More than 2,000,000	BRL 11,250
2	400,000–2,000,000	BRL 4,500
3	Fewer than 400,000	BRL 675

The following table contains the Manage My Fraud and Risk Programs licensing billing events.

Billing Event No.	Billing Event Description
TSC1357/ 2SC1358	MC Alerts Licensing Fee—USD
TKS13575/ 2KS13576	MC Alerts Licensing Fee—Euros
TSC1357/ 2SC1358	MC Alerts Licensing Fee—Reals

Updating a Manage My Fraud and Risk Programs User Profile

If a customer needs to update their Manage My Fraud and Risk Programs user profile or contact information (email address, name, or street address), the customer should change its Mastercard Connect™ user profile. To update the ICAs listed in its Manage My Fraud and Risk Programs profile, the customer should complete an update request.

To delete its Mastercard Connect™ user profile, the customer must complete a termination request on Mastercard Connect™, add or delete ICAs, or terminate its Manage My Fraud and Risk Programs access.

Any changes will take between one and three business days to be reflected in the Manage My Fraud and Risk Programs profile. To make changes to the Manage My Fraud and Risk Programs profile, the customer must:

1. Go to www.mastercardconnect.com.
2. Log on using your **User ID** and **Password**.
3. Click **Store** in the upper right corner of the window. The system displays the Store window.
4. Scroll to or search for the application that you want to order.
5. Click **Add to Cart**. The system displays a confirmation message in the upper right corner of the window.

To check out:

1. Click **Close** to close the Store window when your order is complete.
2. Click **Cart** in the upper right corner of the Mastercard Connect™ window. The system displays the cart.
3. Click **Check out**. The system displays the Order Details window.

If an application requires that you provide additional information, Mastercard Connect will display a message in the Order Details window to let you know that the ordered application requires additional information from you. Click the appropriate item to provide the related information.

1. Click **Review Order** to see the items that you have ordered.
2. Click **Place Order**. You will receive a confirmation number. Make note of this number so that you can track the order if needed. Mastercard Connect™ will send an e-mail to your security administrator to let him or her know that the order is awaiting approval.
3. Click **Close** to complete the order process.

NOTE: Customers should access Manage My Fraud and Risk on a regular basis to ensure access continuity.

Manage My Fraud and Risk Programs—Noncompliance Assessments

Two users from each ICA must be registered in Manage my Fraud and Risk in order for the customer to remain in compliance. Mastercard will notify a non-compliant customer with an e-mail notification to the Principal Contact and Security Contact listed in Mastercard Information online, noting the noncompliance and potential for assessment if not registered within 30 days of the email notification.

The non-compliance notification and assessment will continue until the customer has successfully registered for the required ICAs.

Mastercard may impose the following noncompliance assessments on customers that are not licensed to access the Manage My Fraud and Risk Programs application.

Noncompliance	Assessment
Existing customers not licensed to access Manage My Fraud and Risk Programs	If the customer is not licensed to access the Manage My Fraud and Risk Programs application, Mastercard may assess the customer USD 5,000 for each month of noncompliance.
New customers not licensed to access Manage My Fraud and Risk Programs	If the customer is not licensed to access the Manage My Fraud and Risk Programs application within 30 calendar days of membership, Mastercard may assess the customer USD 5,000 for each month of noncompliance.

NOTE: The effective "date of notice of non-compliance" is the date that an email notice is sent to the Principal (Marketing Parent) Contact and Security Contact of the customer listed in the most recent edition of the Mastercard Connect™ profile. The customer is responsible for ensuring the accuracy of contacts listed in the Member Information online. To change, delete, or add people, email Customer Support at customer_support@mastercard.com for assistance.

Requesting a Manage My Fraud and Risk Programs Application License

New customers have 30 calendar days from the initial date of membership to obtain a license.

Mastercard requires that every ICA number has at least two people licensed to use the Manage My Fraud and Risk Programs application.

To request a license for Manage My Fraud and Risk Programs, follow these steps.

1. Go to www.mastercardconnect.com.
2. Log on using your **User ID** and **Password**.
3. Click **Store** in the upper right corner of the window. The system displays the Store window.
4. Scroll to or search for the application that you want to order.
5. Click **Add to Cart**. The system displays a confirmation message in the upper right corner of the window.

To check out:

1. Click **Close** to close the Store window when your order is complete.
2. Click **Cart** in the upper right corner of the Mastercard Connect™ window. The system displays the cart.
3. Click **Check out**. The system displays the Order Details window.

If an application requires that you provide additional information, Mastercard Connect™ will display a message in the Order Details window to let you know that the ordered application requires additional information from you. Click on the appropriate item to provide the related information.

1. Click **Review Order** to see the items that you have ordered.
2. Click **Place Order**. You will receive a confirmation number. Make note of this number so that you can track the order if needed. Mastercard Connect™ will send an e-mail to your security administrator to let him or her know that the order is awaiting approval.
3. Click **Close** to complete the order process.

NOTE: Customers should monitor their Manage My Fraud and Risk Programs to ensure access continuity.

For instructions on how to register for Mastercard Connect™ access, contact the Mastercard Global Customer Service team.

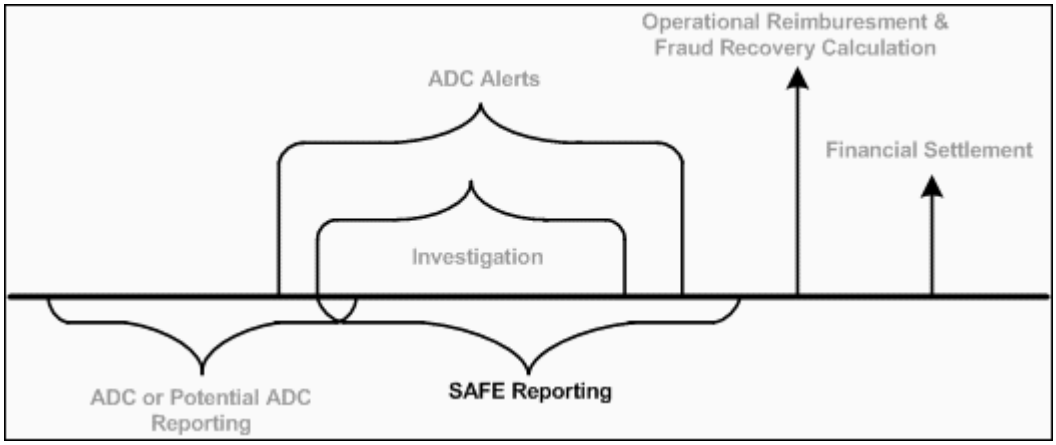
Mastercard will automatically terminate any Mastercard Connect™ user that has not logged on to the Manage My Fraud and Risk Programs application for six months. The customer's Manage My Fraud and Risk Programs license will be terminated at the same time as its Mastercard Connect™ user license. At that time, the customer is deemed not to be in compliance with the obligation to be licensed to use Manage My Fraud and Risk Programs. Once a Manage My Fraud and Risk Programs license is terminated, users who want to renew their license must apply for a new license following the preceding procedures.

Chapter 5 System to Avoid Fraud Effectively (SAFE) Reporting

This chapter describes how the Mastercard Fraud Recovery program interacts with SAFE.

Overview of SAFE Reporting

The following depicts where the submission of counterfeit fraud transaction data into the System to Avoid Fraud Effectively (SAFE) falls in the life cycle of an ADC Event.



The Mastercard Fraud Recovery (FR) program uses POS Entry Mode 80 and eligible POS Entry Mode 90 counterfeit fraud transaction data that is submitted to SAFE by the issuer in order to calculate incremental fraud to be used in the FR calculation. Issuers may adjust SAFE reported transactions that are utilized to calculate the applicable FR following the communication of the final liability notification. However, these adjustments to SAFE reported transactions will not impact the final FR liability.

As a reminder, accurate and timely submission of fraud data to SAFE will assist Mastercard in its efforts to reduce fraud through early identification.

For additional information on SAFE, refer to the *SAFE Products User Guide*, accessible through Publications.

The amount of time that impacted issuers are allocated to enter fraud transactions into SAFE is determined by the number of accounts in the ADC Event indicated as follows:

Tier	Minimum Number of Accounts	Maximum Number of Accounts	At-risk Length (Days)[4]
1	5,000,000	Unlimited	60
2	1,000,000	5,000,000	45

[4] **The ADC SAFE reporting time frame begins on the date of the ADC Alert notification. For example, if the alert is published on 1 March, and if the case falls into Tier 1, Fraud Recovery would be calculated 60 days after 1 March.**

Tier	Minimum Number of Accounts	Maximum Number of Accounts	At-risk Length (Days)[4]
3	30,000	1,000,000	30

Known At-Risk Time Frame

The at-risk time frame is "known" if Mastercard is able to determine a period of time during which Accounts were placed at risk of use in fraudulent transactions due to or in connection with an ADC Event or Potential ADC Event. In such event, the at-risk time frame for an Account number commences as of the date that Mastercard determines that Account became at risk, and ends on the date specified in the first ADC Alert pertaining to that ADC Event or Potential ADC Event disclosing that Account number. The number of days that the Issuer has to report fraudulent transactions to SAFE associated with an Account number disclosed in an ADC Alert is specified in the Alert; an Issuer is ineligible to receive FR associated with a fraudulent transaction arising from use of an Account number if that fraudulent transaction is not timely reported to SAFE.

