Account Data Compromise User Guide

04 February 2016

ADC

Summary of Changes, 4 February 2016

This document pertains to ADC Events in which the first ADC Alert is published on or after 1 January 2016. For ADC Events in which the first ADC Alert is published prior to 1 January 2016, the 15 January 2014 publication of this manual will apply and is available upon request. For a copy of the 15 January 2014 publication of this manual, please send an email to 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
Chapter 2: Reporting an ADC Event or Potential ADC Event	
Added the following sentence to Overview of the Reporting of an ADC Event or Potential ADC Event- • Multiple instances of remote access tools present on systems in an "always on" mode. • Notifications from Issuers or cardholders related to cardholder complaints and chargebacks.	Overview of the Reporting of an ADC Event or Potential ADC Event
Updated ADC Event Reporting Using Manage My Fraud and Risk Programs as follows: • Changed “Users may” to “A customer must” • Added sentence to read: “A responsible customer must report an ADC Event within 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.”	ADC Event Reporting Using Manage My Fraud and Risk Programs

Description of Change	Where to Look
Updated ADC Reporting Form - General Instructions • Added "All required fields marked with an asterisk must be completed to advance the ADC reporting form." • Removed information about "For definitions of the fields on this form, refer to Manage My Fraud and Risk Programs and ADC Reporting Form Field Defination, Documents may be attached to the ADC Reporting Form by clicking gNew, then clicking Attach a File and following the instructions at the bottom of hte form." • Removed "An ADC Incident Report may be attached to the ADC Reporting Form when an Acquirer makes the initial report of an ADC Event or Potential ADC Event. Attach any additional documents that more fuly describe the scope and nature of the ADC Event, such as a forensic report or other description of the ADC Event or Potential ADC Event and its impact. The attachment feature is furhter explained in the Attachments - General Instructions section." • Updated "Issuer View - ADC Reporting form" to "ADC Reporting form" • Updated screenshots • Updated "Repeat this process for up to three additional files" to Repeat this process for additional files". • Added "unique" to the sentence to read: 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 • Added "csv, xls or xlsx" to the sentence to read: All account files must be submitted in either text, csv, xls or xlsx format and must contain at least 10 valid accounts for review by MasterCard • Removed "If the file does not meet validation requirements, customers will also receive an e-mail notification with instructions on how to resubmit their account file via the Manage My Fraud and Risk Programs application."	General Instructions
Updated ADC Event Reporting without the Use of Manage My Fraud and Risk Programs as follows: • Removed "Encrypted File Transfer Method" • Updated "File Transfer Method" to "PGP Encrypted File" • Updated "Encrypted File Transfer" to "PGP Encrypted File"	ADC Event Reporting without the Use of Manage My Fraud and Risk Programs
Chapter 3 - Investigation of an ADC Event or a Potential ADC Event	
Added "Each ICA must have at least two users register for use of the application"	Investigation of an ADC Event or a Potential ADC Event
Chapter 5 -SAFE Reporting	

Description of Change	Where to Look
Added the following to Overview of SAFE Reporting topic • or be included in that Event's calculation	SAFE Reporting
Added two topics: • Known At-Risk Time Frame • Unknown At-Risk Time Frame	• Known AT-Risk Time Frame • Unknown At-Risk Time Frame
Chapter 6 - Operational Reimbursement and Fraud Recovery Calculation	
Updated ADC Operational Reimbursement Factors - ADC Case Eligibility for OR/FR with the following: • Updated "ADC" to "FR" • Updated footnote	ADC Case Eligibility for OR/FR
Updated ADC Operational Reimbursement Factors topic - ADC Operational Reimbursement as follows: • Added a new column "DE 35/45 (Track 2 Date - Service Code)" • Updated row Magnetic Stripe and Chip row with "2xx or 6xx" • Updated ADC OR calculations performed to Events opened • Updated from 40% to 10% • Removed "Chip, and MasterCard Contactless. For additional information refer to section 10.2.5.3 of the MasterCard Security Rules and Procedures manual"	ADC Operational Reimbursement
Updated ADC Operational Reimbursement - ADC Operation Reimbursement with the following: • Added "based on the issuers that have opted in to the ADC program for the year the event occurred" • Updated "Amount USD" to "PayPass USD" • Added note • Updated Appendix	ADC Operation Reimbursement
Updated ADC Operational Reimbursement—Customer Responsibility Cap with the following: • Updated from ADC Fraud Recovery (FR) to Operational Reimbursement (OR)	ADC Operational Reimbursement - Customer Responsibility Cap
Added two sections "Known At-Risk Time Frame" and "Unknown At-Risk Time Frame" to ADC Fraud Recovery Factors topic	ADC Fraud Recovery Factors

Description of Change	Where to Look
Updated Chargeback deductions section with the following: • Removed "Effective on cases added on or after 1 December 2014, the deduction will be reduced to five percent" • Updated from "forty" to "five"	ADC Fraud Recovery Factors - Changeback Deductions
Added footnote to the section EMV Liability Shift Impact	
Added note to Fraud Recovery - BIN Reports	Fraud Recovery - BIN Reports
Chapter 7 - Event Financial Settlement of ADC Events	
Updated ADC Event Financial Settlement Information topic with the following: • Updated from "four" to "several" • Updated the sentence to read: 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.	ADC Event Financial Settlement Information
Updated ADC Event Financial Settlement Information for Issuers topic with the following: • Added "The notifications are sent to the Security Contact of the Parent ICA as listed in the Member Information Manual application at the time of the Event"	ADC Event Financial Settlement Information
Updated ADC Event Final Financial Responsibility Determination with the following: • Added "There is a USD 500 fee for each appeal processed"	ADC Event Final Financial Responsibility Determination
Appendix A - ADC Letter Templates	
Updated screen shots for the following letters: • ADC Event Responsibility Estimate Letter • ADC Event Responsibility Final Letter • Issuer Credit Letter	• ADC Event Responsibility Estimate Letter • ADC Event Responsibility Final Letter • Issuer Credit Letter

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 Customer Operations Team.

account_data_compromise@mastercard.com

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.

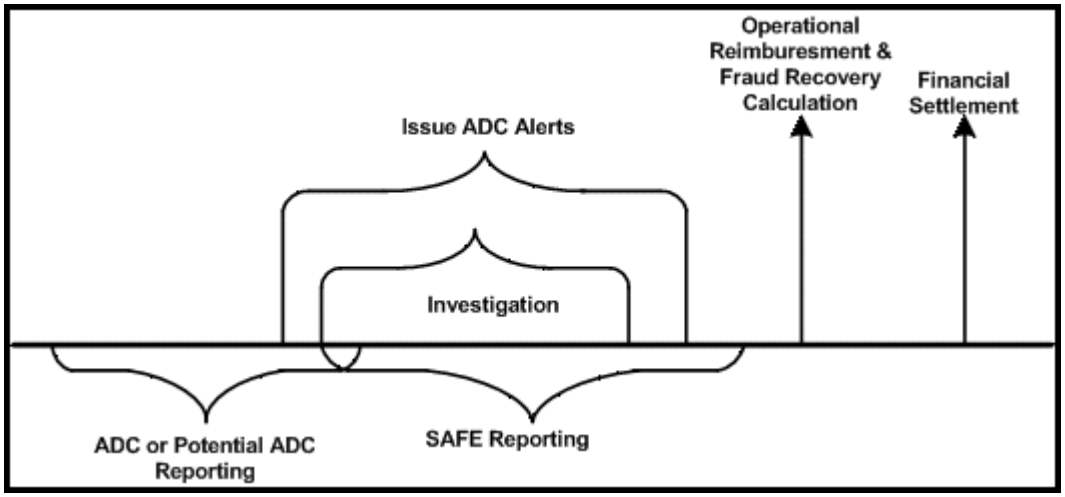
The MasterCard Standards relating to ADC Events or Potential ADC Events are set forth in section 10.2, Account Data Compromise Events, of the *Security Rules and Procedures* manual.

