# Fraud Detection Module Advanced: Checklist

Configuration Guide for the Advanced Fraud Detection Module: Checklist v.4.4.0

# Table of Contents

# 1 What is the Fraud Detection Module?

In distance selling, the fight against fraud requires maximum levels of know-how, speed and flexibility. To help you implement effective risk management, the Fraud Detection Module offers a real-time service that provides all the necessary analysis information, and offers fully customised safeguards for handling dubious transactions.

Use of the Fraud Detection Module does not, however, guarantee protection against all fraud, it only helps you to thwart it. The Fraud Detection Module can be configured based on the risks or past fraud issues that have been encountered by your business.

Unlike the basic Fraud Detection Module, the merchant configures the actual behaviour of the blacklists, whitelists and greylists, along with the rules and limits in the Risk Evaluation list of the Fraud Detection Module.

## 1.1 Benefits

The Fraud Detection Module allows you to:

- Detect anomalies during transactions
- Immediately block attempts by recognised fraudsters
- Mark specific risks for review
- Protect against country-specific risks
- Define and apply fully customised security policies
- Benefit from a conditional payment guarantee (see here) in accordance with your individual acquirer's policies (3-D Secure)

## 1.2 Access

You can access the Fraud Detection Module via the "Fraud detection" link in your account menu.

## 1.3 Contents

The Fraud Detection Module comprises three separate functional areas:

- Fraud detection activation and configuration
- 3-D Secure
- Blacklists / Greylists / Whitelists

IMPORTANT

The VISA/MasterCard criteria described in this documentation are not necessarily available for all payment methods.

The availability of the criteria configuration depends on the payment method. For some payment methods, the configuration is limited.

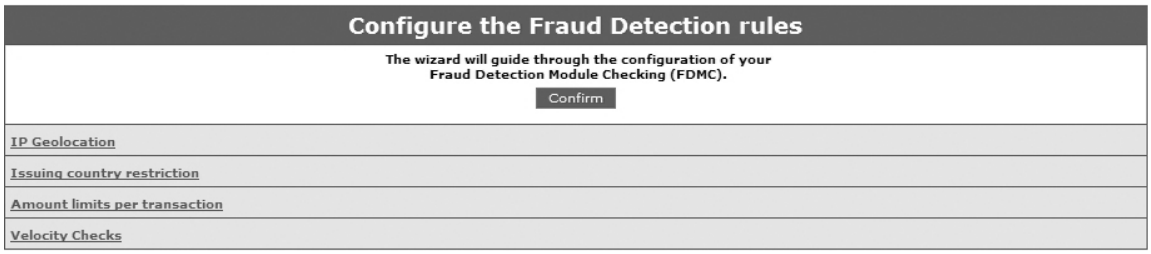
We recommend that you check the specific configuration for your individual payment methods by clicking the "Edit" button next to the payment method in the "Fraud detection activation and configuration" table in your Fraud Detection configuration screen.

# 2 Configuration Wizard

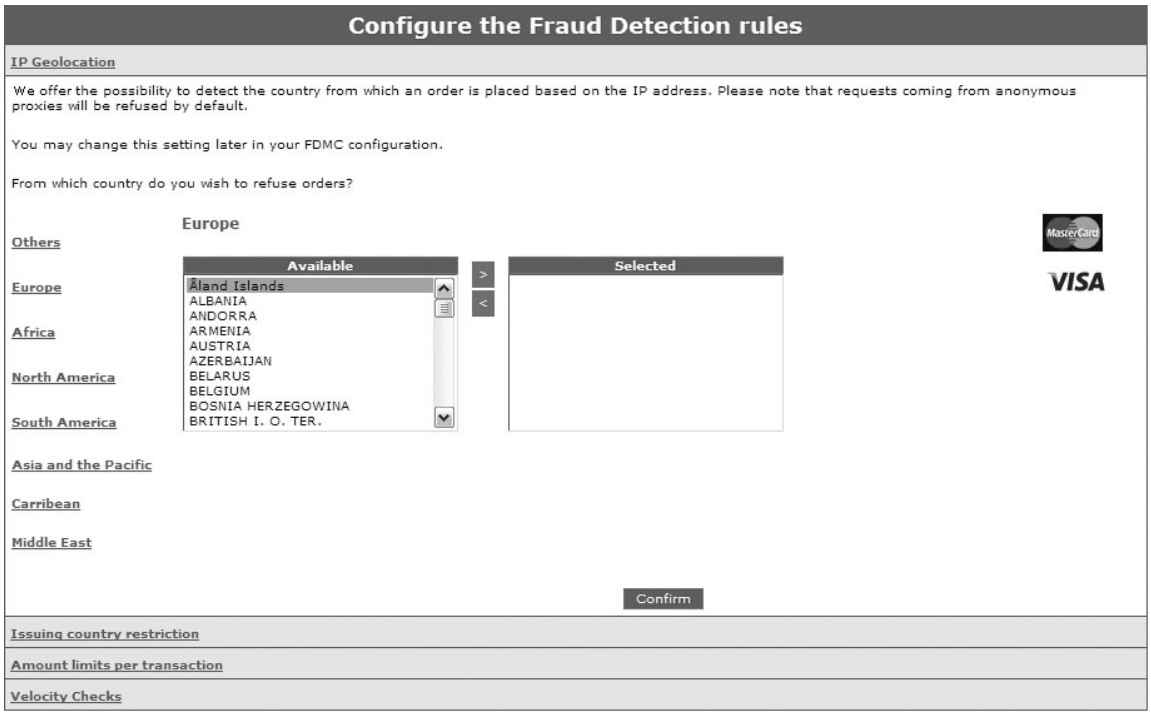
If the Fraud Detection Module has not been configured, a "Configure the Fraud Detection rules" link is visible on the merchant's home screen.

Clicking this link will take you through a configuration wizard, enabling you to follow an easy, step-by-step setup of the risk evaluation. Click on "Confirm" to launch the wizard.