Unknown At-Risk Time Frame

The at-risk time frame is "unknown" if Mastercard is unable to readily determine a known at-risk time frame. In such event, an at-risk time frame for an Account number commences twelve (12) months prior to the date of publication of the first ADC Alert for the ADC Event or Potential ADC Event that discloses that Account number, and ends on the date specified in that ADC Alert. The number of days that the Issuer has to report fraudulent transactions to SAFE associated with an Account number disclosed in an ADC Alert is specified in the Alert; an Issuer is ineligible to receive FR associated with a fraudulent transaction arising from use of an Account number if that fraudulent transaction is not timely reported to SAFE.

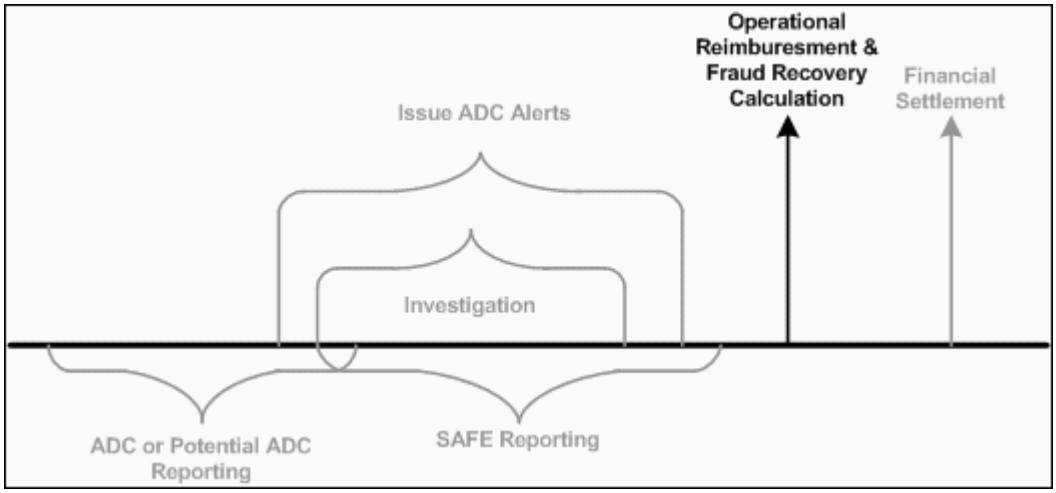
[4] **The ADC SAFE reporting time frame begins on the date of the ADC Alert notification. For example, if the alert is published on 1 March, and if the case falls into Tier 1, Fraud Recovery would be calculated 60 days after 1 March.**

Chapter 6 Operational Reimbursement and Fraud Recovery Calculation

This chapter provides additional details about the calculation of Operational Reimbursement (OR) and Fraud Recovery (FR) programs.

Overview of Operational Reimbursement and Fraud Recovery Calculation

The following depicts where the calculation of Operational Reimbursement (OR) and Fraud Recovery (FR) falls in the life cycle of an ADC Event.



ADC Case Eligibility for OR/FR

Mastercard may invoke OR or OR and FR, for an ADC Event if a minimum of 30,000 eligible Mastercard accounts were impacted, or in instances where an entity has been re-breached, regardless of the number of impacted accounts in the subsequent Event.

In the event that the compromised entity is an e-commerce merchant where only PAN, expiration date, and/or the CVC code have been compromised, only OR will be invoked.

As of 1 January 2016, participation in the reimbursement component of the ADC Program became optional for issuers. On an annual basis, an issuer will choose whether to participate in the reimbursement component of the ADC Program. Should Mastercard determine that an insufficient number of issuers have opted to participate in the reimbursement component for a calendar year, the reimbursement component will not be administered by Mastercard during that calendar year. No issuer will receive any OR or FR for any ADC Event that Mastercard determines to have occurred during that calendar year. The year of the occurrence of an Event is based on the year in which the first Alert for that particular Event was issued by Mastercard.

Each issuer that chooses to participate in the reimbursement component, as a condition of such participation, must agree to hold harmless and release Mastercard and, as applicable, each responsible customer and each agent of each responsible customer from financial and other liability directly or indirectly related to an ADC Event that Mastercard deems to have

occurred during that calendar year. An issuer that chooses not to participate in the reimbursement component will not be eligible for OR or FR for that calendar year.

Following the conclusion of an investigation of an ADC Event by Mastercard, any related OR and/or FR liability will be disclosed to the responsible customer(s) in a final financial liability letter. The responsible customer(s) will have 30 days from the date of the final financial liability letter to either agree with the final liability or submit an appeal. As a condition of agreeing to the determined amount, the responsible customer must both:

- Execute and deliver to Mastercard within 30 calendar days of receipt of the final financial liability letter or a decision by Mastercard on the appeal, whichever is later, a release in a form and substance acceptable to Mastercard memorializing that the customer agrees to not assert a claim arising from or related to the ADC Event against either Mastercard or any issuer that receives OR and/or FR
- Deliver to Mastercard a release in a form and substance acceptable to Mastercard and executed by the merchant (or other agent) that the merchant (or other agent) agrees to not assert a claim arising from or related to the ADC Event against either Mastercard or any issuer that receives OR and/or FR

Mastercard will subsequently debit funds from the responsible customer's account and disburse OR and/or FR, as appropriate, to issuers. If the responsible customer does not agree to the final determined amount, any issuer, including those that opted into the reimbursement program for the calendar year, will have its right to pursue claims against the responsible customer and/or its agent, reinstated.

Estimate of Potential Financial Liability

Mastercard may provide an estimate of potential financial liability to the acquirer(s) responsible for the event.

Mastercard may send Acquirer Pre-Estimate Liability Notifications and Pre-Estimate Liability Reports to (a) the acquirer's ADC Compliance Contact or Security Contact and (b) the Principal Contact listed in the Member Information online application. The estimate is calculated by using the published at-risk accounts and the existing fraud data in SAFE to produce a "snapshot" of the calculation of OR and FR.

Subsequent to the distribution of the Pre-Estimate notification, the number of compromised or potentially compromised accounts may change or the amount of eligible counterfeit fraud reported to SAFE may change, resulting in change(s) in potential financial responsibility for the acquirer(s).

ADC Operational Reimbursement

Operational Reimbursement (OR) is calculated at the Marketing Parent ICA level. All Mastercard (credit and signature debit or PIN debit) accounts that were published in an ADC Alert related to the ADC Event will be included in the calculation based on the issuers that have opted in to the ADC program for the year the event occurred. As of 1 January 2017,

Mastercard ceased issuing OR and FR reimbursement for Mastercard branded magnetic stripe-only cards. [5]

Calculating Operational Reimbursement (OR)

To calculate OR, the following steps are performed:

1. Determine the tier of each impacted issuer based on size.
2. If applicable, exclude accounts which belong to issuers that elected to Opt-Out of the program for the year the event occurred.
3. Identify the type of technology embedded for each eligible account.
4. Multiply each account by the applicable reimbursement rate as defined in Section 6.5.1, Table 1.
5. Subtract the recovery associated with cards that were previously alerted on in the prior 180 days of the applicable ADC Alert.
6. Subtract a fixed deductible for normal card re-issuance.

ADC Operational Reimbursement Factors

Operational Reimbursement (OR) is provided to issuers to partially offset card replacement and account fraud monitoring costs. The following factors are used to calculate ADC OR:

Determine the size of the each impacted issuer.

The tier of each impacted issuer is determined based on the gross dollar volume, obtained from the Quarterly Mastercard Report (QMR), at the Marketing Parent ICA level[6]for the issuer(s) impacted by the event. Please see the below table outlining the applicable tiers:

Tier	Issuer—Gross Dollar Volume
1	0–200 MM
2	201 MM-1 B
3	>1 B

- Identify the type of technology embedded in the card

The ADC OR calculation will utilize a different reimbursement rate for the following technologies embedded in the card:

- Magnetic Stripe
- Magnetic Stripe + Chip
- Magnetic Stripe + *Contactless*

[5] Maestro and Cirrus accounts, and Mastercard accounts with magnetic-stripe only technology are not eligible for OR reimbursement.

[6] As a result of the opt-in process, if the ICA is licensed as a Principal Debit Licensee or Sponsoring Third Party Processor and the Marketing Parent ICA has not opted in, the ICA will be treated as a Marketing Parent ICA to determine the reimbursement rate.

- Magnetic Stripe + Chip + *Contactless*

To determine the type of technology embedded in the card, the Mastercard Authorization File is searched for transactions processed during the 90 days before the date of the ADC Alerts in which a specific account is published.