As defined in the MasterCard *Security Rules and Procedures* section 10.2 an "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 set forth below 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. In fact, MasterCard retains discretion to act (or not act) other than in accordance with this user guide.



Account Data Compromise User Guide Contact Information

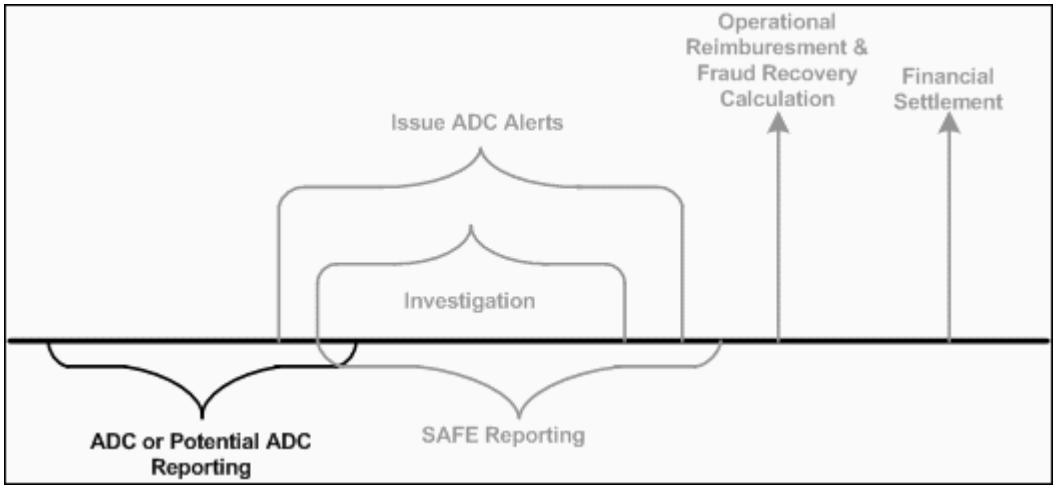
For contact information, refer to the Information Available Online section of the Notices page of this document.

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. ADC Events can include, but are not limited to, the following:

- Internet connections originating from non–business-related IP addresses[4]; 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

[4] 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 MasterCard Security Rules and Procedures section 10.2.2, 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 MasterCard *Security Rules and Procedures*, section 10.2.

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
- A responsible customer must report an ADC Event within 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 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 ADC Reporting Form 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 MasterCard User ID and authentication method.
3. From the top of the MasterCard Connect™ home page, click **Applications**, and then click **Manage My Fraud and Risk Programs**.
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 Member ID will be automatically populated on the Welcome screen. Customers will see their institution name, along with provisioned selections for their Member 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 Manage My Fraud and Risk Programs and ADC Reporting Form Field Definitions.

General Instructions

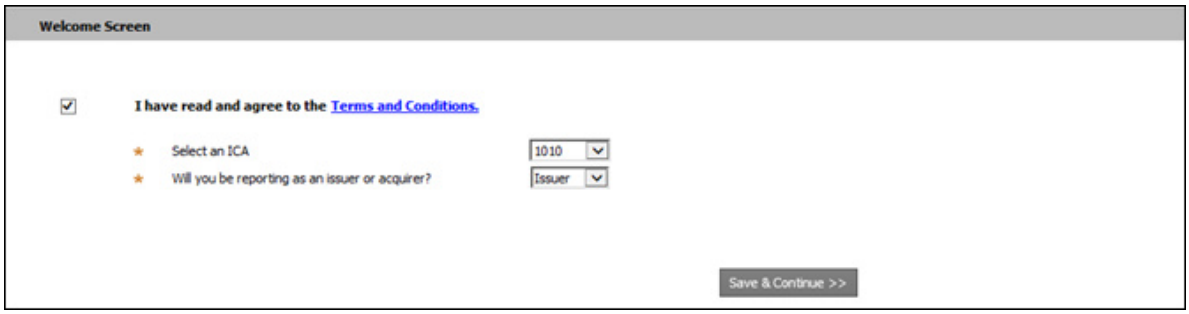
The user must complete all required fields in the ADC Reporting Form. All required fields marked with an asterisk must be completed to advance the ADC reporting form.

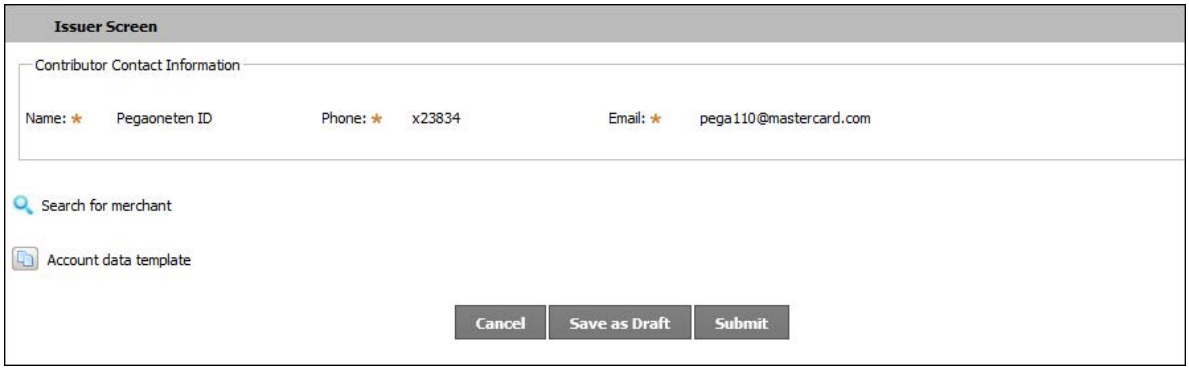
If the information is unknown, and not a required field, it may be left blank. If a required integer value is unknown, enter the number zero. If the required data element or date is unknown about the ADC Event being reported, select (none) or enter today's date by default. Required text fields that are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

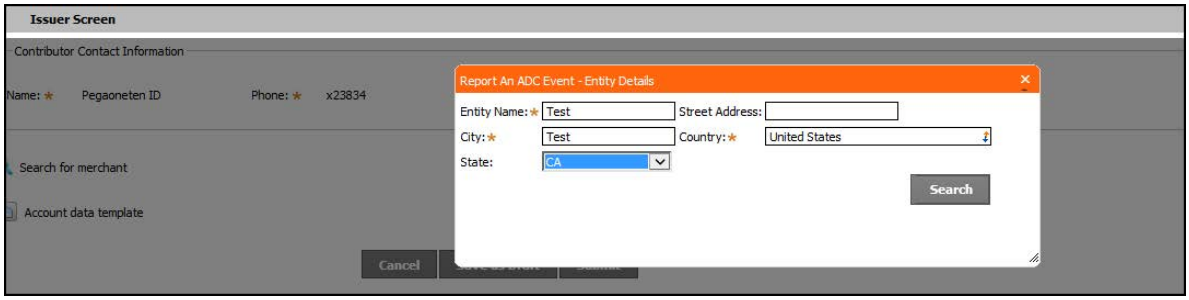
The following are illustrations of the ADC Reporting Form for both an Issuer and Acquirer view within the Manage My Fraud and Risk Programs application.