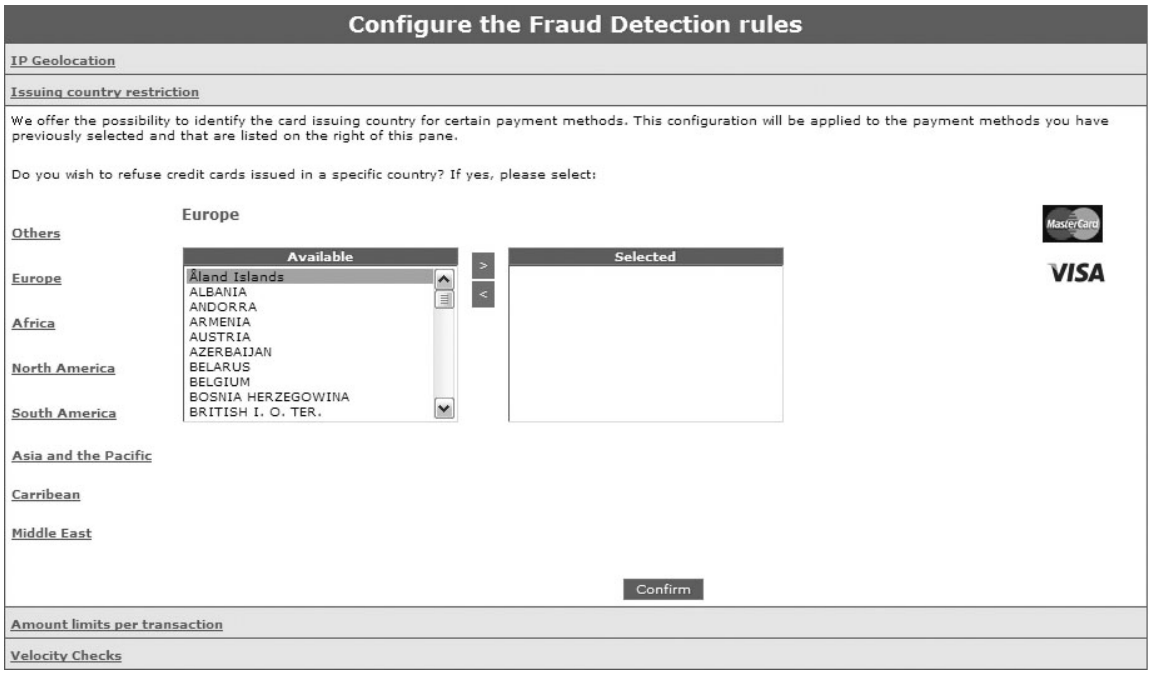
Welcome



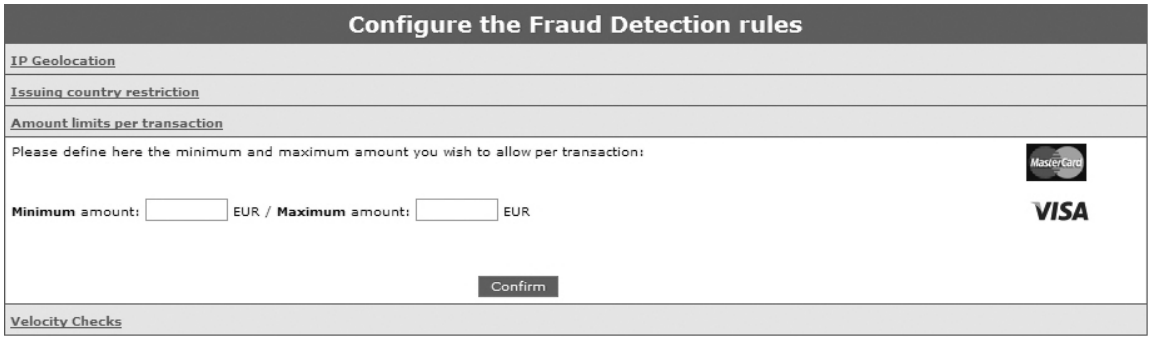

Step 1: IP Geolocation



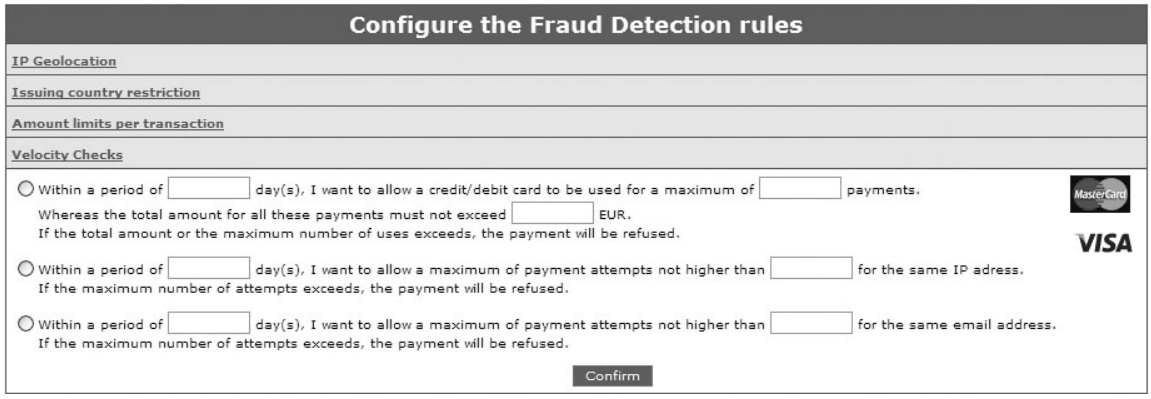

Step 2: Issuing country restrictions



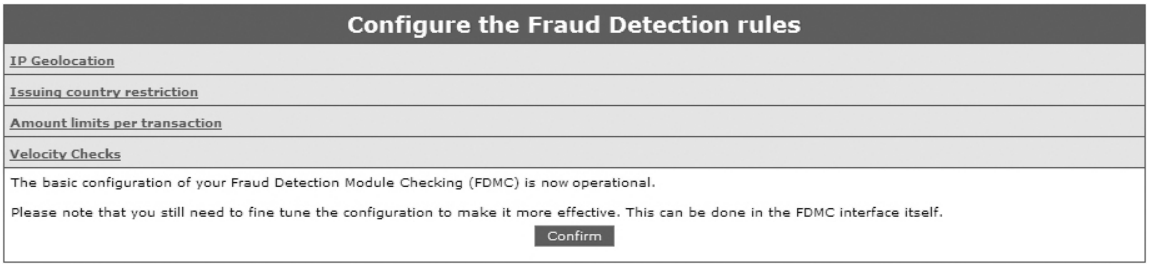

Step 3: Amount limits per transaction




Step 4: Velocity checks




Finished!



# 3 Fraud detection activation and configuration

In the “Fraud detection activation and configuration” table you will see the distinction between the credit cards and other payment methods. We will now take a closer look at the configuration of fraud detection options for credit cards.

To configure the fraud detection options for a specific credit card, click the “Edit” button next to the payment method. You will then see the Risk Evaluation page for this payment method with links to the configuration pages for the different rules, limits and lists.

The actual behaviour of these rules (i.e. whether they block or not) depends on your settings in the “Risk Evaluation” page.

## 3.1 Card country groups

All card countries are accepted by default. Here, the term ‘card country’ means the country in which the card was issued. Our system can identify the card country based on the card’s BIN code. The BIN code is the first 6 digits of a credit card number. A BIN code is linked to a specific bank in a specific country.

You can set a certain risk per card country. There are 3 possible categories to classify a card country:

- High risk
- Medium risk
- Low risk

High-risk card countries can lead to a transaction being blocked or a heightened risk evaluation; medium-risk card countries can lead to a heightened risk evaluation; and low-risk card countries will not be taken into account for risk evaluation.

## 3.2 IP country groups

All IP address countries are accepted by default. Our system can identify the IP address country based on your customer’s IP address. (Although this check gives positive results in 94% of all cases, this IP check is based on externally provided IP listings. There is a slight risk of error, as we rely on the accuracy of this list).

Just as for the card countries, you can set a certain risk per IP country. There are 3 possible categories to classify an IP country:

- High risk
- Medium risk
- Low risk

High-risk IP countries can lead to blocking a transaction or adding to risk evaluation, medium-risk IP countries can add to risk evaluation and low-risk IP countries will not be taken into account for risk evaluation.

Apart from these IP countries, there are also anonymous proxies. Anonymous proxies are internet access providers that allow internet users to hide their IP addresses. We strongly recommend you block transactions originating from anonymous proxies, in the risk evaluation page.

IMPORTANT

“Asia Pacific Network”, “European network”, and “Satellite Provider” refer to IP addresses for which the country of origin is uncertain.

"European network", for example, means that the exact IP country is uncertain but it belongs to Europe. Accepting "European network" as an IP address country does not mean you are accepting payments from all countries in Europe. It means you are accepting payments from IP addresses managed by European institutions (for instance an internet provider active in more than one European country, the European Commission, etc.).