The following table defines the Authorization File data elements used to identify card technology types.

Card Type	DE 22 (Point-of-Service [POS] Entry Mode)	DE 55 (Integrated Circuit Card [ICC] System-related Data)	DE 35/45 (Track 2 Date - Service Code)
Magnetic Stripe	02, 90		
Magnetic Stripe and Chip	05, 06, 79, 80	Present	2xx or 6xx
Magnetic Stripe and *Contactless*	91, 92		
Magnetic Stripe and Chip and *Contactless* (Combo)	07, 08		2xx or 6xx

If no transactions are found in the Mastercard Authorization File for an at-risk account, the card type will be considered to be Magnetic Stripe and Chip.

The number of accounts, by card technology type, are multiplied by the applicable reimbursement rate per tier (as defined in the table below), resulting in a gross eligible reimbursement amount.

Reimbursement Rate Per Tier

	Gross Dollar Volume	Mag Stripe	Chip[7]	Contactless	Combo[8]
1	0–200 MM	USD 0.00	USD 7.25	USD 7.50	USD 8.00
2	201 MM-1 B	USD 0.00	USD 5.00	USD 5.15	USD 5.30

[7] References to Chip in this document refer to Chip cards that support the EMV standard.

[8] A Combo reimbursement rate will be assigned to a card that contains: magnetic stripe, Chip, and Mastercard Contactless technology. For additional information, refer to Chapter 10 of Mastercard *Security Rules and Procedures* manual.

	Gross Dollar Volume	Mag Stripe	Chip[7]	Contactless	Combo[8]
3	> 1B	USD 0.00	USD 3.75	USD 3.95	USD 4.05

These rates are applicable for both card present and card-not-present ADC Events, and are effective for ADC events first alerted on or after 1 January 2017.

- Accounts published in previous alerts in the last 180 days are deducted and are not eligible for OR reimbursement in the event being calculated
- A fixed deductible of 10 percent is subtracted from the gross eligible reimbursement amount to reflect anticipated card expiration

The result is a Net Eligible Reimbursement Amount by Issuer Marketing Parent ICA. The Net Eligible Reimbursement amounts for all issuers are added together and presented to the acquirer as the total operational reimbursement liability amount.

ADC Operational Reimbursement—BIN Reports

Mastercard provides ADC OR reports at the bank identification number (BIN) level free of charge. Each report details ADC OR for a case by ICA number for all BINs within the ICA.

To obtain this report, the issuer must send an email to account_data_compromise@mastercard.com with the following information:

- ICA number
- Issuer's Contact Name and E-mail Address
- Indication of whether this is a one-time request or whether this report should be provided every time OR is invoked for an ADC case
- If it is a one-time request, indicate the ADC Alerts Case number

The BIN Level reports are automatically provided once the BIN level report registration has been completed. The BIN level reports are typically communicated within 48 hours in advance of reimbursed credit.

The OR BIN Level report provides the following information as set forth in the following table:

Marketing Parent ICA	Child ICA	BIN	Magstripe Amount USD	Chip Amount USD	Contactless Amount USD	Combo Amount USD	Total Amount USD
XXXX							
	XXXX	XXXXX	10.00	5.00	1.00		16.00

[7] References to Chip in this document refer to Chip cards that support the EMV standard.

[8] A Combo reimbursement rate will be assigned to a card that contains: magnetic stripe, Chip, and Mastercard Contactless technology. For additional information, refer to Chapter 10 of Mastercard *Security Rules and Procedures* manual.

Marketing Parent ICA	Child ICA	BIN	Magstripe Amount USD	Chip Amount USD	Contactless Amount USD	Combo Amount USD	Total Amount USD
		XXXXX	13.00	4.00			17.00
		Sub-total	**23.00**	**9.00**	**1.00**		**33.00**
	XXXX	XXXXX	10.00	5.00	1.00		16.00
		XXXXX	13.00	4.00			17.00
		Sub-total	**23.00**	**9.00**	**1.00**		**33.00**
	XXXX	XXXXX	10.00	5.00	1.00		16.00
		XXXXX	13.00	4.00			17.00
		Sub-total	**23.00**	**9.00**	**1.00**		**33.00**
		Grand Total	**69.00**	**27.00**	**3.00**		**99.00**

ADC Operational Reimbursement—Acquirers and Issuers

The following describes OR notifications for acquirers and issuers.

Acquirers—Liability Notification

Once the total OR, and/or, OR and FR (if FR applies) is calculated for an ADC Event, Mastercard will notify the responsible customer(s) of the financial responsibility; This notice will be sent to the responsible customer's ADC Compliance Contact/Investigation, Security Contact and/or Principal Contact as defined in Member Information online application. Mastercard will then debit the responsible customer's MCBS account for the amount calculated. See the sample letter in Appendix A, Final Responsibility Letter.

Issuers—Reimbursement Notification

Mastercard will notify the first Security Contact in alphabetical order by last name of the Parent ICA at the time of the calculation (as defined in the Member Information online application Profile of the applicable ICA), of each impacted issuer, the total operational reimbursement amount it will receive for a specific ADC Event and the date that the OR amount will be credited to the issuer's MCBS account. See the sample letter in Appendix A, Issuer Credit Letter.

If additional contacts require receipt of the issuer reimbursement notification, provide the contact name, email information, and ICA of the institution to account_data_compromise@mastercard.com.

ADC Operational Reimbursement—Customer Responsibility Cap

Chapter 10 of Mastercard *Security Rules and Procedures* manual states that Mastercard "may potentially reduce liability" in connection with an ADC Event.Only entities that are PCI level 3 or 4 are eligible for the responsibility cap. Mastercard will determine if the compromised entity is PCI level 3 or 4. Mastercard will evaluate the following factors to determine whether financial liability should be invoked for an ADC Event:

- Annual Mastercard Sales volume for the calendar year prior to the year in which liability is calculated.
- Items noted in Chapter 10 of the *Security Rules and Procedures* manual

The cap is applied to the total ADC Operational Reimbursement (OR) and not to any other fee associated with an ADC Event.

If Mastercard determines a cap for acquirer financial responsibility is appropriate Mastercard will utilize the following tiered formula:

Prior Calendar year's transactions	Merchant Cap percentage applied
< or =50,000	5 percent
50,000 - 500,000	10 percent
>500,000	20 percent

Merchant Cap Example			
Prior calendar year Mastercard Merchant Sales	X	5 percent	Revised Total OR Responsibility with Cap Applied

When total OR is capped by Mastercard, the revised OR total is applied proportionally to all issuers. The following demonstrates how a cap may be applied

Initial Acquirer Responsibility	USD 39,000
Mastercard Merchant Sales	USD 50,000
Cap 5 percent	USD 2,500

The following is a sample of the *Estimated Acquirer Financial Responsibility Report*. Mastercard may send a letter and this report to both:

- The acquirer's ADC Compliance Contact or Security Contact
- The Principal Contact listed in the Member Information online application

Mastercard

ADC Operational Reimbursement/Fraud Recovery
Estimated Acquirer Financial Responsibility Report

Responsible Acquirer Name, ICA XXXX — Report Date:

Case Summary

MC Alerts Case #	ADCXXXX-XX
Case Type	System Breach
Compromised Entity Name	Compromised Entity Name
Total # of Qualifying Alerts	X
Total # of Accounts Eligible for OR/FR	XXXX

Operational Reimbursement calculated dd-mm-yyyy

	Card Types							
Tier	Mag Stripe		Chip		Contactless		Combo	
	Number	Rate	Number	Rate	Number	Rate	Number	Rate
1	X	$0	X	$7.25	X	$7.50	X	$8.00
2	X	$0	X	$5.00	X	$5.15	X	$5.30
3	X	$0	X	$3.75	X	$3.95	X	$4.05

Gross Eligible Reimbursement Amount	$0.00
# of Accounts in Previous Alerts	X
Operational Reimbursement Associated with Previous Alerts	$0.00
Net Eligible Reimbursement Amount	$0.00
Deductible	($0.00)
Net Eligible Reimbursement Amount	$0.00
Eligible Cap	$0.00
Total Estimated Operational Reimbursement	**$0.00**

Fraud Recovery calculated dd-mm-yyyy

Incremental Fraud for Case	$0.00
# of Accounts in Previous Alerts	X
Fraud Associated with Previous Alerts	$0.00
Eligible Fraud Recovery Amount	$0.00
Deductible	($0.00)
Net Eligible Fraud Recovery Amount	$0.00
Eligible Cap	$0.00
Total Estimated Fraud Recovery	**$0.00**

Acquirer Summary

Total Estimated Liability	$0.00
Acquirer Percentage	100.0%
Acquirer Total Estimated Operational Reimbursement	$0.00
Acquirer Total Estimated Fraud Recovery	$0.00
Total Estimated Acquirer Financial Responsibility	**$0.00**

The data in this report is an estimate and represents the case financials in USD as of the calculation dates.

