# Table of Contents

Introduction ......................................................................................................................................... 3  
Audience ......................................................................................................................................... 3  
Changelog ......................................................................................................................................... 3  
1 MasterCard and Visa Programs ........................................................................................................ 4  
2 MasterCard Excessive Chargeback Programme ............................................................................... 5  
3 MasterCard Global Merchant Audit Program .............................................................................. 7  
4 Visa Global Merchant Chargeback Monitoring Programme .......................................................... 9  
5 Visa Global Merchant Fraud Performance Program ...................................................................... 11  
6 Visa Regional Merchant Fraud Performance Program .................................................................... 13  
7 Possible solutions ............................................................................................................................ 14  
7.1 Monitoring chargeback levels ...................................................................................................... 14  
7.2 Defending chargebacks ............................................................................................................... 15  
7.3 AVS – America & UK only ........................................................................................................... 15  
7.4 3D Secure .................................................................................................................................... 15  
7.5 Adyen Fraud settings .................................................................................................................... 16  
8 Summary .......................................................................................................................................... 18
Introduction

Adyen has recognised that fraud and chargebacks are becoming an ever increasing problem for many merchants. For most merchants their fraud and chargeback problems will be related. Adyen wants to warn merchants of the potential implications if they have excessive fraud and chargeback rates, especially the possibility for fines to be levied to encourage the correction of the underlying fraud and chargeback problems. Adyen also wants to work with its merchants to help them reduce their fraud and chargeback problems.

This manual will outline:

- the rules that govern both the MasterCard and Visa fraud and chargeback programs;
- the practicalities of the MasterCard and Visa fraud and chargeback programs;
- the potential fines that can be levied if fraud and chargeback problems are not rectified in a timely fashion; and
- possible solutions to stop fraudulent transactions before they occur.

Please note that each fraud and chargeback program is different and works independently of the others.

It is important to understand that Adyen does not always work directly with MasterCard and Visa in relation to the fraud and chargeback programs. In many cases Adyen works with its Acquiring partners who then deal with MasterCard and Visa directly.

Fines in relation to the programs are levied by MasterCard and Visa to the Acquirer who will then levy them to Adyen who will then levy them on the merchant.

The latest version of this document is available at:

https://support.adyen.com/links/documentation

Audience

This is an information manual for merchants, to provide them with sufficient information to avoid issues and additional costs related to these fraud and chargeback programs.

Changelog

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0</td>
<td>2011-10-20</td>
<td>• Adjustment from internal manual to public information</td>
</tr>
<tr>
<td>5.0</td>
<td>2012-03-02</td>
<td>• Adjustment from additional scheme information</td>
</tr>
<tr>
<td>6.0</td>
<td>2012-06-03</td>
<td>• Adjustment from additional scheme information</td>
</tr>
</tbody>
</table>
# 1 MasterCard and Visa Programs

The table set out below explains the five different MasterCard & Visa programs related to Fraud and/or Chargebacks:

<table>
<thead>
<tr>
<th>Program</th>
<th>Minimum Thresholds</th>
<th>Potential Fines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MasterCard Excessive Chargeback Program</strong></td>
<td>• CTR in excess of 1%; and&lt;br&gt;• at least 100 chargebacks in 1 calendar month.</td>
<td>• USD 25 per chargeback above the allowable threshold; and&lt;br&gt;• A <strong>large</strong> Violation element based upon the Issuer recovery element and basis point score above the accepted thresholds for that month.</td>
</tr>
<tr>
<td><strong>MasterCard Global Merchant Audit Program</strong></td>
<td>• 3 fraudulent transactions; and&lt;br&gt;• At least USD 3,000 in fraudulent transactions; and&lt;br&gt;• A fraud to sales dollar volume ratio minimum of 3% and not exceeding 4.9%</td>
<td>• USD 25,000 for not submitting a special merchant audit questionnaire.</td>
</tr>
<tr>
<td><strong>Visa Global Merchant Chargeback Monitoring Program</strong></td>
<td>• the number of chargebacks in a single month is more than 200; and&lt;br&gt;• the ratio of these chargebacks to the merchant's transactions in the same month is more than 2%.</td>
<td>• USD 100 per chargeback&lt;br&gt;• USD 200 per chargeback if the merchant has not implemented procedures to reduce chargebacks (after month 4)</td>
</tr>
<tr>
<td><strong>Visa Global Merchant Fraud Program</strong></td>
<td>• $25,000 of reported fraud; and&lt;br&gt;• 25 fraud transactions; and&lt;br&gt;• 2.5% fraud-to-sales ratio</td>
<td>• 1st: USD 5,000&lt;br&gt;• increased with an other USD 5,000 for every month on or above the performance thresholds</td>
</tr>
<tr>
<td><strong>Visa Regional Merchant Fraud Program</strong></td>
<td>• $15,000; and&lt;br&gt;• 15 fraud transactions; and&lt;br&gt;• 7.5% fraud to dollar sales ratio</td>
<td>• No financial penalty only chargeback window</td>
</tr>
</tbody>
</table>
2 MasterCard Excessive Chargeback Programme