Most of the time, the IP address country will be identical to the delivery country. The following delivery regions/countries are considered a risk in the acquirer world: Eastern Europe, Asia, Indonesia, Africa and the United States. However, if you do a lot of business in these regions/ countries or you have a specific delivery or order procedure to check the customer's identity, you do not need to set a high-risk level for these regions/countries.

## 3.3 Risky IP country / card country combinations

All IP country / card country combinations are accepted by default.

To configure an IP country / card country combination, select an IP country and a card country you want to combine it with, in the drop-down lists.

In the same way as for the card countries and IP countries, you can set a certain risk per IP country / card country combination. There are 3 possible categories to classify IP country / card country combinations:

- High risk
- Medium risk
- Low risk

High-risk combinations can lead to a transaction being blocked or a heightened risk evaluation; medium-risk combinations can lead to a heightened risk evaluation; and low-risk combinations will not be taken into account for risk evaluation.

## 3.4 Amount limit

You can limit the amount per transaction by entering a minimum and a maximum amount. The currency of the limit will be your main account currency. If you have multiple currencies and a transaction takes place in a currency other than your default one, our system will convert the limit into the other currency.

## 3.5 Utilisation limits

### 3.5.1 Card utilisation

You can set the "maximum utilisation per card, per period" based on the total amount of transactions per card and the number of transactions per card.

You have to configure this limit based on your business/products. If you sell a product a person will not buy more than once a week, for instance, you can limit the card utilisation to 1 time per week.

*Example*

If you do not want to accept more than two transactions on the same day for a certain credit card and you do not want to accept more than 250 EUR on that credit card within that day, you could configure:

- *Maximum utilisation per card, per period 1 day(s)*

- *Total amount of transactions per card, high threshold: 250 EUR*
- *Number of transactions per card, high threshold: 2*

As an advanced usage of this rule you can also set a low and a high threshold, which enables you to either mark a transaction for review (low threshold), or block it completely (high threshold).

The “maximum utilisation per card, per period” limit only applies to cards that were used in transactions resulting in any of the following statuses: 9, 91, 92, 5, 51, 52

### 3.5.2 IP utilisation

You can set the “maximum utilisation per IP address, per period” based on the number of successful transactions per IP address and the total number of transactions (accepted and refused) per IP address.

Fraudsters often work with a list of stolen credit cards, which they try out one by one. The result is that transactions with different cards will be sent from the same IP address. To be able to spot this, you can limit the number of transactions (accepted and refused) per IP address. When an “overuse” is reported to you, it is also important to look at the IP address history. In this way, you can stop the delivery of your goods when you see too many transactions from an IP address using different cards within a certain period of time.

*Example*

If you do not want to accept more than one successful transaction coming from the same IP address within 3 days, and you don’t want to accept more than 3 tries on that IP address in that period, you could configure:

- *Maximum utilisation per IP address, per period 3 day(s)*
- *Number of successful transactions per IP address, high threshold: 1.*
- *Number of transactions (accepted or refused) per IP add., high threshold: 3.*

As an advanced usage of this rule you can also set a low and a high threshold, which enables you to either mark a transaction for review (low threshold), or block it completely (high threshold).

### 3.5.3 Email utilisation

You can set the “maximum utilisation per email address, per period”, i.e. you can decide on the number of times a specific email address can be used within a certain period.

As an advanced usage of this rule you can also set a low and a high threshold, which enables you to either mark a transaction for review (low threshold), or block it completely (high threshold).

The "maximum utilisation per email address, per period" applies to transactions with all statuses.

## 3.6 Risky data

### 3.6.1 Risky Postcodes and Addresses

IMPORTANT

You only need to configure this page once. The configuration of the risky postcodes and addresses is valid for all payment methods.

You can set a certain risk per postcode/address. There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk postcodes or addresses can lead to blocked transactions or a heightened risk evaluation; medium-risk postcodes or addresses can lead to a heightened risk evaluation; and low-risk postcodes or addresses will not be taken into account for risk evaluation.

To configure your list, select the country, enter the postcode and street, click the "Add" button, and set the risk. Click the "Submit" to finish.

To use this functionality, make sure to send the following parameters with associated values in the order request from your website:

| Related input parameter | Format | Explanation | Example |
|---|---|---|---|
| OWNERZIP | AN (10) | Customer's ZIP/postcode | 75420 |
| OWNERADDRESS | AN (35) | Customer's address | Baker Street 221B |

*More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.*

## 3.6.2 Risky Periods (Time of order)

IMPORTANT

- You only need to configure this page once. The configuration of the risky periods is valid for all payment methods.
- The time zone used is CET!

You can set a certain risk per order period. There are 3 possible categories:

- High risk
- Medium risk
- Low risk

High-risk periods can lead to blocked transactions or a heightened risk evaluation; medium-risk periods can lead to a heightened risk evaluation; low-risk periods will not be taken into account for risk evaluation.

To configure the table, select the risk at the bottom of the table, tick the boxes you want to attribute this risk to and click the “Apply” button.

## 3.6.3 Risky Shipping Method

IMPORTANT

You only need to configure this page once. The configuration of the risky shipping methods is valid for all payment methods.

You can set a certain risk per shipping method. There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk shipping methods can lead to blocked transactions or a heightened scoring; medium-risk shipping methods can lead to a heightened scoring; and low-risk shipping methods will not be taken into account for scoring.

To configure your list, enter the shipping method, set the risk, and click the "Add" button. Click "Submit" to finish.

To use this functionality, make sure to send the following parameter with associated value in the order request from your website:

| Related input parameter | Format | Explanation | Example |
|---|---|---|---|
| ECOM_SHIPMETHODTYPE | Integer value: 1-5 | Delivery method<br>You can define and submit a value for each shipping (delivery) method. | 1: Pick up at merchant<br>2: Collection point (Post office, Kiala point...)<br>3: Collect at airport, train station or travel agency<br>4: Transporter (DHL, UPS...)<br>5: Download |

*More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.*

### 3.6.4 Risky Shipping Method Details

IMPORTANT

You only need to configure this page once. The configuration of the risky shipping method details is valid for all payment methods.

You can set a certain risk per entry. There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk shipping method details can lead to blocked transactions or a heightened scoring; medium-risk shipping method details can lead to a heightened scoring; and low-risk shipping method details will not be taken into account for scoring.

To configure your list, enter the value for Shipping Method Details, set the risk, and click the "Add" button. Click the "Submit" button to finish.

To use this functionality, make sure to send the following parameter with associated value in the order request from your website:

| Related input parameter | Format | Explanation | Example |
|---|---|---|---|
| ECOM_SHIPMETHODDETAILS | Free text (max. 50) | Identification of collection point | Post office KR124 |

*More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.*

### 3.6.5 Risky Product Categories

IMPORTANT

You only need to configure this page once. The configuration of the risky product categories is valid for all payment methods.

You can set a certain risk per product category. There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk product categories can lead to blocked transactions or a heightened scoring; medium-risk product categories can lead to a heightened scoring; and low-risk product categories will not be taken into account for scoring.

To configure your list, enter the product category, set the risk, and click the "Add" button. Click the "Submit" button to finish.