The following is a sample of the "Final Financial Responsibility Report." Mastercard may send a letter and this report to both (a) the acquirer's ADC Compliance Contact or Security Contact and (b) the Principal Contact listed in the Member Information online application.

Mastercard

ADC Operational Reimbursement/Fraud Recovery
Final Acquirer Financial Responsibility Report

Responsible Acquirer Name, ICA XXXX — Report Date:

Case Summary

MC Alerts Case #	ADCXXXX-XX
Case Type	System Breach
Compromised Entity Name	Compromised Entity Name
Total # of Qualifying Alerts	X
Total # of Accounts Eligible for OR/FR	XXXX

Operational Reimbursement calculated dd-mm-yyyy

	Card Types							
Tier	Mag Stripe		Chip		Contactless		Combo	
	Number	Rate	Number	Rate	Number	Rate	Number	Rate
1	X	$0	X	$7.25	X	$7.50	X	$8.00
2	X	$0	X	$5.00	X	$5.15	X	$5.30
3	X	$0	X	$3.75	X	$3.95	X	$4.05

Gross Eligible Reimbursement Amount	$0.00
# of Accounts in Previous Alerts	X
Operational Reimbursement Associated with Previous Alerts	$0.00
Net Eligible Reimbursement Amount	$0.00
Deductible	($0.00)
Net Eligible Reimbursement Amount	$0.00
Eligible Cap	$0.00
Total Estimated Operational Reimbursement	**$0.00**

Fraud Recovery calculated dd-mm-yyyy

Incremental Fraud for Case	$0.00
# of Accounts in Previous Alerts	X
Fraud Associated with Previous Alerts	$0.00
Eligible Fraud Recovery Amount	$0.00
Deductible	($0.00)
Net Eligible Fraud Recovery Amount	$0.00
Eligible Cap	$0.00
Total Estimated Fraud Recovery	**$0.00**

Acquirer Summary

Total Estimated Liability	$0.00
Acquirer Percentage	100.0%
Acquirer Total Estimated Operational Reimbursement	$0.00
Acquirer Total Estimated Fraud Recovery	$0.00
Total Estimated Acquirer Financial Responsibility	**$0.00**

ADC Fraud Recovery

Chapter10 of the *Security Rules and Procedures* manual sets forth standards regarding fraud recovery. The following is a summary of factors used to calculate Fraud Recovery (FR), effective 1 January 2016.

- A = Total counterfeit fraud for all opted in issuers' at-risk accounts specific to an ADC Event as reported to the System to Avoid Fraud Effectively (SAFE) during the at-risk time frame

- B = Baseline fraud (Counterfeit fraud for at-risk accounts immediately preceding the first day of the at-risk time frame) that would typically be seen for all non-event related fraud during 12 months prior to the at-risk time
- C = Net incremental counterfeit fraud associated with the ADC Event during the at-risk time frame
- D = Fraud reported on accounts that were previously alerted on 180 days prior to the ADC Event
- E = Standard deductible to recognize chargeback recoveries on transactions using at-risk accounts (updated annually). Effective December 1, 2014, this rate is set at 5 percent
- F = Net eligible for fraud recovery amount

NOTE: FR is calculated in USD.

Eligible counterfeit fraud:		A
Less baseline fraud:	–	B
Net incremental fraud		C
Minus duplicate fraud	–	D
Minus standard chargeback	–	E
Net eligible for FR		F

ADC Fraud Recovery—BIN Reports

Mastercard offers an optional report that details ADC Fraud Recovery (FR) reimbursement amounts. The FR BIN Level Report is available free of charge.

To obtain this report, the issuer must send an email to account_data_compromise@mastercard.com with the following information:

- ICA Number
- Issuer's Contact Name and E-mail Address
- Indication of whether this is a one-time request or whether this report should be provided every time FR is invoked for an ADC case
- If it is a one-time request, indicate the ADC Alerts Case number

BIN Level reports provide FR totals by Marketing Parent ICA, Child ICA, and BIN. Consequently, the issuer (Marketing Parent ICA) receives a report showing the number and type of accounts reimbursed. The report provides information similar to that shown in the following table and are typically communicated within 48 hours in advance of reimbursement credit.

Marketing Parent ICA	Child ICA	BIN	Total Fraud Recovery Amount USD
NNNN			

Marketing Parent ICA	Child ICA	BIN	Total Fraud Recovery Amount USD
		NNNNNN	10.00
		NNNNNN	13.00
		Subtotal	23.00
	NNNN	NNNN	
		NNNNNN	10.00
		NNNNNN	13.00
		Subtotal	23.00
	NNNN		
			10.00
			13.00
		Subtotal	23.00
		Grand Total	69.00

ADC Fraud Recovery—Notification

The following describes FR notifications for responsible customers and issuers.

Responsible Customer—Liability Notification

Once the total OR, and/or, OR and FR (if FR applies) is calculated for an ADC Event, Mastercard will notify the responsible customers of the financial responsibility; This notice will be sent to the responsible customer's ADC Compliance/Investigation Contact, Security Contact, and/or Principal Contact as defined in the Member Information online application Profile of the applicable ICA. Mastercard will then debit the responsible customer's MCBS account for the amount calculated. See the sample letter in Appendix A, Final Responsibility Letter.

Issuer—Reimbursement Notification

Mastercard will notify the first Security Contact in alphabetical order by last name of the Parent ICA at the time of the calculation as defined in the Member Information online application, of the total fraud recovery it will receive for a specific ADC Event and the date that the fraud recovery amount will be credited to the issuer's MCBS account. See the sample in Appendix A, Issuer Credit Letter.

If additional contacts require receipt of the issuer reimbursement notification, please provide the contact name, email information and Parent ICA of the institution to account_data_compromise@mastercard.com.

ADC Fraud Recovery—Acquirer Responsibility Cap

Chapter 10 of the Mastercard *Security Rules and Procedures* manual states that Mastercard "may potentially reduce liability" in connection with an ADC Event. Only entities that are PCI level 3 or 4 are eligible for the responsibility cap. Mastercard will determine if the compromised entity is PCI level 3 or 4. Mastercard will evaluate the following factors to determine whether a responsibility cap should be invoked for an ADC Event.

- Prior calendar year's annual Mastercard sales volume
- Items noted in Chapter 10 of the *Security Rules and Procedures* manual

The cap is applied to the total ADC Fraud Recovery (FR) and not to any other fee associated with an ADC Event.

If Mastercard determines a cap for acquirer financial responsibility is appropriate Mastercard will utilize the following tiered formula:

Prior Calendar year's transactions	Merchant Cap percentage applied
< or =50,000	5 percent
50,000 - 500,000	10 percent
>500,000	20 percent

ADC Fraud Recovery Factors

Mastercard uses the following factors to calculate ADC Fraud Recovery (FR) at the Marketing Parent ICA level.

Counterfeit Fraud Baseline

Using accounts published via the Manage My Fraud and Risk Programs Connect Application, Mastercard will calculate (a) a counterfeit baseline by looking at POS 90 and POS 80 eligible counterfeit fraud that was reported to the System to Avoid Fraud Effectively (SAFE) program at the Marketing Parent ICA level and (b) the incremental counterfeit fraud associated with the applicable ADC Event. Mastercard will determine the incremental fraud amount by calculating the amount of eligible counterfeit fraud for an ADC Event by Marketing Parent ICA and reducing the total event-specific counterfeit fraud amount by the baseline counterfeit fraud experienced by the issuing Marketing Parent ICA for the at-risk accounts prior to the start of the at-risk time frame for the ADC Event.

At-Risk Time Frame

When the at-risk start date is known, the fraud recovery formula uses that start date and an end date is determined by using the following table.

If the fraud recovery time frame is not known, the start date will begin 365 days before the date the ADC Alert associated with the case was published and calculate the end date using the following table.

Tier	Minimum Number of Accounts	Maximum Number of Accounts	No. of Days after the Date of ADC Alerts Publication
1	5,000,001	Unlimited	60
2	1,000,001	5,000,000	45
3	30,000[9]	1,000,000	30

Known At-risk Time Frame

The at-risk time frame is "known" if Mastercard is able to determine a period of time during which Accounts were placed at risk of use in fraudulent transactions due to or in connection with an ADC Event or Potential ADC Event. In such event, the at-risk time frame for an Account number commences as of the date that Mastercard determines that Account became at risk, and ends on the date specified in the first ADC Alert pertaining to that ADC Event or Potential ADC Event disclosing that Account number. The number of days that the Issuer has to report fraudulent Transactions to SAFE associated with an Account number disclosed in an ADC Alert is specified in the Alert; an Issuer is ineligible to receive FR associated with a fraudulent Transaction arising from use of an Account number if that fraudulent Transaction is not timely reported to SAFE.