MasterCard closely monitors all chargebacks.

Every month, Adyen's acquiring partners track every merchant's MasterCard chargeback to transaction ratio (CTR). The CTR is the number of MasterCard chargebacks received by the acquirer for a merchant in a calendar month, divided by the number of the merchant's MasterCard sales transactions in the preceding month.

An example of the calculation and the formula can be seen below.

\[
CTR = \frac{\text{# of February Chargebacks}}{\text{# of January Settled Transactions}}
\]

<table>
<thead>
<tr>
<th>Chargeback Month</th>
<th>February</th>
</tr>
</thead>
<tbody>
<tr>
<td># of February chargebacks</td>
<td>1000</td>
</tr>
<tr>
<td># of January settled transactions</td>
<td>50000</td>
</tr>
<tr>
<td>February CTR</td>
<td>2.00%</td>
</tr>
</tbody>
</table>

MasterCard monitors two types of merchant's as set out below:

<table>
<thead>
<tr>
<th>Program</th>
<th>Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chargeback Monitored Merchant</td>
<td>• CTR in excess of 1%; and&lt;br&gt;• at least 100 charge-backs in 1 calendar month.</td>
</tr>
<tr>
<td>Excessive Chargeback Merchant</td>
<td>• two consecutive calendar months (the “trigger months”) the merchant has a minimum CTR of 1,5%; and&lt;br&gt;• at least 100 chargebacks in each month; and&lt;br&gt;• this designation is maintained until the merchant's CTR is below 1,5 % for two consecutive months</td>
</tr>
</tbody>
</table>
Potential Fines

MasterCard will issue fines if a merchant is an Excessive Chargeback Merchant. The calculation of the MasterCard fine is formula driven and consists of two components - an Issuer Recovery element ($25 per chargeback) and a Violation element. The violation element is calculated after taking into account the Issuer Recovery element and the basis point score. We cannot give an exact figure on this as each case will be different however the figure can be very large.

Tier Structure

Mastercard has established a tiered structure for merchants identified as ECMs as described below.

Tier 1 ECM

Mastercard considers a merchant as a Tier 1 ECM during the first through sixth month (whether consecutive or non-consecutive) that the merchant is identified as ECM.

Tier 2 ECM

Mastercard considers a merchant as a Tier 2 ECM during the seventh through twelfth month (whether consecutive or non-consecutive) that the merchant is identified as ECM.

Additional Tier 2 ECM Requirements

With respect to a Tier 2 ECM, Mastercard may require the acquirer to undergo a Fraud Management Program (FMP) Level 3 Customer review, at the acquirer's expense, as described in Chapter 13 fo the Security Rules and Procedures manual.

After a merchant has been an ECM for 12 months (whether consecutive or non-consecutive), the acquirer may be deemed to be in violation of Mastercard rule 5.11.7. In addition to the standard ECM issuer reimbursement and violation assessments, the acquirer may be subject to a noncompliance assemssement of up to USD 50,000 per month for each month after the twelfth month that the merchant remains an ECM.

Potential termination

Please be aware that some acquirers will terminate merchants if they remain in the Mastercard Excessive Chargeback Programme (either CMM or ECM status) for a total of 3 months.
MasterCard Excessive Chargeback Programme

Chargeback-Monitored Merchant Reporting Requirements

Each calendar month, a separate CMM report must be submitted to Mastercard in case the merchant qualified as a CMM for the previous calendar month. The report must be submitted no later than 40 days from the end of the calendar month.

Mastercard will assess the acquirer a reporting fee of USD 50 for each CMM report submitted. The CMM reporting must continue until the merchant is no longer identified as a CMM for two consecutive months.