To use this functionality, make sure to send the following parameter with associated value in the order request from your website:

| Related input parameter | Format | Explanation | Example |
|---|---|---|---|
| ITEMFDMPRODUCTCATEGx | Integer value (1-19) | Product category<br>1: Food & gastronomy<br>2: Car & Motorbike<br>3: Culture & leisure<br>4: Home & garden<br>5: Appliances<br>6: Auctions and bulk purchases<br>7: Flowers & gifts<br>8: Computer & software<br>9: Health & beauty<br>10: Services for individuals<br>11: Services for professionals<br>12: Sports<br>13: Clothing & accessories<br>14: Travel & tourism<br>15: Hifi, photo & video<br>16: Telephony & communication<br>17: Jewelry & precious metals<br>18: Baby articles and accessories<br>19: Sound & light<br>(replace "x" with a number to send multiple items: ITEMFDMPRODUCTCATEG1, ITEMFDMPRODUCTCATEG2, etc.) | 14 |

| Related input parameter | Format | Explanation | Example |
|---|---|---|---|
| ITEMIDx | AN (15) | Item identification<br>(replace "x" with a number to send multiple items: ITEMID1, ITEMID2, etc.) | ab123 |
| ITEMPRICEx | N | Item price<br>(replace "x" with a number to send multiple items: ITEMPRICE1, ITEMPRICE2, etc.) | 1500 |
| ITEMQUANTx | N | Item quantity<br>(replace "x" with a number to send multiple items: ITEMQUANT1, ITEMQUANT2, etc.) | 3 |

*More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.*

### 3.6.6 Risky Time To Delivery

IMPORTANT

You only need to configure this page once. The configuration of the risky time to delivery is valid for all payment methods.

You can set a certain risk per time (amount in hours). There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk time to delivery can lead to blocked transactions or a heightened scoring; medium-risk time to delivery can lead to a heightened scoring; and low-risk time to delivery will not be taken into account for scoring.

To configure your list, enter the the value for time to delivery, set the risk, and click the "Add" button. Click the "Submit" button to finish.

To use this functionality, make sure to send the following parameter with associated value in the order request from your website:

| Related input parameter | Format | Explanation | Example |
|---|---|---|---|
| ECOM_SHIPMETHODSPEED | Integer value | The number of hours required for the delivery | 24 |

*More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.*

### 3.6.7 Risky Subbrands

IMPORTANT

You only need to configure this page once. The configuration of the risky subbrands is valid for all payment methods.

You can set a certain risk per subbrand. There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk subbrands can lead to blocked transactions or a heightened scoring; medium-risk subbrands can lead to a heightened scoring; and low-risk subbrands will not be taken into account for scoring.

To configure your list, enter the subbrand, set the risk, and click the "Add" button. Click the "Submit" button to finish.

### 3.6.8 Risky Issuer Numbers

IMPORTANT

You only need to configure this page once. The configuration of the risky issuer numbers is valid for all payment methods.

You can set a certain risk per number. There are 3 possible levels:

- High risk
- Medium risk
- Low risk

High-risk issuer numbers can lead to blocked transactions or a heightened scoring; medium-risk issuer numbers can lead to a heightened scoring; and low-risk issuer numbers will not be taken into account for scoring.

To configure your list, enter the issuer number, set the risk and click the "Add" button. Click the "Submit" button to finish.

## 3.7 Duplicate settings

On the right of each payment method in the "Fraud detection activation and configuration" overview, you see a "Duplicate" button. This button enables you to copy the settings configured for one payment method to one or more other payment methods in the list. Consequently, when you have several payment methods in your account, you don't have to make the same configuration multiple times.

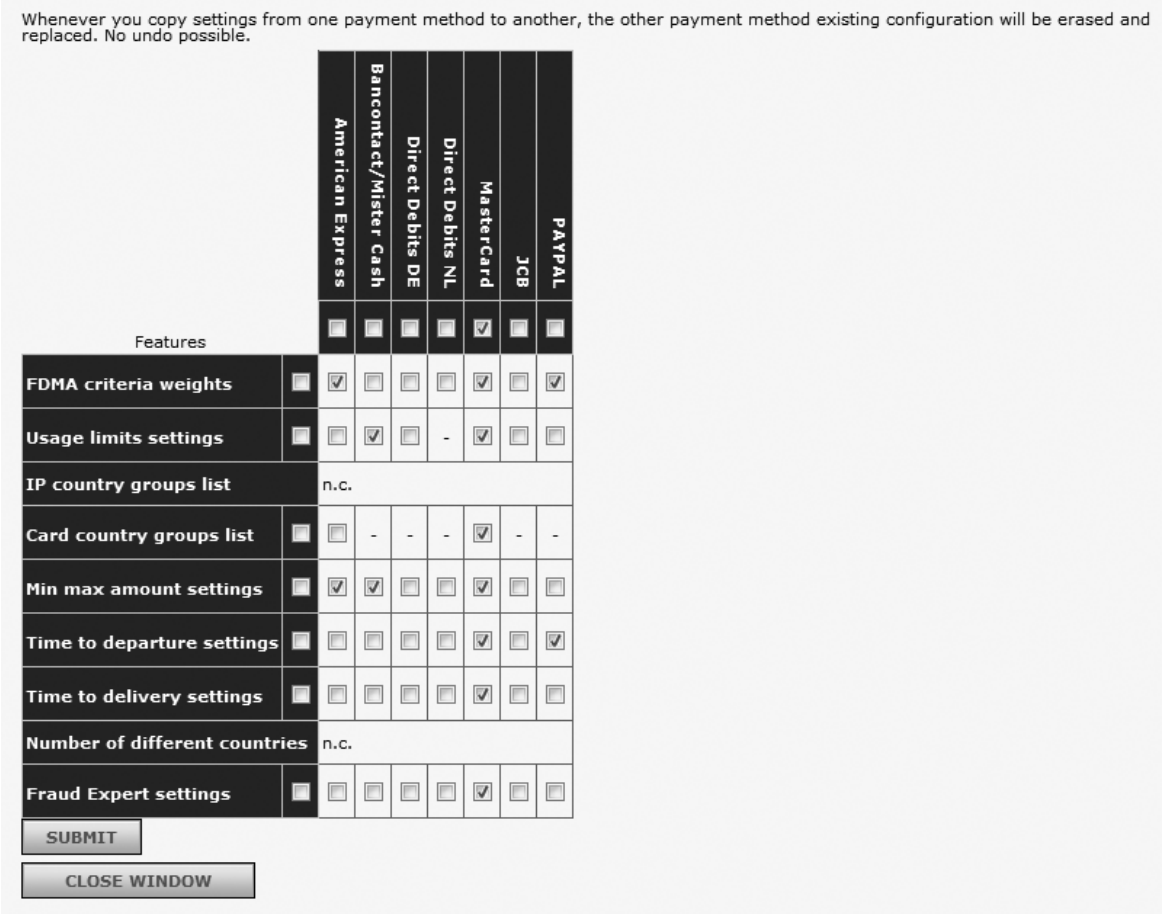
IMPORTANT

If you have already set up the fraud detection for a payment method to which you wish to copy settings from another payment method, the original settings will be overwritten by the copied settings.