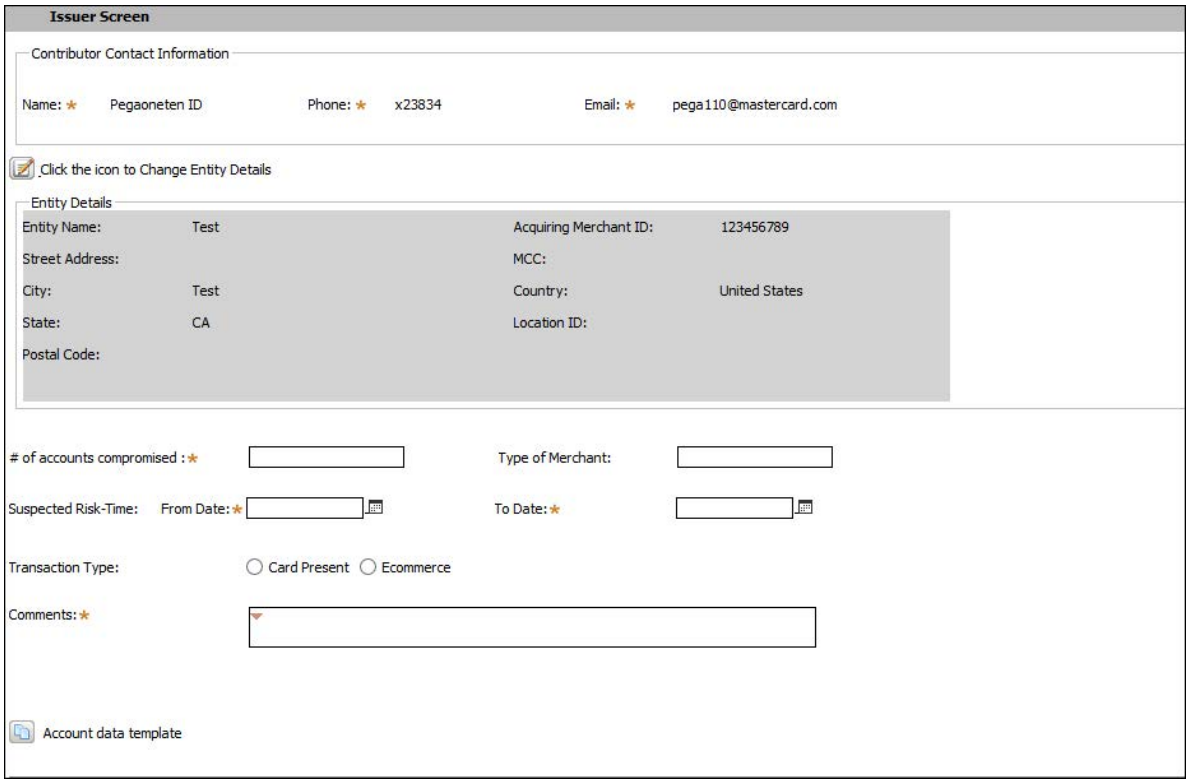
NOTE: Issuers are required to report actual fraudulent transactions to the System to Avoid Fraud Effectively (SAFE).