Unknown At-risk Time Frame

The at-risk time frame is "unknown" if Mastercard is unable to readily determine a known at-risk time frame. In such event, an at-risk time frame for an Account number commences twelve (12) months prior to the date of publication of the first ADC Alert for the ADC Event or Potential ADC Event that discloses that Account number, and ends on the date specified in that ADC Alert. The number of days that the Issuer has to report fraudulent Transactions to SAFE associated with an Account number disclosed in an ADC Alert is specified in the Alert; an Issuer is ineligible to receive FR associated with a fraudulent Transaction arising from use of an Account number if that fraudulent Transaction is not timely reported to SAFE.

Refer to the following examples of how the at-risk time frames set forth in the table above are applied.

The following table shows an ADC event with a known at-risk time frame.

ADC Alerts Publication Date	03/01/09
Number of Accounts in the ADC Alerts	500,000

[9] Mastercard reserves the right to invoke FR for cases that are less than 30,000 accounts.

At-risk Length	30 Calendar Days (from table above for 500,000 accounts – Tier 3)
At-risk Time Frame—Start Date (Known)	02/01/08
At-risk Time Frame—End Date (Calculated)	03/01/09 plus 30 days = 3/31/09

The following table shows an ADC event with an unknown at-risk time frame.

ADC Alerts Publication Date	03/01/09
Number of Accounts in the ADC Alerts	500,000
At-risk Length	30 Calendar Days (from table above for 500,000 accounts – Tier 3)
At-risk Time Frame—Start Date (Unknown and Calculated)	02/01/08
At-risk Time Frame—End Date (Calculated)	3/31/09 (03/01/09 plus 30 days)

Incremental Counterfeit Fraud Calculation

Mastercard determines the "incremental" fraud by determining the fraud for an ADC Event by Marketing Parent ICA and then reducing the total eligible counterfeit fraud by the baseline counterfeit fraud experienced by the issuing Marketing Parent ICA 12 months before the at-risk time frame.

Duplicate Fraud

The incremental fraud is reduced by the amount of counterfeit fraud on unique at-risk accounts published in ADC Alerts during 180 days prior to the alert date.

Chargeback Deduction

A 5 percent deductible is applied to the total estimate/final recovery. This includes Incremental Fraud and all other applicable deductions.

EMV Liability Shift Impact

Accounts that qualify for a counterfeit fraud chargeback will be removed from consideration during the liability calculation process. Issuers who have implemented EMV chip cards will have the opportunity to chargeback their counterfeit fraud to the non-chip enabled party. Transactions that qualify for a counterfeit fraud chargeback will be removed from the calculations regardless of whether the issuer files the chargeback.[10]

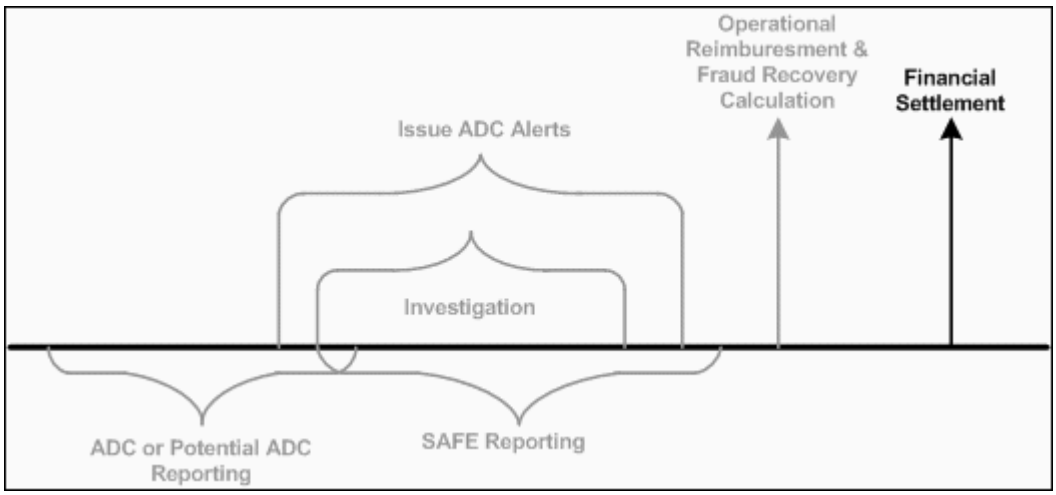
[10] Refer to the Dispute Resolution Manual for eligible chargebacks

Chapter 7 Financial Settlement of ADC Events

This chapter describes financial settlement of losses encountered as a result of an ADC Event, including operational reimbursement, fraud recovery, and the Annual Service Fee.

Overview of the Financial Settlement of ADC Events

The following depicts where identification of the financial liability falls in the life cycle of an ADC Event.



ADC Event Financial Settlement Information

Following the conclusion of an ADC investigation, Mastercard will determine the financial responsibility for an ADC Event, should liability apply. The final financial responsibility. For an ADC case, there are several types of potential responsibility:

- Operational Reimbursement Liability
- Fraud Recovery Liability
- Non-compliance assessment associated with a Mastercard Rules violation
- PCI violations

When Mastercard determines that the ADC investigation is complete, financial responsibility is communicated to the acquiring bank (see Appendix A, Final Responsibility Letter). Section 7.3 identifies the billing events associated with final liability that will be debited 30 days after the final notification.

Operational Reimbursement

Mastercard will notify the responsible customer of any operational reimbursement responsibility.

Operational Reimbursement Billing Event Codes for Acquirers

Upon completion of the OR process, Mastercard debits the responsible customer(s) through MCBS. The debit appears on the weekly MCBS billing statement. For billing event codes

associated with operational reimbursement debits, refer to the *Mastercard Consolidated Billing System* (MCBS) document.

Country/Region	MCBS Billing Event ID	MCBS Statement Description
U.S.	2SC1327	Account Data Compromise Issuer Reimbursement Liability
Brazil	2SC1327	Account Data Compromise Issuer Reimbursement Liability (Brazil)

Fraud Recovery

Mastercard will notify the responsible customer of any fraud recovery responsibility.

Fraud Recovery Billing Event Codes for Acquirers

Upon completion of the FR process Mastercard will debit the responsible customer using MCBS. The debits will appear on the weekly MCBS billing statement. For billing event codes associated with fraud recovery debits, refer to the *Mastercard Consolidated Billing System* (MCBS) document.

Country/Region	MCBS Billing Event ID	MCBS Statement Description
U.S.	2SC1214	Account Data Compromise Issuer Reimbursement Liability
Brazil	2SC1214	Account Data Compromise Issuer Reimbursement Liability (Brazil)

ADC Event Financial Settlement Information for Issuers

Mastercard will provide partial reimbursement to issuers for losses incurred as the result of an ADC Event should the Event qualify for liability. There are two types of issuer reimbursement:

- Operational Reimbursement
- Fraud Recovery

During the week prior to reimbursement, Mastercard endeavors to send a reimbursement (credit) letter to each issuer that Mastercard anticipates will receive reimbursement. The following sections explain the communication and billing events associated with issuer reimbursement. The notifications are sent to the Security Contact of that Marketing Parent ICA as listed in the Member Information Manual online application at the time of the Event.

Operational Reimbursement Notification

Mastercard credits an issuer's MCBS account with the ADC operational reimbursement for each applicable Marketing Parent ICA.

A breakdown of the operational reimbursement by the bank identification number (BIN) level is available upon request. For more information, refer to the previous section–ADC Operational Reimbursement—BIN Reports.

Operational Reimbursement Billing Event Codes for Issuers

Upon completion of the OR process, Mastercard credits issuers through MCBS. The credits appear on the weekly MCBS billing statement. Detailed below are the billing event codes associated with OR credits.

Country/Region	Billing Event	MCBS Statement Description
Global (excluding Brazil)	2PN-CRD2325	ADC—Credit for Operational Reimbursement
Brazil	2PN-CRD2325	ADC—Credit for Operational Reimbursement

Fraud Recovery—Reimbursement Notification

Mastercard credits the issuer's MCBS account with the total ADC fraud recovery for each applicable Marketing Parent ICA.

A breakdown of the fraud recovery by bank identification number (BIN) level is available upon request. For more information, refer to the previous section–ADC Fraud Recovery—BIN Reports.

Fraud Recovery Billing Event Codes for Issuers

Upon completion of the FR process Mastercard credits issuers through MCBS. The credits appear on the weekly MCBS billing statement. Following are the detailed billing event codes associated with FR credits.

The following table shows ADC FR codes that appear on the MCBS statement.

Country/Region	MCBS Billing Event ID	MCBS Statement Description
Global (excluding Brazil)	2SC-CRD1214	US Credit (Issuer)
Brazil	2SC-CRD1214	Brazil Credit (Issuer)

Annual Fees

As of 1 January 2016, Mastercard no longer imposes an ADC Administrative Fee on issuers. Instead, Mastercard applies an Annual Service Fee on issuers as explained below:

- Issuers that choose to participate in the reimbursement component of the Mastercard ADC Program, will be assessed the determined service fee as shown in the table below.
- Issuers that choose not to participate in the reimbursement component of the ADC Program will not be assessed an annual service fee. As a reminder, issuers that Opt-Out will not receive any financial reimbursement through the ADC reimbursement program for that calendar year.