The following settings can be copied, depending on whether the intended payment method supports them:

- FDMA criteria weights
- Usage limits settings
- IP country groups list
- Card country groups list
- Min max amount settings
- Time to departure settings
- Time to delivery settings
- Number of different countries
- Fraud Expert settings

*Example*



Whenever you copy settings from one payment method to another, the other payment method existing configuration will be erased and replaced. No undo possible.

| Features | | American Express | Bancontact/Mister Cash | Direct Debits DE | Direct Debits NL | MasterCard | JCB | PAYPAL |
|---|---|---|---|---|---|---|---|---|
| | | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ |
| FDMA criteria weights | ☐ | ☑ | ☐ | ☐ | ☐ | ☑ | ☐ | ☑ |
| Usage limits settings | ☐ | ☐ | ☑ | ☐ | - | ☑ | ☐ | ☐ |
| IP country groups list | | n.c. | | | | | | |
| Card country groups list | ☐ | ☐ | - | - | - | ☑ | - | - |
| Min max amount settings | ☐ | ☑ | ☑ | ☐ | ☐ | ☑ | ☐ | ☐ |
| Time to departure settings | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☑ |
| Time to delivery settings | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ |
| Number of different countries | | n.c. | | | | | | |
| Fraud Expert settings | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ |

SUBMIT

CLOSE WINDOW

# 4 3-D Secure

3-D Secure offers an additional level of security, as it allows customers to be identified unambiguously through technologies – such as html passwords, Digipass, card readers, biometrics, etc. – implemented by the issuing banks.

By offering 3-D Secure, a merchant benefits from a conditional payment guarantee (see here), as described in the 3-D Secure contract with his acquirer. Under these conditions, a merchant's account is no longer debited for disputes over "non-identification of the cardholder". (This does not extend to disputes over other matters!)

At least the following brands have implemented the 3-D Secure protocol:

- Visa under the name of Verified by Visa
- MasterCard under the name of SecureCode
- JCB under the name of J-Secure
- American Express under the name of SafeKey

## 4.1 General

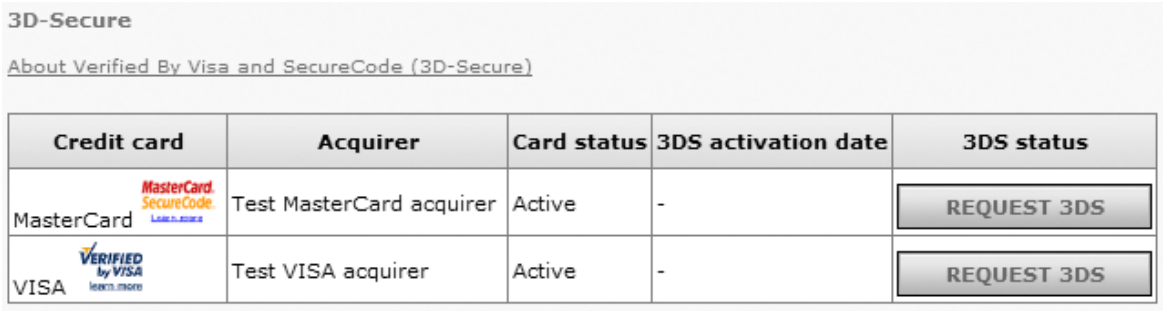
### 4.1.1 Affiliation request

If 3-D Secure is not activated for your account, you will see a “Request 3DS” button in the “3-D Secure” table.

If you click this “Request 3DS” button, an email will be sent to your acquirer. If your contract with your acquirer does not provide for 3-D Secure, you can contact your acquirer for more information on registering for 3-D Secure, if you would like your acquirer to provide the 3-D Secure payment option.

Note: To enroll for SafeKey, please contact American Express or go to the SafeKey portal.

Once 3-D Secure has been enabled in your account you will see the activation date in the table. You can change the configuration for 3-D Secure by clicking the ‘edit’ button next to the payment methods.




### 4.1.2 Standard 3-D Secure transaction processing

1. When we receive the credit card details from your customer, our system sends a request to the VISA/MasterCard/JCB/AmEx directory to establish whether the card is registered, i.e. the cardholder has received some means of identification linked to his/her card and, if appropriate, obtains the issuer authentication server data.

2. If the card is registered, our system redirects the buyer to the issuer authentication server to initiate the authentication.

3. Our system receives the result of the authentication and processes the payment in the usual way.

If authentication is successful, the merchant can benefit from the conditional payment guarantee provided by his acquirer.

If the card is not registered, the merchant receives some level of conditional payment guarantee provided by his acquirer.

In both cases therefore under certain conditions (defined by VISA, MasterCard and financial organisations, and as described in the 3-D Secure contract with his acquirer), the merchant has a payment guarantee, even without receiving identifying information from the customer. These conditional payment guarantee rules are exclusively managed between the merchant and his acquirer. ePDQ only acts as a technical intermediary.

## 4.2 Configuration options

The following are the configuration options for Verified by Visa, MasterCard SecureCode, JCB J-Secure and AmEx SafeKey. Depending on your acquirer, some (or all) of these options might be inaccessible.

### 4.2.1 Technical problem

The merchant can choose to *continue* or *interrupt* the transaction if a technical problem prevents connection to the VISA/MasterCard/JCB/AmEx directory during the 3-D Secure registration check.

If a technical problem prevents our system from connecting to the VISA/MasterCard/JCB/AmEx directory (step 1), VISA/MasterCard/JCB/AmEx recommends that the process should be continued without authentication (*continue* option). In this case, however, the merchant will not benefit from the conditional payment guarantee (see here).

### 4.2.2 Identification service temporarily unavailable

The merchant can choose to *continue* or *interrupt* the transaction, if the cardholder identification service is temporarily unavailable.

If the issuer authentication server is temporarily unavailable (step 2), cardholder identification is not possible. In this event, VISA/MasterCard/JCB/AmEx recommends continuing the process (*continue* option). In this case however, the merchant will not benefit from the conditional payment guarantee (see here).

### 4.2.3 Authentication fails (MasterCard only)

The merchant may choose to *continue* or *interrupt* the transaction, should the authentication fail.

Should cardholder authentication fail (step 3), MasterCard recommends interrupting the payment processing be interrupted (*interrupt* option). If the transaction continues, the merchant will not benefit from the conditional payment guarantee (see here).

### 4.2.4 Activate/Deactivate 3-D Secure

Here the merchant can switch on/off 3-D Secure for all VISA/MasterCard/JCB/AmEx cards.

> WARNING
>
> If 3-D Secure is disabled, the merchant will not benefit from the conditional payment guarantee (see here).

# 5 Blacklists, Greylists and Whitelists Configuration

In the advanced Fraud Detection Module, you can generate your own blacklists and greylists for credit cards, based on BIN codes, credit card numbers, email addresses, phone numbers, names, generic data and IP addresses from which you do not wish or might not wish to accept transactions. There are also two whitelists, based on IP addresses and a Client unique identifier.

The actual behaviour of these lists (i.e. whether they block or not) depends on your settings in the Risk Evaluation page.

"No", in the main menu, indicates that nothing has been configured in the blacklist/greylist/whitelist concerned. When a blacklist/greylist/whitelist has been configured, the status will be "Yes".

## 5.1 General list functionalities

### 5.1.1 Entries

In the advanced Fraud Detection Module there is no limit to the number of entries in the lists. You can enter up to 1000 items at a time in the submission text box.

You can always delete entries in your lists by enabling the boxes in the "Delete" column and clicking the "Submit" button.

### 5.1.2 Comments

You can add a comment to an entry in a blacklist, greylist or whitelist.

You can either enter the comment in the "Comment" field when an item is submitted. All items entered during this submission will then have the same comment.

You can also add or delete a comment by clicking the "..." link in the comment column.