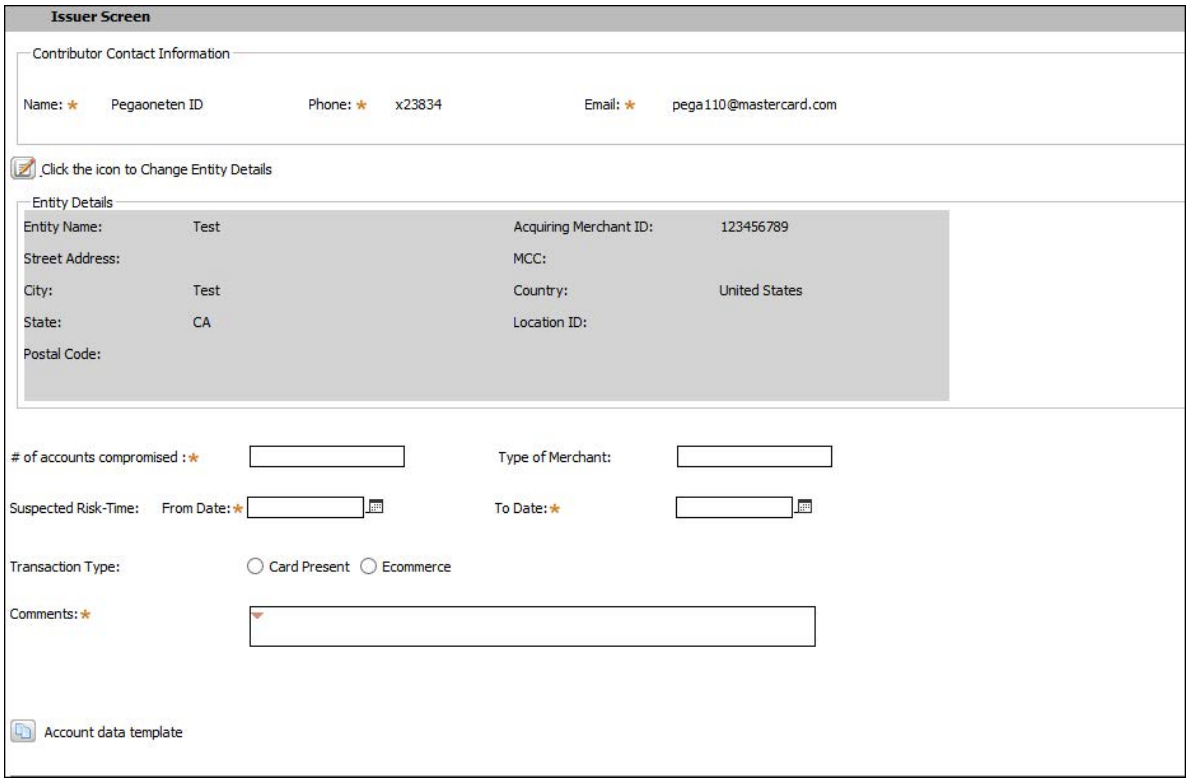
ADC Reporting form







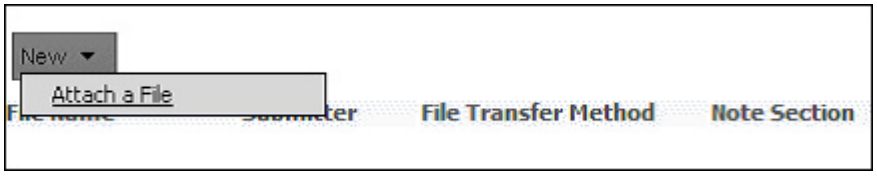




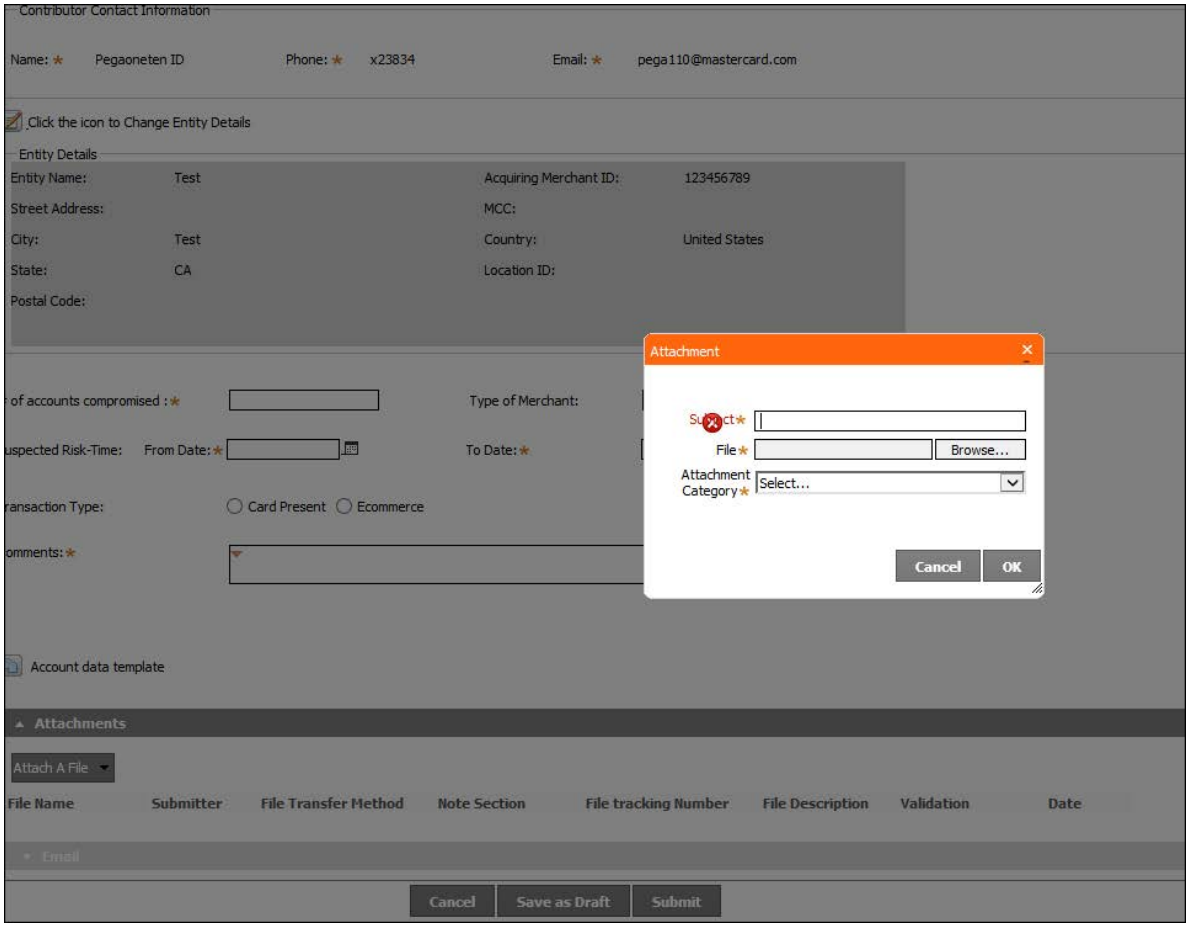
Attachments—General Instructions

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 on the **Browse** button. 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 the Attachments tab 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 Accts" 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 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 using either the Manage My Fraud and Risk Programs application or the Secure Upload product.

All account files must be submitted in either text, csv, xls or xlsx format and must contain at least 10 valid accounts for review by MasterCard. Customers that do not submit a file that meets the validation requirements will be sent an email asking to resubmit the account file with the proper requirements.

Customers will receive an e-mail 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 mailto: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 Incident Report form may be submitted to MasterCard using one of the following methods.

- Secure Upload
- Secure Upload—URL and password (available only to MasterCard Connect™ non-customers)
- 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. MasterCard will accept all submissions regardless of the format used, and MasterCard will reformat any file not submitted appropriately.

Secure Upload

The Secure Upload product allows for the secure file transfer of compromise information through a secure MasterCard Web site.

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.

MasterCard will provide temporary access for non-customers to Secure Upload for the secure transmission of compromised accounts. Refer to Secure Upload Access for Non-customers for directions about how non-customers can access Secure Upload.

Secure Upload Access for Non-Customers

A non-customer that needs to submit account data to MasterCard can do so through Secure Upload using a URL and password.

To obtain access to Secure Upload, send an email message to mastercard_alerts_administrator@mastercard.com. Include the following information in your email message:

- Case number or potentially compromised entity name
- User's contact information (name, title, organization, address, city, state, email address, and phone number)

PGP Encrypted File

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

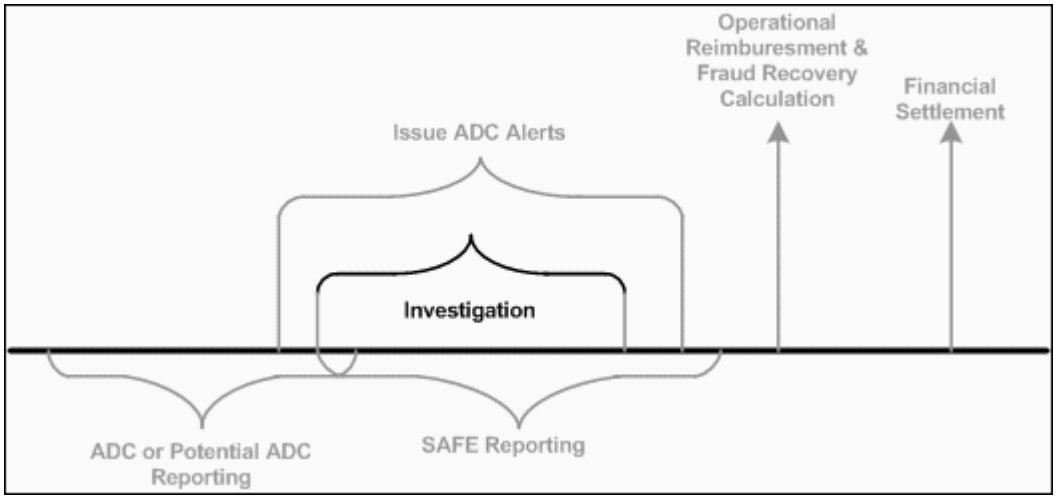
Send all encrypted files to account_data_compromise@mastercard.com.

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 section 10.2.2 of the 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 commenced 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 Merchant Acquirer 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 must engage a PCI Forensic Investigator (PFI).

For the process of engaging a PFI to conduct a forensic investigation, refer to the *Security Rules and Procedures* manual, section 10.2.2.

MasterCard *Security Rules and Procedures* manual, section 10.2.2.1 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 report may dramatically change from one calculation to another.

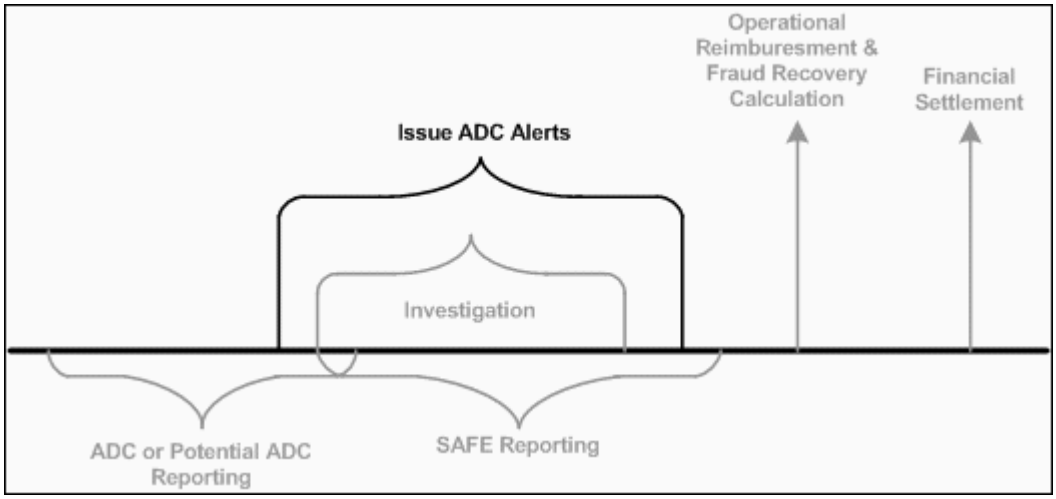
The customer may request to have the estimate re-calculated at any time during the investigation by emailing the Account Data Compromise Help Desk at account_data_compromise@mastercard.com.

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

This chapter describes how to view MasterCard ADC Alerts via Manage My Risk and Fraud.

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. To be eligible for Operational Reimbursement (OR) and Fraud Recovery (FR), as described in section 10.2.4.3 in the MasterCard *Security Rules and Procedures*, a customer must have and maintain an active Manage My Fraud and Risk Programs license for all of its member IDs/ICA numbers.