Excessive Chargeback Merchant Reporting Requirement

Within 30 days of the end of the second trigger month, and on a monthly basis thereafter, the acquirer must submit a separate ECM report for each of its ECMs until that ECM's CTR is below 150 basis point for two consecutive months. Mastercard will assess a reporting fee of USD 100 for each ECM report submitted. A report must be sent monthly until the merchant is no longer identified as an ECM for two consecutive months. If the merchant is identified as CMM during those months, then the CMM reporting requirements will apply.
3 MasterCard Global Merchant Audit Program

The Global Merchant Audit Program uses a rolling six months of data to identify merchants that in any calendar month meet the criteria set out in the table below. The fraud figures are related to when the transaction occurred not when the fraudulent transaction was reported.

The table set out below explains the different tiers of the MasterCard Global Merchant Audit Program.

<table>
<thead>
<tr>
<th>A merchant location is classified in the Following GMAP tier....</th>
<th>If in any calendar month, the merchant location meets the following fraud criteria...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1 – Information Fraud alert</td>
<td>• 3 fraudulent transactions; and&lt;br&gt;• At least USD 3,000 in fraudulent transactions; and&lt;br&gt;• A fraud to sales dollar volume ratio minimum of 3% and not exceeding 4.99%</td>
</tr>
<tr>
<td>Tier 2 – Suggested Training alert</td>
<td>• 4 fraudulent transactions; and&lt;br&gt;• At least USD 4,000 in fraudulent transactions; and&lt;br&gt;• A fraud to sales dollar volume ratio minimum of 5% and not exceeding 7.99%</td>
</tr>
<tr>
<td>Tier 3 - High Fraud alert</td>
<td>• 5 fraudulent transactions; and&lt;br&gt;• At least USD 5,000 in fraudulent transactions; and&lt;br&gt;• A fraud to sales dollar volume ratio minimum of 8%</td>
</tr>
</tbody>
</table>

If MasterCard identifies a merchant in Tier 2, Adyen will recommend the merchant undertakes a fraud training program.

If MasterCard identifies a merchant in tier 3, MasterCard will usually issue an audit of the merchant, this means:

1. The acquirer will require the merchant to fill in a questionare outlining what steps it is taking to stop its fraud problem. The merchant must return the
question are within 25 days after Adyen notifies the merchant. Adyen will liaise with its merchant's to ensure the questionnaire is completed correctly; and

2. If MasterCard is not happy with the response then they will require the merchant to create and implement a fraud control action plan within 90 days of being placed in the Global Merchant Audit Program.

Longterm if the fraud issues of the merchant are not resolved by the fraud control action plan then the acquirer and / or MasterCard will open up a six month chargeback window and possibly revoke the right for the merchant to accept MasterCard payments.

**Potential Fines**

MasterCard does not supply details of specific fines however a continued violation will fall under what MasterCard describes as “Category A noncompliance”. Category A noncompliance occurs when a merchant affects payment system integrity. MasterCard has the authority to impose monetary noncompliance assessments for Category A noncompliance.
4 Visa Global Merchant Chargeback Monitoring Programme

Visa separately monitors international and country-to-country chargebacks. A international transaction is for example when a UK based merchant sells goods to a shopper with a French issued credit card. A country-to-country chargeback is when an UK merchant received a chargeback from a shopper with an UK issued card.


Visa Europe measures the chargebacks received in a single month (irrespective of the date the actual transaction took place) against the transactions received in the same month.

The formula and an example of a calculation are set out below:

\[ \text{CTR} = \frac{\# \text{ of January Chargebacks}}{\# \text{ of January Settled Transactions}} \]

**Example Calculation Month**

<table>
<thead>
<tr>
<th>Chargeback Month</th>
<th>January</th>
</tr>
</thead>
<tbody>
<tr>
<td># of January chargebacks</td>
<td>250</td>
</tr>
<tr>
<td># of January transactions</td>
<td>7500</td>
</tr>
<tr>
<td>CTR</td>
<td>3.33%</td>
</tr>
</tbody>
</table>

Visa will place merchant's in their Excessive ChargeBack Program under two criteria:

1. the number of chargebacks (international or country-to-country) in a single month is more than 200; and
2. the ratio of these chargebacks to the merchant's sales (international or country-to-country) in the same month is more than 2%.

A merchant that has ben placed in the Global Merchant Chargeback Monitoring Programme will be granted a 3 month remediation period to reduce excessive chargebacks (the remediation period is not applicable for high risk merchants).
Potential Fines

When a merchant's CTR is above 2% then the potential Visa fine is between $100 and $200 per chargeback (at Visa's discretion). Therefore, an appeal process exists when the circumstances of the excess are identified as well as the merchant's actions to correct the situation.