The Annual Service Fee will be based on the number of Mastercard issued accounts reported to Quarterly Mastercard Report (QMR) for the year prior. Mastercard will assess this fee at the Marketing Parent ICA level corresponding to the same method for issuer reimbursements.

Fees

The following table provides the Annual Service Fee for North America region.

Account Range Based on the QMR	Annual Opt-In Rate (USD)
0–400,000	2,500
400,001–700,000	5,000
700,001–3 million	20,000
3 million–10 million	30,000
10 million–20 million	75,000
More than 20 million	100,000

The following table provides the Annual Service Fee for the Europe region.

Account Range Based on the QMR	Annual Opt-In Rate (EUR)
0–400,000	500
400,001–700,000	1,000
700,001–3 million	4,000
3 million–10 million	6,000
10 million–20 million	15,000
More than 20 million	20,000

The following table presents the Annual Service Fee for all regions except for Europe and North America.

Account Range Based on the QMR	Annual Opt-In Rate (USD)
0–400,000	500
400,001–700,000	1,000
700,001–3 million	4,000
3 million–10 million	6,000
10 million–20 million	15,000
More than 20 million	20,000

Billing Events

The following Mastercard Consolidated Billing System (MCBS) billing event will apply for all regions except Europe region.

Billing Event	Billing Event Description	Service ID
2SC1218	ADC Recovery Program Service Fee	SC

The following Mastercard Consolidated Billing System (MCBS) billing event will apply for Europe.

Billing Event	Billing Event Description	Service ID
2KS6002	ADC Recovery Program Service Fee	KS

ADC Event Final Financial Responsibility Determination

Pursuant to Chapter 10 of the *Security Rules and Procedures*, upon completion of its investigation, if Mastercard determines that a customer bears financial responsibility for an ADC Event or Potential ADC Event, Mastercard will notify the responsible Customer of such determination and, either contemporaneous with such notification or thereafter, specify the amount of the customer's financial responsibility for the ADC Event or Potential ADC Event.

The responsible customer has thirty (30) calendar days from the date of such final notification of the amount of the customer's financial responsibility to submit a written appeal to Mastercard, together with any documentation and/or other information that the customer wishes Mastercard to consider in connection with the appeal. Only an appeal that both

contends that the Mastercard financial responsibility determination was not in accordance with the Standards and specifies with particularity the basis for such contention will be considered.

After review of the responsible customer's appeal, Mastercard will notify the responsible customer of the appeal resolution. If the appeal is denied, Mastercard will proceed with the normal debit process through the MCBS billing on the date specified in the appeal resolution notification. There is a USD 500 fee for each appeal processed.

Appendix A ADC Letter Templates

This appendix provides the template to use for writing a responsibility estimate letter, final responsibility letter and credit letter.

ADC Event Responsibility Estimate Letter

Mastercard sends an ADC Event Responsibility Estimate Letter to indicate that it has a preliminary and conditional estimate.

Franchise Integrity
Account Data Compromise
account_data_compromise@mastercard.com

Date

Acquirer Security Contact
Acquirer Company Name
Acquirer Address1
Acquirer State/ZIP
Acquirer Country

POTENTIAL ACCOUNT DATA COMPROMISE EVENT RESPONSIBILITY
MC ALERTS CASE #ADCNNNN-YY, MERCHANT NAME, ICA <<NNNN>>

Dear Security Contact:

Mastercard is currently investigating the above-referenced potential Account Data Compromise (ADC) Event. Mastercard will not comment further about this matter until the investigation is completed. However, as a courtesy to <<Acquirer Name>>, Mastercard has prepared a preliminary and conditional financial estimate of Operational Reimbursement (OR) and Fraud Recovery (FR). The OR and FR is based on the number of "at-risk" accounts published to date for this Event in Mastercard Alerts.

As the acquirer of record, Mastercard may determine that <<Acquirer Name>> is responsible for OR and/or FR. Any actual responsibility will be determined after the investigation concludes.

The current estimated OR and FR is as follows:

	Estimated Responsibility
Operational Reimbursement	$xxxx.xx
Fraud Recovery	$xxxx.xx
Total	$xxxx.xx

Again, please note that these are preliminary, conditional estimates only. Further, the estimate may be subject to a PCI-related Cap per Section 10.2.5.3 of the Mastercard *Security Rules and Procedures* Manual. This letter does not address other potential fees, assessments or the like that may relate to or arise in connection with the above referenced potential ADC Event. Mastercard values its relationship with <<Acquirer Name>> and is committed to enforcing data security standards for the protection of cardholder information throughout the transaction life cycle. We trust <<Acquirer Name>> supports our initiatives to ensure that all participants, including merchants, vendors, and processors, effectively safeguard and secure payment account data.

Mastercard 2000 Purchase Street Purchase, NY 10577-2509

Please respond to this communication if you believe this event qualifies for a deductible due to Hybrid POS terminal processing thresholds identified in Section 10.2.5.4 and 10.2.5.5 of the Mastercard *Security Rules and Procedures* Manual.

If you have any questions or require further clarification, please contact the Mastercard ADC Team at account_data_compromise@mastercard.com or your Mastercard Customer Fraud Management Representative.

Sincerely,

Mastercard Account Data Compromise

ADC Event Final Responsibility Letter

Mastercard sends a Final Responsibility Letter after an ADC investigation is complete to indicate financial responsibilities.

mastercard

Franchise Integrity
Account Data Compromise

account_data_compromise@mastercard.com

Date

Acquirer Security Contact
Acquirer Company Name
Acquirer Address1
Acquirer State/ZIP
Acquirer Country

ACCOUNT DATA COMPROMISE EVENT RESPONSIBILITY
MC ALERTS CASE #ADCNNNN-YY, MERCHANT NAME, ICA <NNNN>

Dear Security Contact:

This letter is to advise <<Acquirer Name>> that Mastercard has completed its investigation of the above-referenced account data compromise (ADC) event (the "Event") and has determined that an ADC event occurred at <<MERCHANT NAME>> for which <<Acquirer Name>> is responsible. A Customer found to be responsible for an ADC event also assumes certain financial responsibilities. For your convenience, these financial responsibilities are separately addressed below.

PCI Violations
Mastercard has determined that <<Acquirer Name>> is responsible for its merchant's violation of one or more requirement(s) of the PCI Data Security Standards. These requirements and Mastercard's findings are provided in the chart on page <<Page Number>>. For a more complete explanation of these requirements, please see Section 10.2.5.1 of the current edition of the Mastercard *Security Rules and Procedures* manual (the "Manual"). As set forth in therein, Mastercard may assess a Customer up to USD 100,000 for each violation of a requirement.

Mastercard has elected not to impose an assessment for such failure at this time subject to <<Acquirer Name>> completing both of the following:

1) Within 30 days complete and submit the attached Mastercard Site Data Protection Account Data Compromise Information Form and;

2) Within 60 days provide evidence in the form of the Attestation of Compliance (AOC), received from the Qualified Security Assessor (QSA), that the compromised entity has achieved full compliance with the *Payment Card Industry Data Security Standard* as set forth in Section 10.3.4.3 of the Manual.

Both documents should be returned via e-mail to pci_adc@mastercard.com.

Mastercard 2000 Purchase Street Purchase, NY 10577-2509

Should <<Acquirer Name>> fail to file the Mastercard Site Data Protection Account Data Compromise Information Form <<dd-mm-yy>> and/or submit to Mastercard an AOC by <<dd-mm-yy>>, Mastercard reserves the right to assess <<Acquirer Name>> for failure to comply with the SDP and/or Mastercard ADC Program requirements.

If you have questions about satisfying the SDP Program and the PCI DSS requirements referenced above, contact sdp@mastercard.com.

Operational Reimbursement and Fraud Recovery
As set forth in Section 10.2.5.3 of the Manual, <<Acquirer Name>> is responsible for ADC Operational Reimbursement and ADC Fraud Recovery in the following amounts:

Item Description	Item Total
ADC Operational Reimbursement	$xxxx.xx
ADC Fraud Recovery	$xxxx.xx
Total	$xxxx.xx

For your convenience, attached to this letter is additional information pertaining to ADC Operational Reimbursement and ADC Fraud Recovery associated with this Event.

Conclusion
Please be advised that, on <<dd-mm-yy>>, <<Acquirer Name>>, ICA <nnnn> will be debited for the above-cited financial liabilities totaling <$xxxx.xx> via the Mastercard Consolidated Billing Services system. Mastercard reserves the right to re-open its investigation of the Event should Mastercard deem it necessary or appropriate to do so. We value our relationship with <<Acquirer Name>> and know that you share our view of the importance of account data security.

Please respond to this communication if you believe this event qualifies for a deductible due to Hybrid POS terminal processing thresholds identified in Section 10.2.5.4 and 10.2.5.5 of the Manual.