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.

Notification of Compromised Accounts Using Manage My Fraud and Risk Programs

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.

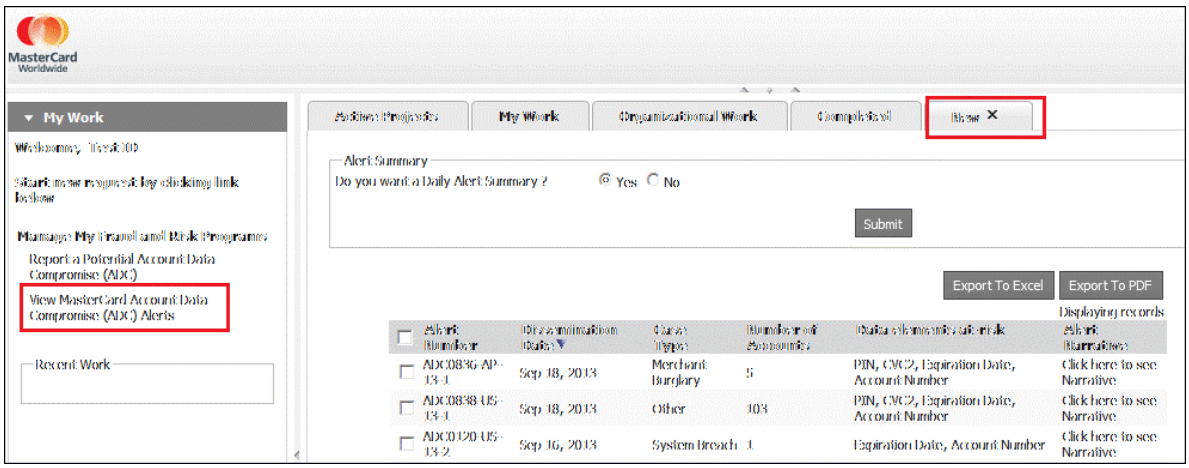
MasterCard may also notify by email or otherwise of an ADC Alert. The notification instructs the issuer to log on to Manage My Fraud and Risk Programs to obtain a list of at-risk accounts and may include information about the ADC Event or Potential ADC Event.

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 Applications, 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.
5. 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.
6. Customers can select one or more Alert Numbers to view in either .txt or .csv format by checking the box and select "Retrieve Alerts.



NOTE: If more than one Alert is selected for download, a user may have to wait up to two minutes for the file to be processed and receive a pop-up message indicating the download request has been initiated.

The .txt file option will only provide the primary account number (PAN) data, while the .csv option will provide several additional supplemental data fields with varying lengths and start positions.

If a user is to download Alert data in .csv file format, this information must be imported into Microsoft Excel in order to view the account numbers without truncation. Please refer to the Manage My Fraud and Risk Programs Dissemination File Format and Field Definitions section for additional information on supplemental data fields and .csv importing instructions.

Data within these columns can be sorted in ascending or descending order by clicking on the column headers. The **Export to Excel** or **Export to PDF** buttons will export a list of all Alerts viewable within the Manage My Fraud and Risk Programs Product to either Excel or PDF format.

The Daily Alert Summary Preferences button allows users to specify a Yes/No toggle to receive a nightly email communication of all Alerts impacting their provisioned accounts.

Manage My Fraud and Risk Programs Quarterly Fees

MasterCard assesses a quarterly license fee at the (Parent) customer ID/ICA number level through MCBS for access to Manage My Fraud and Risk Program. 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 preceding 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.

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 the Brazil region.

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
2SC1357	MC Alerts licensing fee—USD
2KS13575	MC Alerts licensing fee—Euros
2SC1357	MC Alerts licensing fee—Reals

Updating a Manage My Fraud and Risk Programs User Profile

A new customer has 30 calendar days from the initial date of membership to obtain a license.

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

To delete their MasterCard Connect™ user profile, the customer must complete a termination request on MasterCard Connect™, add or delete ICAs, or terminate their 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

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

MasterCard will notify a non-compliant customer with an e-mail notification to the Principal Contact and Security Contact listed in the *MasterCard Information Manual* (MIM) noting the non-compliance and potential for assessment if not registered within 30 days of the e-mail notification. Two users from each ICA must be registered to remain in compliance. 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
Customer 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 compliance" is the date that an email notice is sent to the Principal (Parent) Contact and Security Contact of the customer listed in the most recent edition of the MasterCard MIM MasterCard Connect™ profile. The customer is responsible for ensuring the accuracy of contacts listed in the MIM. To change, delete, or add people, email Customer Support at customer_support@mastercard.com for assistance.

Requesting a Manage My Fraud and Risk Programs License

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

MasterCard requires that every ICA number have 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 Customer Operations Support (COS) team.

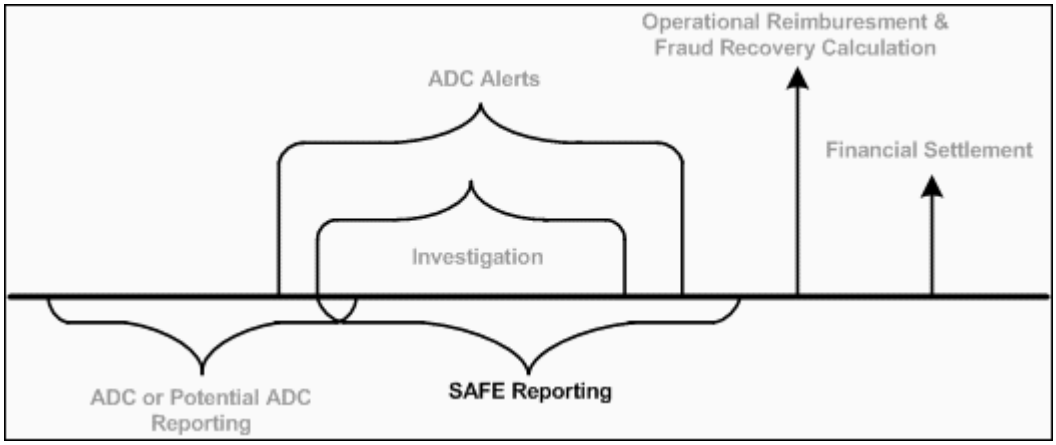
MasterCard will automatically terminate any MasterCard Connect™ user that has not logged on to the Manage My Fraud and Risk Programs application for nine months. The customer's Manage My Fraud and Risk Programs license will be terminated at the same time as its MasterCard Connect™ user license. At that 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 SAFE Reporting

This chapter describes how the MasterCard Fraud Recovery program interacts with SAFE in the reporting of fraud data and the calculation of incremental fraud.

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 90, counterfeit fraud transaction data that is submitted to SAFE by the issuer for calculating incremental fraud to be used in the FR calculation. Once the final FR is calculated, issuers will be able to modify their SAFE transactions, however the FR amounts will not change or be included in that Event's calculation. .

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 instructions about using SAFE, refer to the *SAFE Products User Guide*, available on the Publications Web site on the Security/Risk Services Web page.