Note:

1. For the purposes of administering Merchant compliance under the Global Merchant Chargeback Monitoring Program, if a merchant submits transactions for a single Merchant location using multiple names, Visa Europe may group the Merchant activity performed under the multiple names.

2. If Visa Europe determines that an Acquirer or its Merchant modified the Merchant name or Merchant data in any way to circumvent the Global Merchant Chargeback Monitoring Program, Visa Europe may:
   • Assess a fine of US $10,000 per Merchant, per month, to the Acquirer;
   • Permanently disqualify the Merchant and its principals from participating in the Visa program.

Potential termination

Please be aware that some acquirers will terminate merchants if they remain in the VISA GMCMP for a total of 3 months.
5 Visa Global Merchant Fraud Performance Program

The Global Merchant Fraud Performance Program applies if a merchant is located in one region and a card is issued in another region. For example if a merchant was located in Europe and the card was issued in Asia then this programme would apply.

There are two categories in the program as set out in the tables below.

| Minimum Fraud Performance | • $25,000 of reported fraud; and |
|                          | • 25 fraud transactions; and |
|                          | • 2.5% fraud to sales ratio |
| Excessive Fraud Performance | • $250,000 of reported fraud; and |
|                            | • 2.5% fraud to sales ratio |

For merchant's who meet or exceed the minimum fraud performance thresholds, remediation consists of:

1. Workout period – There is a three month workout period during which Adyen will work with the merchant to remedy the fraud problem. No financial penalties will be imposed at this time.

2. Enforcement Period – If the merchant does not reduce fraud to below the accepted thresholds, it can become liable for chargeback liability (if it isn't already) and fines following the workout period. Continued non-compliance can lead to the revoking of the merchants right to accept Visa payments.

For merchant's who meet or exceed the excessive fraud performance thresholds, remediation consists of:

1. Workout period – There is no workout period

2. Enforcement period – Effective immediately, the merchant is subject to charge-back liability for fraudulent transactions. In the beginning of month three, fines are applied in addition to charge-back liability. Continued non-compliance can lead to the revocation of the right to accept Visa payments.
Potential fines
Fines begin at $5,000 per month and increase by $5,000 increments for every month the merchant meets or exceeds the thresholds. Fines are applied in USD as set out in the table below:

| 1st fine | $5,000.00 |
| 2nd fine | $10,000.00 |
| 3rd fine | $15,000.00 |
6 Visa Regional Merchant Fraud Performance Program

The Visa Regional Merchant Fraud Performance Program is separate from the Visa Global Merchant Fraud Performance Program. It only applies to transactions where the Card was Issued in the same region as the merchant is located (i.e European Issued card with a European located merchant).

The Programme parameters are set out below:

| Workout Parameters | • $15,000.00  
|                    | • 15 fraud transactions; and  
|                    | • 7.5% fraud to sales ratio  
| High Risk Parameters | • $40,000.00  
|                     | • 20 fraud transactions; and  
|                     | • 20% fraud to sales ratio |

For merchant's who meet or exceed the regional fraud performance thresholds, remediation consists of:

Workout period – There is a three month workout period during which Adyen will work with the merchant to remedy the fraud problem. No financial penalties will be imposed at this time.

High Risk Period – If the merchant does not reduce fraud to below the accepted thresholds, it can become liable for chargeback liability (if it isn't already) and fines following the workout period. Continued non compliance can lead to the revoking of the merchants right to accept Visa payments.
7 Possible solutions

7.1 Monitoring chargeback levels

- Many merchant's do not monitor their chargeback levels. It is important that merchant's realise there is a problem before MasterCard and Visa start levying fines. In the Adyen back office, merchant's have a real time view of all chargebacks they receive if they navigate to the Disputes section of their Adyen customer area.

- Adyen is currently developing a tool so merchant's can accurately view their MasterCard and Visa CTR's in their Adyen customer area.

- Merchant's can also receive an automatic email advising them of when a chargeback is received. This email can be set up as set out below:

  a) Login to the Adyen Customer Area
  b) Click on the "Settings" menu
  c) In the "System Messages" box click “Edit System Mesage”
  d) Click the "New" button

  Set fields as follows:

  a) System Component: CHARGEBACKS
  b) Delivery Type: email
  c) Click the "Add" button

  To see the email address to which this email will be send to:

  a) Login
  b) Click "Settings" menu
  c) Click "My User" box

Your details are in the "User Contact Details" section. It is also here that you can add or change the contact details of the person who will receive the automated email.
7.2 Defending chargebacks

- Merchant's can most times defend chargebacks through their Adyen customer area. They can click into each Dispute in the Disputes section of their Adyen back office. After clicking into a dispute their is a tool where merchant's can upload documentation to defend a chargeback.