If you have any questions or require further clarification, please contact the Mastercard ADC Team at account_data_compromise@mastercard.com or your Mastercard Customer Fraud Management Representative.

Sincerely,

Mastercard Account Data Compromise

Issuer Credit Letter

Mastercard sends an Issuer Credit Letter after an ADC investigation is complete to indicate recovery amounts to be credited.

mastercard

Franchise Integrity
Account Data Compromise

account_data_compromise@mastercard.com

Date

Issuer Security Contact
Issuer Company Name
Issuer Address1
Issuer State/ZIP
Issuer Country

ACCOUNT DATA COMPROMISE (ADC) – MASTERCARD ALERTS CASE #ADC CaseNo.
ISSUER OPERATIONAL REIMBURSEMENT AND/OR FRAUD LOSS RECOVERY

Dear Security Contact:

In accordance with Mastercard Standards, and more particularly the Account Data Protection Standards and Programs set forth in chapter 10 of the Mastercard *Security Rules and Procedures* manual, this notice sets forth the ADC Operational Reimbursement and ADC Fraud recovery amounts to be credited to and debited from Guaranty Bank & Trust Company via Mastercard Billing System (MCBS) account on MCBS Delivery Date.

Operational Reimbursement calculated [Calculation Date]

Description	Billing Event	Total
Net Operational Reimbursement	$netORAmtLbl	$totalORAmt
Operational Reimbursement Administration Fee	$mcORAdmFeeLbl	$mcORAdminFee

Card Types								
Tier	**Mag Stripe**		Chip		PayPass		Combo	
	Number	**Rate**	Number	Rate	Number	Rate	Number	Rate
$tierCode	$msNo	$msRt	$cpRt	$cpNo	$ppNo	$ppRt	$cbNo	$cbRt

Gross Eligible Reimbursement Amount	$gross
Deductible	$stdDeductible
Net Eligible Reimbursement Amount	$newfield3
Cap Applied	$orCapApplied
MC Admin Fee	$mcORAdmin
Total Operational Reimbursement	**$totalORAmtNum**

Mastercard 2000 Purchase Street Purchase, NY 10577-2509

Fraud Recovery calculated [Calculation Date]

Description	Billing Event	Total
Net Fraud Recovery	NA	NA
Fraud Recovery Administration Fee	NA	NA

Incremental Fraud for Case	$IncrFRAmt
# of Accounts in Previous Alerts	$totDpAccCt
Fraud Associated with Previous Alerts	$dpFdAmt
Eligible Fraud Recovery Amount	$totFDRecAmt
Deductible	$calCBTotAmt
Net Eligible Fraud Recovery Amount	$netEgFRAmt
Cap Applied	$frCapApplied
MC Admin Fee	$netEGFRA
Total Fraud Recovery	**$totFRAmtNum**

The Mastercard ADC rules section 10.2.5.3 states "When determining financial responsibility, Mastercard may take into consideration the compromised entity's PCI level (as set forth in section 10.3.4), annual sales volume, and the factors set forth in section 10.2.5.2." If a PCI cap applies to this case, the reduction in reimbursement is already taken from the Operational Reimbursement and Fraud Recovery totals stated above.
For more information regarding the ADC Operational Reimbursement or the Fraud Loss Recovery Standards and calculation methodologies please see:

- Mastercard Security Rules and Procedures Manual - Section 10.2.5.3; and
- Mastercard Account Data Compromise User Guide – Chapter 6 and 7

The above documentation can be found on Mastercard Online through the Manuals and Publications web page.

If you have any questions regarding this reimbursement, you may contact your Customer and Security Risk Services representative, or the Customer Operations Support team at one of the following phone numbers.

1-800-999-0363 (in Canada and U.S. regions)
1-636-722-6176
1-636-722-6292 (Spanish language support)

Sincerely,

Mastercard Account Data Compromise

Appendix B ADC Program Resources

This appendix provides information and data requirements the ADC program needs for the accurate submission and maintenance of customer, merchant, or third party service provider data for aspects of the ADC process.

Applications of the Member Information Online to an ADC Event

The *Mastercard Information Manual* presents multiple uses to customers when handling an ADC Event or Potential ADC Event.

The Member Information Online contains customer contact information which is the responsibility of the customer to keep the contact information updated.

The operational reimbursement and fraud recovery applications use the Member Information Online through Mastercard Connect™ to obtain the contact information that is used to communicate with affected issuers and acquirers when communicating details pertaining to an ADC Event or Potential ADC Event. Customers must perform a periodic review and update of the Principal Contact and Security Contact name, address, email address, and phone number.

For questions concerning the access and update of ICA number profile in the Member Information Online, please contact the Customer Operations Services team, Technical Account Manager, or Regional Security Representative.

Applications of QMR to an ADC Event

Quarterly Mastercard Reporting (QMR) presents multiple uses to customers when handling an ADC Event or Potential ADC Event.

Mastercard, Cirrus, or Maestro principal customers are required to report performance data to Mastercard on a quarterly basis. Reporting is done through online forms that can be found in the Mastercard Connect™ portal, QMR Direct.

The Operational Reimbursement program uses data each issuer provides through the QMR to determine the issuing volume for each ICA. The issuer volume is used to associate the issuer with a specific card reimbursement cost when accounts are compromised.

Additionally, QMR reported accounts are utilized to determine the Annual Service Fee for issuers that elect to participate in the ADC Program.

Applications of the Mastercard Registration Program to an ADC Event

The Mastercard Registration Program (MRP) is a mandatory program that requires customers to register entities that provide program services to the customer and certain types of merchants.

Refer to Chapter 9 of the Mastercard *Security Rules and Procedures* manual for more information regarding the MRP.

Applications of SAFE to an ADC Event

The System to Avoid Fraud Effectively (SAFE) is a useful tool to customers when handling an ADC Event or Potential ADC Event.

SAFE is a database that maintains a repository of fraudulent transactions with fraud types submitted by issuers. Mastercard requires issuers to report to SAFE, at the customer ID level, all Mastercard transactions that the issuer considers to be fraudulent. Refer to the *SAFE Products User Guide*, available on Mastercard Connect's Security/Risk Services webpage for more information.

Applications of Mastercard Connect to an ADC Event

Mastercard Connect is a useful tool to customers when handling an ADC Event or Potential ADC Event.

Mastercard Connect™ is the Mastercard information portal (communication delivery platform) for delivering business tools and secure communications capabilities to customers worldwide. Core services and various PC-based tools are available through Mastercard Connect™.

Customers must register for access to Mastercard Connect™ to use the Manage My Fraud and Risk Programs application. Mastercard Connect™ registration is free by navigating the internet browser to www.mastercardconnect.com and selecting the **Enroll Now** link to begin the registration process.

Applications of Manage My Fraud and Risk Programs to an ADC Event

The Manage My Fraud and Risk Programs application is a useful tool to customers when handling an ADC Event or Potential ADC Event.

Manage My Fraud and Risk Programs is a product available on Mastercard Connect™ that serves as the distribution method for an ADC Event or potential ADC Event, and permits issuers and acquirers to submit requests for Account Data Compromise (ADC) investigations.

For questions regarding the Manage My Fraud and Risk Programs application, contact the Global Customer Service team or your Regional Customer Security and Risk Services representative.

Appendix C Manage My Fraud and Risk Programs ADC Reporting Form Status Codes

This appendix explains the ADC Reporting Form status codes used in the ADC Summary.

Overview—Manage My Fraud and Risk Programs ADC Reporting Form Status Codes

To review the status of any reported ADC Event or Potential ADC Event, the customer must navigate to the Manage My Fraud and Risk Programs application on Mastercard Connect™ and select the "My Work" tab.

The Project Status designates one of the following classifications:

- Draft

  Indicates that the data entered in the ADC Reporting Form was saved but not submitted to Mastercard; often this occurs when required information in the ADC Reporting Form is not present or complete.

- Submitted to Mastercard for review

  Indicates the issuer or acquirer has completed the ADC Reporting Form and it has been submitted for Mastercard review.

- Cancelled

  Indicates the data entered in the ADC Reporting Form was not saved, and no information will be submitted to Mastercard.

- Completed

  Indicates that the investigation request has been reviewed and that no further investigation will be conducted.