The amount of time the issuer has to enter fraud transaction information 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)[5]
1	5,000,000	Unlimited	60
2	1,000,000	5,000,000	45
3	30,000	1,000,000	30

[5] **The At-Risk Length time frame begins on the date of the first ADC Alerts notification. 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.**

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. MasterCard will determine the number of days that the Issuer has to report fraudulent Transactions to SAFE for a disclosed Account number as follows:

- If MasterCard publishes an ADC Alert before MasterCard has received a final PFI report concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 30, 45, or 60 days to report fraudulent Transactions to SAFE.
- If MasterCard publishes an ADC Alert after MasterCard has received a final PFI report, and previous alerts have been published, concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 20, 35, or 50 days to report fraudulent Transactions 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. MasterCard will determine the number of days that the Issuer has to report fraudulent Transactions to SAFE for a disclosed Account number as follows:

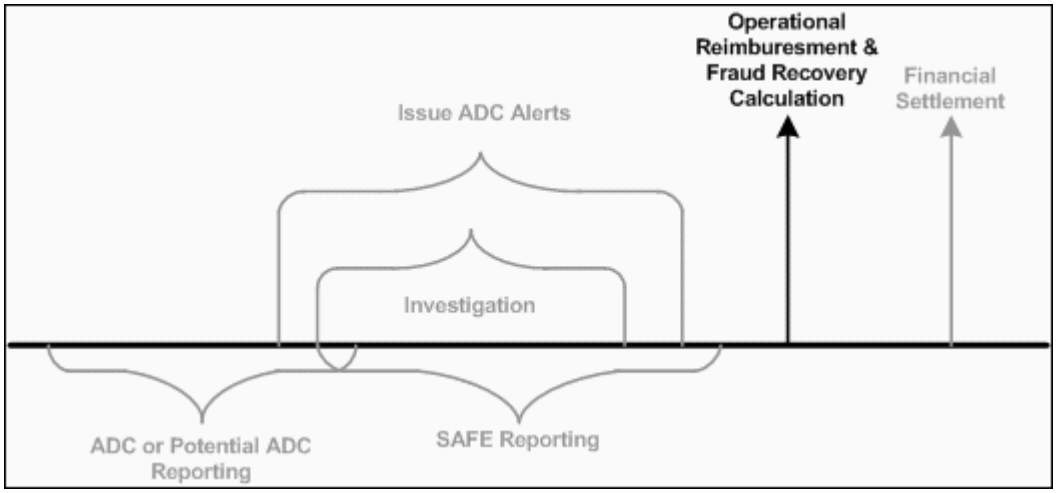
- If MasterCard publishes an ADC Alert before MasterCard has received a final PFI report concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 30, 45, or 60 days to report fraudulent Transactions to SAFE.
- If MasterCard publishes an ADC Alert after MasterCard has received a final PFI report, and previous alerts have been published, concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 20, 35, or 50 days to report fraudulent Transactions to SAFE.

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 Impacting at a minimum 30,000 MasterCard accounts. The MasterCard ADC reimbursement program is optional for issuers. Only issuers that opt into the MasterCard ADC reimbursement program will be eligible for reimbursement for OR or OR and FR for an ADC event each calendar year.

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.

Estimate of Potential Financial Liability

As a service to acquirers, MasterCard may provide, prior to the completion of the investigation, an estimate of potential financial liability to the acquirer responsible for the event.

MasterCard may send an Acquirer Responsibility Estimate letter and Acquirer Estimated Financial Liability report to (a) the acquirer's ADC Compliance Contact or Security Contact and (b) the Principal Contact listed in the *MasterCard Information Manual* (MIM). The estimate uses the published at-risk accounts and the existing fraud data in SAFE to produce a "snapshot" of the calculation of OR and FR.

Once the estimate letter and report are published, the number of compromised or potentially compromised accounts may change or the amount of counterfeit fraud reported to SAFE may change, resulting in a change in potential financial responsibility for the acquirer. The acquirer may request MasterCard to provide an updated potential financial responsibility report with the recalculated estimate.

To request an updated Estimated Acquirer Financial Liability Report, send an email message to account_data_compromise@mastercard.com. Provide contact name and telephone number and the case number.

ADC Operational Reimbursement

Operational Reimbursement (OR) is calculated based on the issuer parent ICA licensed to Manage My Fraud and Risk Programs at the time of the alert. All MasterCard branded (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 [6] .

Calculating OR

To calculate OR, the following steps are performed:

1. Assign the issuer to a tier based on the size of their portfolio.
2. Identify the type of technology embedded in the card and reimbursement amount based on the tier identified in step 1.
3. Multiply the type of card by the dollar amount as defined in section 6.5.1, table 1.
4. Subtract the operational reimbursement associated with cards that were previous alerted in the prior 180 days of the ADC Event.
5. Subtract a Fixed Deductible for normal card re-issue.

ADC Operational Reimbursement Factors

The following factors are used to calculate ADC OR.

- Determine the size of the issuer

The MasterCard OR program uses a tiered approach to provide partial reimbursement for the cost to replace a card. The tier is based on the gross dollar volume, obtained from the Quarterly Member Report (QMR), at the parent ICA [7]level for the issuer(s) impacted by the event. The gross dollar volume of the issuer is compared with the following table to determine the tier to use for calculating the average cost per card into which the issuer falls. Based on customer feedback, customers pay less for larger quantities of cards ordered and processed; therefore, the reimbursement rates assigned by tier will reflect these discounts.

[6] Maestro accounts are not eligible for OR reimbursement.

[7] 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 Parent ICA has not opted in, the ICA will be treated as a Parent ICA to determine the reimbursement rate.

Issuer—Gross Dollar Volume

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*
- 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		

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

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

Reimbursement Rate Per Tier for a Card Present Transaction

Issuer—Gross Dollar					
Tier	**Volume**	**Mag Stripe**	**Chip[8]**	**Contactless**	**Combo[9]**
1	0–200 MM	USD 6.25	USD 7.25	USD 7.50	USD 8.00
2	201 MM-1 B	USD 4.00	USD 5.00	USD 5.15	USD 5.30
3	> 1B	USD 2.70	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 opened after 1 January 2016.

- 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 Parent ICA. The Net Eligible Reimbursement amounts for all Issuers are added together and presented to the Acquirer as the total operational reimbursement amount.

ADC Operational Reimbursement—BIN Reports

MasterCard provides ADC OR reports at the bank identification number (BIN) level at no 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:

- Parent ICA number
- ADC Alerts Case Number
- Issuer's Contact Name and Phone Number
- 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

The BIN Level reports are automatically provided once the BIN level report registration has been completed.

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

[9] A "Combo" reimbursement rate will be assigned to a card that contains all three types: magnetic stripe, Chip, and MasterCard PayPass. For additional information, refer to section 10.2.5.3 of the MasterCard *Security Rules and Procedures* manual.

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

Parent ICA	Child ICA	BIN	Magstripe Amount USD	Chip Amount USD	PayPass Amount USD	Combo Amount USD	Total Amount USD
XXXX							
	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**
	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**

NOTE: For ADC Events prior to 1 January 2016, the Bin report will have an additional column indicating the Administration Fee that was included and deducted in the credit amount.

ADC Operational Reimbursement

The following describes OR notifications for acquirers and issuers.

Acquirers—Liability Notification

Once the total OR is calculated for an ADC Event, MasterCard notifies the responsible customers of the financial responsibility; This notice will be sent to the responsible customer's (a) ADC Compliance Contact or Security Contact and (b) Principal Contact. 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 parent ICA Security Contact (as defined in the MIM), 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.