### 5.1.3 Reason

For each entry in a blacklist or greylist, you can select a reason why you want to enter the data: actual fraud or commercial dispute.

IMPORTANT

Only select "actual fraud" if the customer really has committed fraud, e.g. when a cardholder uses a card that does not belong to him.

### 5.1.4 Filter

You can filter the data in the lists using the "Filter" button at the top of the table. You can filter by date and list content.

You can remove a filter by clicking the "Remove filter" button.

### 5.1.5 List downloads

You can download the list content in an excel file by clicking the "Download List" button at the top of the table.

If you click the "Download List" button when you have applied a filter, the filtered content will be downloaded.

### 5.1.6 Blacklist hit warning

In the blacklists you can enable a radio button in order to send a warning email when a blacklist is hit.

IMPORTANT

You only need to enable/disable this option once. The configuration of this option is valid for all blacklists.

## 5.2 Whitelists

Whitelists contain data from privileged customers and/or data used to override other rules (depending on the merchant's risk evaluation settings).

### 5.2.1 IP address whitelist

You can enter IP addresses of customers you'd like to receive orders from, in the trusted IP addresses list. If a customer's unique IP address is in this whitelist, this can override all IP-related blocking rules (depending on the merchant's risk evaluation settings).

In order for our system to check the customer's IP address, merchants working via DirectLink need to send the IP address in the "REMOTE_ADDR" field.

### 5.2.2 Unique customer identifier whitelist

The Customer Unique Identifier (CUI) is an identifier allocated by the merchant to his customer. It can be a name, customer number, email address etc. If the merchant wishes to use this, the CUI has to be sent in an additional field called "CUID" (alpha-num, 50 characters max.).

If a customer's unique CUI is in this whitelist, this can override all other blocking rules (depending on the merchant's risk evaluation settings), except the card blacklist.

## 5.3 Blacklists / Greylists

Blacklists contain such data as credit card numbers, IP addresses, email addresses, etc. from which you do not wish to accept transactions, based on previous (fraud or commercial dispute) experiences.

Greylists contain "doubtful" data waiting either to be transferred to your blacklist or to be deleted. Greylists contain data you are not 100% sure should belong on your blacklists. Greylist data can not lead to blocking a transaction.

*Example*: You have had issues with transactions coming from a specific IP address but are not sure this IP address is a dedicated IP address belonging to one individual. The IP address might also represent a whole company/building or might shortly be attributed to another person by the provider.

In this case, you would not want to put this IP address in your IP address blacklist straight away, as you do not want to disadvantage/block other potential customers. You can put the IP address in the IP address greylist until you are sure whether to move it to your IP address blacklist or delete it from the greylist.

You can move data from the greylist to the blacklist by selecting the boxes in the "Move to blacklist" column of the greylist and clicking "Submit".

### 5.3.1 Card number

In your credit card blacklist/greylist, you must enter the full credit card number.

In the card blacklist, you can enable a radio button in order to greylist the IP address of transactions with a card blacklist match.

If you have activated the Direct Debits NL, Direct Debits DE or Direct Debits AT payment methods in your account, the card blacklist/greylist will also double as an account blacklist/greylist for entering bank account numbers.

### 5.3.2 BIN

The BIN code is the first 6 digits of a credit card number. A BIN code is linked to a specific bank in a specific country. Consequently, you can enter all credit cards issued by bank X in country Y into your list, simply by adding the BIN code.

### 5.3.3 IP address

In your IP addresses blacklist or greylist, you can enter not only a specific IP address, but also a range of IP addresses using the following formats: a.b.c-d.0-255 or a.b.c-d.* or a.b.c.d-e.

In order for our system to check the customer's IP address, merchants working via DirectLink need to send the IP address along in the "REMOTE_ADDR" field.

### 5.3.4 Email address

The email address can be a fixed address or a whole range of addresses (domain), which is indicated by an asterisk ('*') in front of the '@' sign. The email address entered by the merchant will appear in the "Email" column. Based on this email address, our system will generate the "Partial match".

For our system to be able to check the customer's email address, the merchant must also send the email address in the order details.

### 5.3.5 Name

The merchant can enter customer names in the blacklist or greylist. The name entered by the merchant will appear in the "Name" column. Based on this name, our system will generate two other versions of the name: the "Cleaned name" and the "Partial match".

For our system to be able to check the name, the merchant must also send the customer's name in the order details.

### 5.3.6 Phone number

The merchant can enter the customer's phone number in the blacklist or greylist. The phone number entered by the merchant will appear in the "Phone number" column. Based on this phone number, our system will generate two other versions: the "Cleaned number" and the "Partial match".

For our system to be able to check the customer's phone number, the merchant must also send the phone number in the order details.

### 5.3.7 Generic data

The generic data blacklist and greylist allow the merchant to have a fully personalised list where he can enter data he wishes to take into account for the transaction fraud risk. The data needs to be alphanumeric and must not exceed 50 characters.

For our system to be able to check the generic data, the merchant must also send the data along in the "GENERIC_BL" field in the order (alpha-num, 50 characters max).

# 6 Risk Evaluation

A list of criteria can be found in the Risk Evaluation page which contains all the criteria that can be defined in the Fraud Detection Module.

IMPORTANT

In contrast to the basic Fraud Detection Module, where the blocking behaviour is set in the blacklists/whitelists, blocking rules, etc., the merchant configures the actual behaviour of the blacklists/greylists/whitelists, along with the limits and rules, in the Risk Evaluation list.

An action can be specified for each criterion.

- Block
- Review
- None
- Override Blocking

Not all options are available for all criteria.

- If one of the criteria is matched with a “Blocking” Action, the transaction will be blocked and we will set its status to “Authorisation declined”.
- If one of the “Review” criteria is matched, the transaction will have to be reviewed manually.
- Otherwise, the transaction is considered as non-fraudulent.

Conditions: Because some information originates from externally provided listings, we rely on their correctness and cannot guarantee a 100% correct result.

The following is a (non-exhaustive) selection of evaluation criteria:

- *3-D Secure*: when the cardholder is fully 3-D Secure authenticated (identification OK) and the cardholder is not registered. When a credit card is 3-D Secure and you have a 3-D Secure contract with your acquirer, you will have a conditional payment guarantee (see Section 2.1.2) for the transaction. So even if you do not wish to receive payments from certain card or IP countries due to a high risk of fraud, you can still permit transactions with 3-D Secure credit cards from these countries, as the risk is much lower.
- *Anonymous proxies*: Anonymous proxies are internet access providers that allow internet users to hide their IP addresses. We recommend that you do not accept payments originating from an anonymous proxy!
- *Free email*: fraudsters mostly use fake email accounts created via free email services. Our system will check (based on externally provided listings) if the customer’s email address is free or not. The merchant can decide to add a risk risk evaluation to transactions where the customer's email address is a free email address. For our system to be able to check the customer’s email address, the merchant must also send the email address in the order details.
- *Number of different countries*: The merchant can indicate the number of different countries (card country for VISA/MasterCard/American Express, IP country, invoicing address country if sent) he allows and set the risk evaluation action if the number exceeds the set limit.
- *IP country is different from the CC country* (for VISA, MasterCard and American Express only): when you set this parameter to “Block transaction”, you only allow transactions to pass if the customer’s IP address is in the same country as his credit card issuer, in other words: only if the card country and IP address country are identical. This check is not performed if the IP address comes from an anonymous proxy, the Asia Pacific network, the European network or a satellite provider.
- *Invoicing address different to delivery address*: this indicates whether the invoicing address is considered to be different from the delivery address, based on the value of the extra field “addMatch” which the merchant sends us in the order details. If the value is “1” the invoicing and delivery address will be considered identical. If the value is “0” they will be considered different from each other.
- *Amount limit, Utilisation limits*