Appendix D Mastercard ADC Dissemination Text File Format Legend

Field	Start Position	Length	Description	Example
Primary Account Number (PAN)	1	20	numeric, trailing spaces	67000000000000000000
Expiration Date	21	5	YYMM, numeric, trailing space	1012
Case Number	26	20	alphanumeric, trailing space	MCA1234-SAMEA-10-99
Alert Date	46	9	YYYYMMDD, numeric, date of the alert	20100322
Issuing ICA	55	11	The issuing ICA of the compromised PAN	1001
Data Elements (at-risk)	66	24	numeric, contains leading zero, trailing space	01 02 03
At-Risk Time Frame Start	90	9	YYYYMMDD for the time frame (beginning date), trailing space	20100312
At-Risk Time Frame End	99	9	YYYYMMDD for the time frame (ending date) trailing space	20100312
Case Type	108	3	numeric, contains leading zero, trailing space	01
Financial Network Code	111	4	alphanumeric, a three-character code identifies the type of card product, trailing space	MIS
Fraud Indicator	115	3	numeric, contains leading zero, two digit fraud indicator, trailing space,01 is high fraud risk, 02 is moderate fraud risk, 03 is low fraud risk, 04 is not applicable (NA)	01
Previous Alert (1)	118	2	alphanumeric, indicator Y or N informing if PAN has been in a prior alert, trailing space	Y
Previous Case Number (1)	120	20	alphanumeric, trailing space	MCA1234-SAMEA-10-98
Previous Alert Date (1)	140	9	YYYYMMDD for prior alert date	20100321
Previous Data Elements (at-risk) (1)	149	24	numeric, contains leading zero, trailing space	01 02
Previous Case Type (1)	173	3	numeric, contains leading zero, trailing space	03
Previous Case Number (2)	176	20	alphanumeric, trailing space	MCA1234-SAMEA-10-97
Previous Alert Date (2)	196	9	YYYYMMDD for prior alert date	20100320
Previous Data Elements (at-risk) (2)	205	24	numeric, contains leading zero, trailing space	01 03
Previous Case Type (2)	229	3	numeric, contains leading zero, trailing space	02
Previous Case Number (3)	232	20	alphanumeric, trailing space	MCA1234-SAMEA-10-96
Previous Alert Date (3)	252	9	YYYYMMDD for prior alert date	20100320
Previous Data Elements (at-risk) (3)	261	24	numeric, contains leading zero, trailing space	05
Previous Case Type (3)	285	3	numeric, contains leading zero, trailing space	01
Linked/Associated Case Number	288	Variable	alphanumeric	ADC-0230-11

Appendix E Manage My Fraud and Risk Programs and ADC Reporting Form Field Definitions

This appendix provides a list of fields on Section A, Page 1 of the ADC Form and their descriptions.

ADC Reporting Form—Issuer View—Field Descriptions

The following is a list of fields on the ADC Reporting Form—Issuer View and their descriptions.

Contributor Contact Information	
Field Title	**Field Description**
Do you want to override the contact information?	The Manage My Fraud and Risk Programs application automatically populates this field with the name of the user logged into the application as it appears in his or her Mastercard Connect profile. If the user selects No, they will be prompted to enter the contact Name, Email, and Phone for the event.
Potentially Compromised Entity Description Information	
Entity Name	Enter the partial or full name of the potentially compromised entity.
City	Enter the partial or full name of the known city
Street Address	Enter the partial or full street address, if known
Country	Enter the known country
State	If applicable, select the state
Expected Entity Not Returned	If the entity search yields no results, enter the fields of the merchant or potential ADC event being reported

All required fields are denoted with an asterisk within the ADC Reporting Form.

Potentially Compromised Entity Description Information	
Do you know the suspected At-Risk time frame?	If known, enter the suspected time frame of compromise. The From Date and To Date can be selected through a pop-up calendar by clicking the calendar icon next to the field.
Total fraud loss (USD) to date for affected account numbers	Enter either the known total fraud losses in USD to date for the accounts being provided or the total population of affected accounts. These fraud losses should already have been reported to SAFE. If unknown, enter zero and indicate this information in the contributor comments section of the form.
Suspected compromise type	Select the suspected compromise type for the affected entity. Hold down the shift button to select more than one if known. If suspected compromise does not appear on the list, select Other and enter the compromise type.

Type of Fraud	If available, enter the type of fraud transactions (such as counterfeit or card not present) that were submitted to SAFE for this case. Hold down the shift button to select more than one type of fraud. If type of fraud does not appear on the list, select Other and enter the type of fraud.
Contributor Comments	Enter additional information or clarification for the merchant or potential ADC event being reported.
Attachments	Mastercard requires issuers to submit a minimum of 10 Mastercard accounts using the "Compromised Accts" Attachment Category upon initial submission of a potential ADC event. Additional files can be submitted in addition to the compromised account information to assist with the investigation.

One of the following options may be chosen when you have finished the ADC Reporting Form.

Potentially Compromised Entity Description Information	
Cancel	Erases all information and attachments from the system with a record of the tracking number. The project status and former ADC Reporting Form ID number show as "Cancelled" in the Completed work tab.
Save as Draft	Saves the entered information and attachments but does not release the report to Mastercard. The project status and ADC Reporting Form ID number remain as "Draft" in your "My Work" tab along with the Start Date.
Submit	Submits the report to Mastercard. The user can view the report in the "My Work" tab. The Project Status appears as "Submitted to MC for Review."

NOTE: If you leave the ADC reporting form input page for any reason, click Save as Draft at the bottom of the page to ensure that your information is saved.

NOTE: The ADC Reprint Form is location-specific. If a multi-location entity chain or franchise is reported, a specific location must be provided in the Potentially Compromised Entity Description Information fields. Additional clarification can be added to the Contributor comments within the ADC Reporting Form.

ADC Reporting Form—Acquirer View—Field Descriptions

The following is a list of fields on the ADC Reporting Form—Acquirer View and their descriptions.

NOTE: Only information on the Entity Details tab is required. All other tabs can be filled out with known information, but not required for submission to Mastercard for review.

Contributor Contact Information	
Field Title	**Field Description**
Contributor Name	Enter the user name
Contributor Phone	Enter user phone number
Potentially Compromised Entity Description Information	
Entity Name	Enter the partial or full name of the potentially compromised entity.
City	Enter the partial or full name of the known city
Street Address	Enter the partial or full street address, if known
Country	Enter the known country
State	If applicable, select the state
Expected Entity Not Returned	If the entity search yields no results, enter the fields of the merchant or potential ADC event being reported

All required fields are denoted with an asterisk within the ADC Reporting Form.

Potentially Compromised Entity Description Information	
Is entity part of a franchise?	If known, enter the merchant ID(s)
Terminal ID(s)	If known, enter the Terminal ID(s) in which counterfeit transactions may have occurred
POS mode used at terminal	If known, enter the POS mode used at affected terminal
MCC Code	Enter category code of merchant (if known)
Acquired Date	Enter entity acquired date. If unknown, enter current date and elaborate in comments section of the E-Commerce Details tab.

Attachments	Acquirers can submit Mastercard accounts using the "At Risk Accounts" Attachment Category upon initial submission of a potential ADC event. Additional files can be submitted in addition to the at-risk account information to assist with the investigation by uploading files with the corresponding Attachment Category type.

An acquirer may fill out the additional tabs within the reporting form, but they are not required for submission of the ADC Reporting Form. They do assist Mastercard in obtaining additional information about a potentially compromised entity.

Registration Details–MRP Information

- Is the entity registered with the MRP program?
- Does the entity use a TPP or ISO?
- Does the entity use a DSE?
- Was the entity terminated?
- Number of Mastercard annual incoming credit/debit/POS PIN/ATM transactions
- PCI Level
- SDP Status
- SDP date validate to
- PCI QFI that certified

Compromise Details–Potential Compromise Description Information

- First known date of ADC
- Method of discovery
- POS entry modes used for at-risk transactions
- Data elements processed
- Has the entity been previously suspected as being compromised?

Investigation Details

- Individuals involved
- Number of Mastercard at-risk accounts
- Investigation details
- Investigation findings that address skimming/terminal tampering
- Data elements at-risk due to compromise or vulnerabilities
- Suspected At-Risk Time Frame (Beginning date/Ending date)
- Comments on suspected at-risk time frame

Network Details–Network and Payment Application Description Information

- POS software name
- POS software version

- Date of POS software install
- Date of software update(s)
- Data elements stored
- Remediation efforts taken
- Remediation efforts taken
- Remediation dates
- Does the entity have remote access connectivity?
- URLs involved in compromise

E-Commerce Details–Entity Information

- Is entity an e-commerce entity?
- Other information
- Was law enforcement notified?
- Comments

One of the following options may be chosen when you have finished the ADC Reporting Form.

Potentially Compromised Entity Description Information	
Cancel	Erases all information and attachments from the system with a record of the tracking number. The project status and former ADC Reporting Form ID number show as "Cancelled" in the Completed work tab.
Save as Draft	Saves the entered information and attachments but does not release the report to Mastercard. The project status and ADC Reporting Form ID number remain as "Draft" in your "My Work" tab along with the Start Date.
Submit	Submits the report to Mastercard. The user can view the report in the "My Work" tab. The Project Status appears as "Submitted to MC for Review."

NOTE: If you leave the ADC reporting form input page for any reason, click Save as Draft at the bottom of the page to ensure that your information is saved.

NOTE: The ADC Reprint Form is location-specific. If a multi-location entity chain or franchise is reported, a specific location must be provided in the Potentially Compromised Entity Description Information fields. Additional clarification can be added to the Contributor comments within the ADC Reporting Form.

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.