- Once uploaded this material gets passed on to our acquiring partners who pass it on to Mastercard and Visa. Examples of defence material can include extract logs, signed courier or delivery company docket's or invoices and emails or communications from the shopper admitting they received the goods.

7.3 AVS – America & UK only

- If a merchant provides goods or services to shoppers with USA or UK issued cards then we recommend that AVS is used at all times. AVS is still not well implemented in other parts of Europe therefore we do not recommend its use.

7.4 3D Secure

- Adyen always recommends the use of 3D secure. Long term, Adyen sees the use of 3D secure as a key way to stop fraud. 3D secure may lead to a higher refusal rate however will lower merchant's fraud rates. If a merchant's would like to test 3D Secure then Adyen can activate it (very easily) for a test period and merchant's can then analyse their conversion rates during the test period. It is also very easy to de activate if you believe it is having a strong impact on your conversion rates.

- It is important to understand that even if a merchant has initiated 3D secure its fraud level will still be monitored by the schemes. Although it would not be receiving chargebacks and therefore cannot be an excessive chargeback merchant it is possible (& has occurred) that a merchant with 3D Secure can be placed in the Visa & Mastercard fraud program.

- There is an automatic liability shift to the issuing banks for personal cards once 3D secure has been initiated by a merchant, however if a merchant has excessive chargebacks and fraud then the schemes may open up a six month window where the liability for chargebacks shifts from the MasterCard and Visa to the merchant.
Possible solutions

7.5 Adyen Fraud settings

If you are a merchant with excessive fraud and chargeback levels please work with your Adyen representative to perfect your Adyen fraud settings. Fraud settings need to be different for each merchant's given their different business models and payment methods.

1. Issuing card v different shopper country
   - Many fraudulent transactions occur with a differing shopper IP address and Issuing card country. If a merchant has a high number of fraudulent transactions Adyen recommends using this tool. It can either be set to 100/100 which will block all transactions which have a differing shopper country and issuing card country or if a merchant has a number of legitimate transactions from differing shopper and issuing card countries then we also recommend setting the check at 90 and manually filtering the transactions. Manually filtering means merchants manually checking a transaction and refunding any that it believes to be fraudulent. This means a merchant will not incur chargeback costs if it has chargeback liability. Adyen is developing on a tool which will stop transactions that reach a certain score and then merchant's can decide whether they would like to refuse or authorise the transaction.

2. Issuing card country
   - If a merchant notices a high number of fraudulent transactions from cards issued in one country then they can block cards issued in that country. For example, the highest percentage of fraud comes from USA issued cards. If after carrying out analysis merchants discover they do not have shoppers buying with USA issued cards then they can put USA on the “Issuing Country Referral List” which is located on each merchant's fraud settings. This may affect shoppers who live in Europe but hold a USA issued card however from our experience this is usually a very low percentage of shoppers.

3. High Risk Shopper Country
   - If a merchant has a number of fraudulent transactions from one Shopper country than they can block all transactions from those shopper countries via the Shopper IP originates from high-risk country block located on their Adyen fraud tool.
4. Velocity Checks

- Velocity checks are efficient at stopping fraudulent transactions as if a fraudster is successful in one transaction through a merchant they will usually try and repeat the process. For some merchant's, velocity checks would not be suitable as legitimate transactions may be stopped (this would occur when shoppers frequently buy items or subscriptions through a merchant each day). However, when shopper's would only usually buy goods through a merchant very infrequently then they are very helpful in stopping fraudulent transactions. If for example a merchant would only usually buy goods once a day or once a week then Adyen advises strengthening the velocity checks. If you don't understand what a velocity check is then a merchant's Adyen representative can explain it and work with them to perfect these settings.
8 Summary

Adyen will always work with its merchants to decrease their fraud and chargeback levels, however merchant's must constantly monitor their fraud and chargeback levels and adapt their fraud settings and business practices accordingly to ensure fraud and chargeback levels are reduced.

If merchant's ever want further clarification on any issue related to fraud or chargebacks then they should contact their Adyen representative who will provide further clarification.