- *CUI whitelist identification*
- *Trusted IP address*
- *Card/BIN/IP address/email/phone/cardholder name/generic data in blacklist and greylist*
- *High and medium-risk card countries, High and medium-risk IP countries, High and medium-risk postcodes, High and medium-risk order times*

IMPORTANT

We strongly recommend setting the following risk evaluation criteria to “Block” in the risk evaluation page:

- Card in blacklist
- Anonymous proxy (under IP country)

# 7 Filters

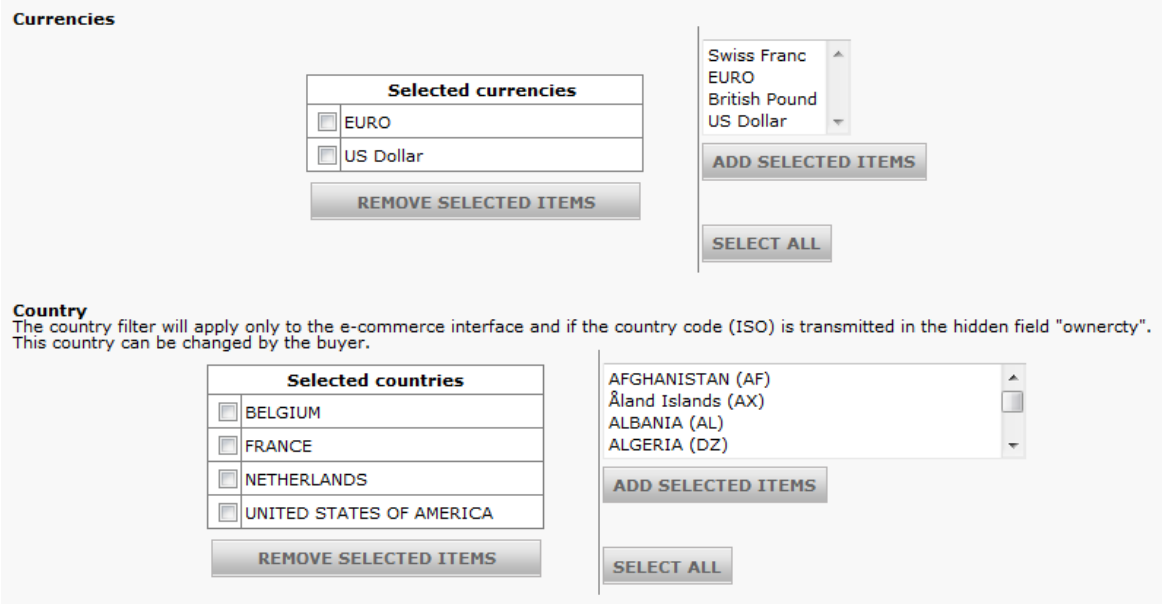
Filters are applicable before the customer has chosen his payment method. You can choose to hide specific payment methods from customers from a certain country or from customers paying in a certain currency on the orderstandard.asp page (e-commerce).

To configure a filter for a specific payment method, go to the payment method configuration page ("Payment methods" link in the menu) and click the "Edit filter" button next to the payment method.

If you do not set a filter, the payment method will be shown to all customers. If you wish to limit your payment method to certain currencies or countries, you can select them from the lists on the right-hand side of the screen.

Important: Before our system can apply the filters you set, you must either send your customer's country code in the "ownercty" hidden field for each transaction, or enter "?" in the "ownercty" field if you want our system to automatically detect your customer's country from his IP address. (Please refer to the e-Commerce Integration Guides for further information.)

The next screenshot shows the choice of EUR and USD as payment currencies that can be used for VISA transactions from Belgium, France, the Netherlands and the USA. If a customer has to pay an amount in GBP from the UK, he will not see VISA as a payment method in your payment methods list.



# 8 Feedback

## 8.1 Transaction view in the back office

### 8.1.1 Advanced selection criteria

When you look up a transaction via the “View transactions” or “Financial history” link in your account menu, you will have two extra criteria in the “Advanced selection criteria”: Risk category and IP address.

In the “Risk category” you can select transactions of a certain colour.

You can use the IP address field to look up all transactions from the same IP address or from IP addresses starting with the same digits.

### 8.1.2 Transaction List

When you display your transaction list via “View transactions” or “Financial history” in your back office, you will notice the risk category with the matching colour in the list, under the "Rating" column. When you click on the risk, you will be directed to the risk evaluation details for the transaction.

When there is no risk evaluation result for the transaction, e.g. when the authorisation has been declined, you will notice green and blue check icons in the list (if you have 3-D Secure activated for your account).

The green check icon represents a 3-D Secure transaction where the customer paid with a 3-D Secure registered credit card. With these transactions, your acquirer provides you with a conditional payment guarantee.

The blue check icon represents a 3-D Secure transaction where the customer has paid with a credit card that is not 3-D Secure registered. These transactions involve a certain level of conditional payment guarantee, based on the specific details in the 3-D Secure contract with your acquirer.

Transactions with no icon at all are transactions that have not been processed using 3-D Secure. The conditional payment guarantee will not apply to these transactions.

Transactions with an exclamation mark indicate transactions where the customer’s authentication failed. The conditional payment guarantee will not be applicable for transactions which you chose to proceed with (*continue*) where the authentication failed (for MasterCard, see here).

*For more information about the conditional payment guarantee, see here*

### 8.1.3 Transaction details

In the transaction details (financial page), you will see additional information such as the card verification code result (if the CVC code has been entered by the customer), card country, IP address country and IP address, as well as the Risk Category.


#### 8.1.3.1 Dispute

The “Dispute” button will lead you to a page where you can add certain transaction details to your blacklists. This option allows you to add to your blacklist the card number used for the transaction without having to know the full card number, for instance.

You can also simply mark the transaction as a commercial dispute or fraud.

IMPORTANT

Only select "actual fraud" as the type if the customer really has committed fraud with this card, for instance when a cardholder uses a card that does not belong to him.


### 8.1.3.2 View transactions from same IP address

When you click the "View transactions from the same IP address" button, a list will be displayed containing all the transactions originating from the same IP address within a certain period.

### 8.1.3.3 View risk evaluation details

When you click the "View risk details" button, you can consult additional information concerning the risk evaluation calculation. You will see a list of risk evaluation criteria that have been taken into account for the calculation, along with the risk evaluation result. Criteria that have been met are highlighted in bold typeface in the criteria list.

| Criteria | Value | Comment |
|---|---|---|
| 3-D Secure | - | **No** : ECI : 7 |
| CUI whitelist identification | - | **No** : Client Identification : - |
| **Trusted IP address** | - | **Yes Criteria overriding**: Received IP address : 10.0.1.128 |
| Card in greylist | - | **No** : Card number / Account number : XXXXXXXXXXXX1111 |
| IP address in greylist | - | **No** : Received IP address : 10.0.1.128 |
| Card holder name in name greylist | - | **No** : Card owner name : hva |
| IP country | - | **No** : IP country : 99 / Country not found |
| **IP cty <> CC cty** | **Review** | **Yes** : Card country / IP country : US / 99 |
| **Max utilization / card, low threshold** | **Review** | **Yes** : number of utilisations for the card : 2 |
| **Max amount / card, low threshold** | **Review** | **Yes** : amount for the card : 2.00 EUR |
| **Max utilization / IP, low threshold** | **Review** | **Yes** : number of utilisations for the IP add. : 2 |
| Unauthorized card country/IP country combination | - | **No** : Card country: US / IP country: 99 |
| | - | **Category: Orange (O)** |

Fraud-trail analysis

In the risk evaluation details page, you can compare the transaction to transactions that have been registered with the same card number, BIN, IP address, email address, cardholder name, credit card country and IP address country within a certain period which you can define.