ADC Operational Reimbursement—Customer Responsibility Cap

Section 10.2.5.2 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. If so, MasterCard will evaluate the following factors to determine whether a responsibility should be invoked for an ADC Event:

- Prior calendar year's annual MasterCard sales volume.
- Items noted in section 10.2.5.2 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 % applied**
<=50,000	5%
50,000 - 500,000	10%
>500,000	20%

Merchant Cap Example			
Prior calendar year MasterCard Merchant Sales	X	5%	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
PCI Cap 5%	USD 2,500

MasterCard Worldwide
ADC Operational Reimbursement/Fraud Recovery
Estimated Acquirer Financial Responsibility Report

ACQUIRER NAME - ICA nnnn — Report Date: 07-Jul-2015

Case Summary

MC Alerts Case #	ADCnnn-YY
Case Type	System Breach
Compromised Entity Name	Comrpomised Entity Name
Total # of Qualifying Alerts	n
Total # of Accounts Eligible for OR/FR	nnnn

Operational Reimbursement calculated dd-mmm-yyy

	Card Types							
Tier	Mag Stripe		Chip		PayPass		Combo	
	Number	Rate	Number	Rate	Number	Rate	Number	Rate
1	nnn	$6.25	nnn	$7.25	nnn	$7.50	nnn	$8.00
2	nnn	$4.00	nnn	$5.00	nnn	$5.15	nnn	$5.30
3	nnn	$2.70	nnn	$3.75	nnn	$3.95	nnn	$4.05

Gross Eligible Reimbursement Amount	$0.00
# of Accounts in Previous Alerts	n
Operationsl Reimbursement Associated with Previous Aler	$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-mmm-yyyy

Incremental Fraud for Case	$0.00
# of Accounts in Previous Alerts	0
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
Acquirer Percentage	100.0%
Acquirer Total Estimated Operational Reimbursement	$5,992.92
Acquirer Total Estimated Fraud Recovery	$0.00
Total Estimated Acquirer Financial Responsibility	**0**

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 *MasterCard Information Manual* (MIM).

MasterCard Worldwide
ADC Operational Reimbursement/Fraud Recovery
Final Acquirer Financial Responsibility Report

ACQUIRER NAME - ICA nnnn — Report Date: 07-Jul-2015

Case Summary

MC Alerts Case #	ADCnnn-YY
Case Type	System Breach
Compromised Entity Name	Comrpomised Entity Name
Total # of Qualifying Alerts	n
Total # of Accounts Eligible for OR/FR	nnnn

Operational Reimbursement calculated dd-mmm-yyy

	Card Types							
Tier	Mag Stripe		Chip		PayPass		Combo	
	Number	Rate	Number	Rate	Number	Rate	Number	Rate
1	nnn	$6.25	nnn	$7.25	nnn	$7.50	nnn	$8.00
2	nnn	$4.00	nnn	$5.00	nnn	$5.15	nnn	$5.30
3	nnn	$2.70	nnn	$3.75	nnn	$3.95	nnn	$4.05

Gross Eligible Reimbursement Amount	$0.00
# of Accounts in Previous Alerts	n
Operations l Reimbursement Associated with Previous Aler	$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-mmm-yyyy

Incremental Fraud for Case	$0.00
# of Accounts in Previous Alerts	0
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
Acquirer Percentage	100.0%
Acquirer Total Estimated Operational Reimbursement	$5,992.92
Acquirer Total Estimated Fraud Recovery	$0.00
Total Estimated Acquirer Financial Responsibility	**0**

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

ADC Fraud Recovery

Section 10.2.5.5 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 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%
- F = Net eligible for fraud recovery amount

NOTE: FR is calculated in USD.

Total 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 Recover (FR) reimbursement amounts at the Parent, Child, and bank identification number (BIN) level. The FR BIN Level Report is available at no charge.

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

- Parent ICA number
- ADC Alerts Case Number
- Issuer's Contact Name and Phone Number
- 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

BIN Level reports provide FR totals by parent ICA, child ICA, and BIN. Consequently, the issuer (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.

Parent ICA	Child ICA	BIN	Total Fraud Recovery Amount USD
NNNN			
		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

NOTE: For ADC Events prior to 1 January 2016, the Bin report will have an additional column indicating the Administration Fee that was included and deducted in the credit amount

ADC Fraud Recovery—Notification

The following describes FR notifications for responsible customers and issuers.

Responsible Customer—Liability Notification

Once the final ADC FR is determined for an ADC Event, MasterCard notifies the responsible customer(s) of financial responsibility. This notice is sent to the responsible customer's (a) ADC Compliance Contact or Security Contact and (b) Principal Contact. MasterCard will then debit the responsible customer's MCBS account the amount calculated. See the sample in Appendix A, Final Responsibility Letter.

Issuer—Reimbursement Notification

MasterCard will notify the parent ICA Security Contact (as defined in the MIM) 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.

ADC Fraud Recovery—Acquirer Responsibility Cap

Section 10.2.5.2 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. If so, 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 section 10.2.5.2 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 appropriateMasterCard will utilize the following tiered formula:

Prior Calendar year's tranasctions	Merchant Cap % applied
<=50,000	5%
50,000 - 500,000	10%
>500,000	20%

ADC Fraud Recovery Factors

MasterCard uses the following factors to calculate ADC Fraud Recovery (FR) at the parent ICA level.

Counterfeit Fraud Baseline (Items A and B Above)

Using accounts published in Manage My Fraud and Risk Programs, MasterCard will calculate (a) a counterfeit baseline by looking at POS 90 and POS 80 counterfeit fraud that was reported to the System to Avoid Fraud Effectively (SAFE) at the parent ICA level and (b) the incremental counterfeit fraud associated with an ADC Event. MasterCard will determine the incremental fraud amount by calculating the amount of counterfeit fraud for an ADC Event by parent ICA and reducing the total event-specific counterfeit fraud amount by the baseline counterfeit fraud experienced by the issuing parent ICA for the at-risk accounts before 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 first 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[10]	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. MasterCard will determine the number of days that the Issuer has to report fraudulent Transactions to SAFE for a disclosed Account number as follows:

- If MasterCard publishes an ADC Alert before MasterCard has received a final PFI report, and previous alerts have been published, concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 30, 45, or 60 days to report fraudulent Transactions to SAFE.
- If MasterCard publishes an ADC Alert after MasterCard has received a final PFI report concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 20, 35, or 50 days to report fraudulent Transactions 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. MasterCard

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

will determine the number of days that the Issuer has to report fraudulent Transactions to SAFE for a disclosed Account number as follows:

- If MasterCard publishes an ADC Alert before MasterCard has received a final PFI report, and previous alerts have been published, concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 30, 45, or 60 days to report fraudulent Transactions to SAFE.
- If MasterCard publishes an ADC Alert after MasterCard has received a final PFI report concerning the ADC Event or Potential ADC Event, then that ADC Alert will specify whether the Issuer has 20, 35, or 50 days to report fraudulent Transactions 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
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 parent ICA and then reducing the total counterfeit fraud by the baseline counterfeit fraud experienced by the issuing 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 the six months prior to the alert date.

Chargeback Deduction

The chargeback deduction represents the issuer's ability to charge back transactions. A five percent deduction will be applied to the incremental fraud amount.

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 compliant party. Transactions that qualify for a counterfeit fraud chargeback will be removed from the calculations regardless of whether the issuer files the chargeback. . [11]

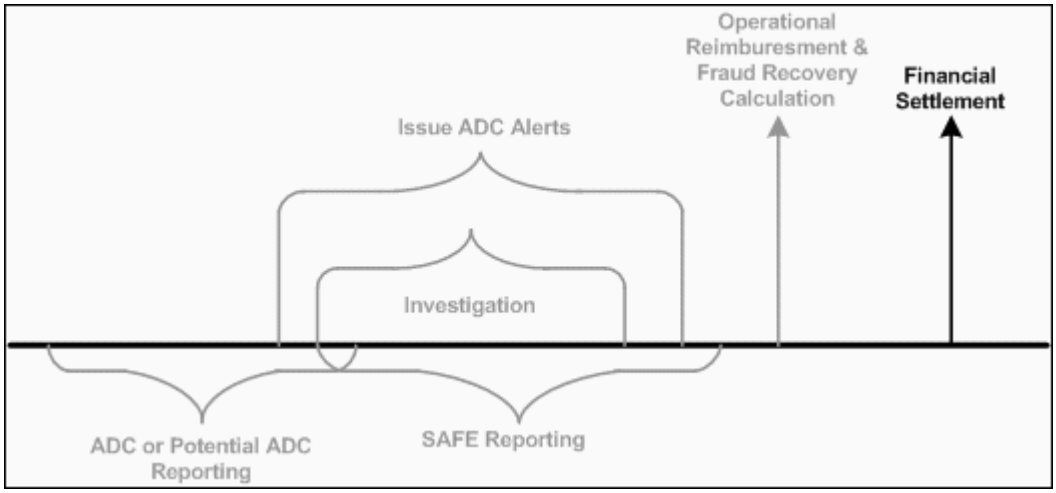
[11] Refer to the Dispute Resolution Manual for eligible chargebacks

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 final financial liability falls in the life cycle of an ADC Event.



ADC Event Financial Settlement Information

A final step of a MasterCard ADC Event is determining 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

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.

Fraud Recovery—Responsible Member Responsibility

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

Fraud Recovery—Billing Event Codes

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 *MasterCardConsolidated Billing System*(MCBS) document.

ADC Event Financial Settlement Information for Issuers

A final step of a MasterCard ADC Event is providing partial reimbursement to issuers for losses incurred as the result of an ADC Event. 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 Parent ICA as listed in the Member Information Manual application at the time of the Event.

Operational Reimbursement Notification

MasterCard credits an issuer's MCBS account with the ADC operational reimbursement payout for applicable parent ICA numbers.

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
U.S.	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 payout for applicable parent ICA numbers.

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
U.S.	2SC-CRD1214	US Credit (Issuer)
Brazil	2SC-CRD1214	Brazil Credit (Issuer)

Annual Fees

Effective 1 January 2016, MasterCard will no longer impose an ADC Administrative Fee on issuers. Instead, MasterCard will apply an Annual Service Fee on issuers as explained below:

- Issuers that choose to participate in the reimbursement component of the MasterCard ADC Program, as well as receive the value and benefit of MasterCard ADC investigations, 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 receive any financial reimbursement for that calendar year. However, these issuers will continue to receive ADC Alerts as well as the value and benefit of MasterCard ADC investigations and, therefore, will be assessed the service fee at a 50 percent reduced rate.

The Annual Service Fee will be based on the number of MasterCard issued cards reported to Quarterly MasterCard Report (QMR) for the year prior to the issuer's opt-in year of the program. MasterCard will assess this fee at the Parent ICA level corresponding to the same method for issuer reimbursements.

Fees

The following table presents the Annual Service Fee effective 1 January 2016.

Card Range Based on QMR	Opt-In Rate (USD)	Opt-Out Rate (USD)
0–700,000	5,000	2,500

Card Range Based on QMR	Opt-In Rate (USD)	Opt-Out Rate (USD)
700,001–3 million	20,000	10,000
3 million–10 million	30,000	15,000
10 million–20 million	75,000	37,500
More than 20 million	100,000	50,000

Billing Events

The following MasterCard Consolidated Billing System (MCBS) billing event will apply. The first billing will occur on or after 14 February 2016.

Billing Event	Billing Event Description	Service ID
2SC1218	Annual Service fee assessed to Issuer for the Account Data Compromise Recovery Program	SC

ADC Event Final Financial Responsibility Determination

Pursuant to section 10.2.6 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.

MasterCard
Franchise Integrity
2200 MasterCard Blvd
O' Fallon, MO 63368, USA

dd month yyyy

Security Contact Name
Security Contact Institution Name
Address Line 1
Address Line 2
City, State Zip
Country

POTENTIAL ACCOUNT DATA COMPROMISE EVENT RESPONSIBILITY
ADC ALERTS CASE # MCANNNN-YY, MERCHANT NAME, ICA NNNN

Dear <<Security Contact Name>>:

MasterCard is currently investigating the above-referenced potential Account Data Compromise (ADC) event. MasterCard will not comment further about the 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, it is possible that MasterCard will 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

Confidential Page 1

Again, please note that these are preliminary, conditional estimates only. Further, the estimate may be subject to a 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>>. MasterCard 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.

Please contact us, or contact your MasterCard Customer Fraud Management representative if you have any questions.

Sincerely,

Fraud Investigations

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
2000 Purchase Street
Purchase, NY 10577-2509

dd month yyyy

Security Contact Name
Security Contact Institution Name
Address Line 1
Address Line 2
City, State Zip
Country

ACCOUNT DATA COMPROMISE EVENT – FINAL FINANCIAL LIABILITY
ADC ALERTS CASE # MCANNNN-YY, MERCHANT NAME, ICA NNNN

Dear <<Security Contact Name>>

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 account data compromise event occurred at <<Merchant name>> for which <<Acquirer name>> is responsible. A member 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 certain requirements of the PCI Data Security Standard. These requirements and MasterCard's finding are provided in the chart on page ___. 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 member 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.

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

Page | 1

If you have questions about satisfying the SDP program and PCI DSS requirements referenced above, please send your questions to the sdp@mastercard.com email box.

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	xxx.xx
ADC Fraud Recovery	xxx.xx
Total	xxx.xx

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

Case Management Fee
As set forth in section 10.2.5.6 of the Manual, MasterCard may assess the responsible member for all investigation and other costs incurred by MasterCard in connection with an ADC event or potential ADC event. The Event Case Management Fee Structure is set forth in section 7.2 of the Account Data Compromise User Guide. Accordingly, MasterCard will bill <<Acquirer Name>> a case management fee on <dd-month-yyyy> in the amount of <xxx.xx.>

Conclusion
Please be advised that, on dd-month-yyyy , <<Acquirer Name>> ICA <nnn> will be debited for the above-cited financial liabilities totaling <xxx.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. MasterCard values our relationship with the <<Acquirer Name>> and know that you share our view of the importance of account data security.

Please contact us, or contact your MasterCard Customer Fraud Management representative if you have any questions.

Sincerely,

Fraud Investigations

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
2000Purchase Street
Purchase, NY 10577-2509

$currentDate

$issrCntNm
$issuerCompanyName
$issuerAddress1
$issuerAddress2
$cityStateZip
$country

ACCOUNT DATA COMPROMISE(ADC) – MASTERCARD ALERTS CASE # $adcCaseNo - 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 $issuerCompanyName via MasterCard Billing System (MCBS) account on $mcbsDeliveryDate.

Operational Reimbursement calculated $orCalculatedDate

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	$cpNo	$cpRt	$ppNo	$ppRt	$cbNo	$cbRt

Gross Eligible Reimbursement Amount	$gross
# of Accounts in previous Alerts	$newfield
Operational Reimbursement Associated with Previous Alerts	$newfield2
Net Eligible Reimbursement Amount	$newfield3
Deductible	$stdDeductible
Net Eligible Reimbursement Amount	$calculatedNetReimb

Cap Applied	$orCapApplied
MC Admin Fee	$mcORAdmin

Total Operational Reimbursement	**$totalORAmtNum**

Fraud Recovery calculated $frCalculatedDate

Description	Billing Event	Total
Net Fraud Recovery	$netFRAmtLbl	$totFRAmt
Fraud Recovery Administration Fee	$mcFRAdmFeeLbl	$mcFRAdminFee

Incremental Fraud for Case	$magIncrFRAmt
# 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, contact your MasterCard Customer Fraud Management 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,

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, DSE, or TPP data for aspects of the ADC process.

Applications of the MIM to an ADC Event

The *MasterCard Information Manual* (MIM) presents multiple uses to customers when handling an ADC Event or Potential ADC Event.

The MIM 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 MIM 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 Primary Contact and Security Contact name, address, email address, and phone number.

For questions concerning the access and update of ICA number profile in the MIM, 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 on-line 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.

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, even if the corresponding accounts are not closed or not statused as fraud.

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 on MasterCard Connect™.

Customers must register for access to MasterCard Connect™ to use the Manage My Fraud and Risk Program 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 replaces MasterCard Alerts and serves as the distribution method for account data compromise events 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, please contact the Customer Operations Services 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.

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.