You can tick one or more search criteria boxes and select the logical operator you would like to

apply to the selected search criteria (AND or OR). When you click the "Start lookup" button, we will retrieve all transactions matching the selected criteria.

The first lookup will be based on the values of the original transaction, so for each criteria there is one value we will check. When you perform the next lookup ("Start lookup 2", "Start lookup 3", etc...) we will search in the results of the previous lookup. In successive lookups, the criteria can have multiple values, multiplying the results and uncovering possible fraud trails.

### 8.1.4 Error codes

When a transaction has been retained by our system based on the rules you set in the Fraud Detection Module, you will find the reason in the error message for the transaction. With a few exceptions, all error codes related to Fraud detection begin with "300011", followed by two more digits.

*More information about statuses and error codes can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.*

The following non-exhaustive list contains examples of the most relevant ones:

3 / 30001100 Unauthorised customer country

3 / 30001120 IP address on merchant's blacklist

3 / 30001130 BIN on merchant's blacklist

3 / 30001140 Card on merchant's blacklist

3 / 30131002 You have reached the total amount permitted

3 / 30001102 Number of different countries too high

3 / 30001141 E-mail on blacklist

3 / 30001142 Passenger name on blacklist

3 / 30001143 Cardholder name on blacklist

3 / 30001144 Passenger name different from owner name

3 / 30001145 Time to departure too short

3 / 30001154 You have reached the permitted usage limit

3 / 30001155 You have reached the permitted usage limit

## 8.2 Supplementary transaction parameters

In your post-sale requests, redirections with feedback, file downloads and DirectLink XML responses, supplementary transaction parameters relating to risk evaluation will be returned.

The list of supplementary parameters is set out below.

These fields will be empty if a format validation error occurred for the transaction details.

| Parameter | Value |
|---|---|
| IPCTY | Originating country of IP address.<br>Format: 2-character alphabetic ISO code. If this parameter is not available, “99” will be returned in the response.<br>This IP check is based on externally provided IP listings, so there is a slight risk of error, as we rely on the correctness of this list. The check gives positive results in 94% of all cases. |
| CCCTY | Originating country of credit card.<br>This is only available for VISA, MasterCard and American Express. This value |

| Parameter | Value |
|---|---|
| | will be empty for all other brands/payment methods. Format: 2-character alphabetic ISO code. If this parameter is not available, “99” will be returned in the response.<br><br>This credit card country check is based on externally provided listings, so there is a slight risk of error, as we rely on the correctness of this list. The check gives positive results in 94% of all cases. |
| ECI | Electronic Commerce Indicator. The possible ECI values and their meaning are set out below:<br><br>1 Manually keyed<br><br>2 Recurring payments<br><br>3 Instalment payments<br><br>5 Cardholder identification successful<br><br>6 Merchant supports identification but not cardholder, conditional payment guarantee rules apply (see here)<br><br>7 E-commerce with SSL encryption<br><br>9 Recurring after first E-Commerce transaction<br><br>12 Merchant supports identification but not cardholder, conditional payment guarantee rules apply (see here) (idem 6)<br><br>91 Cardholder identification FAILED !!!! (Conditional payment guarantee (see here) may apply. Please check with your acquirer)<br><br>92 Issuing bank authentication site temporarily unavailable, but transaction continued |
| CVCCHECK | Result of the card verification code check. Possible values:<br><br>KO The CVC has been sent but the acquirer has given a negative response to the CVC check, i.e. the CVC is wrong.<br><br>OK 1. The CVC has been sent and the acquirer has given a positive response to the CVC check, i.e. the CVC is correct OR<br><br>2. The acquirer sent an authorisation code, but did not return a specific result for the CVC check.<br><br>NO All other cases. For instance, no CVC transmitted, the acquirer has replied that a CVC check was not possible, the acquirer declined the authorisation but did not provide a specific result for the CVC check, etc. |
| AAVCHECK | Result of the automatic address verification. This verification is currently only available for American Express. Possible values:<br><br>KO The address has been sent but the acquirer has given a negative response for the address check, i.e. the address is wrong.<br><br>OK 1. The address has been sent and the acquirer has returned a positive response for the address check, i.e. the address is correct OR<br><br>2. The acquirer sent an authorisation code but did not return a specific response for the address check.<br><br>NO All other cases. For instance, no address transmitted; the acquirer has replied that an address check was not possible; the acquirer declined |

| Parameter | Value |
|---|---|
| | the authorisation but did not provide a specific result for the address check, etc. |
| VC | Virtual card. Possible values:<br>ECB: For E Carte Bleue<br>ICN: For Internet City Number<br>NO: All other cases. For instance, the card is not a virtual card, the card is a type of virtual card not known to us, etc. |
| IP | Customer's IP address, as detected by our system in a 3-tier integration, or sent to us by the merchant in a 2-tier integration. |

Advanced Fields

| | |
|---|---|
| NBRUSAGE | Number of times a credit card has been used during a certain period (when the "maximum utilisation per card, per period" rule is configured). |
| NBRIPUSAGE | Number of times an IP address has been used during a certain period (when the "maximum utilisation per IP address, per period" rule is configured). |
| SCO_CATEGORY | The colour of the category the end risk belongs to, based on the settings in the risk evaluation page (Multi-criteria selection of the payment methods > risk evaluation).<br>The possible values are G (for green), O (for orange) and R (for red). |

*More information about these fields can be found in your ePDQ account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.*

# 9 Appendix: Travel

If you hold an account with travel functionalities, you can configure additional rules and criteria in the risk evaluation page.

## 9.1 Passenger name

All passenger names (with a limit of 6) are taken into account for the risk evaluation, not just the primary passenger. The merchant can set a risk for three criteria linked to the passenger name (s):

- Passenger name on blacklist
- Passenger name on greylist
- Passenger name different from cardholder name

The blacklist/greylist used for the passenger name is the name blacklist/greylist.

## 9.2 Itinerary

### 9.2.1 Airport groups (Risky itinerary)

You can set a risk category per airport, which we will take into account when calculating the risk of your customer's itinerary (if you have configured the Risky Itinerary criterion in the risk evaluation page).

There are 3 possible categories to classify an airport:

- High risk
- Medium risk
- Low risk

High-risk countries and medium-risk countries can increase the risk evaluation; low-risk countries will not be taken into account for risk evaluation. Only enter medium or high-risk airports. Low-risk airports will not be taken into account and will not be listed.

To configure your list, enter the airport (e.g. "VIE" for Vienna), set the risk and click the "Submit" button.

You can also indicate whether you want stopovers to be taken into account for the risky itinerary calculation.

### 9.2.2 One-way ticket

Since one-way tickets are more risky than return tickets, you can add an extra risk for this criterion.

### 9.2.3 Departure airport

You can indicate departure airports which have a lower risk for you and assign an extra risk to all others by configuring the "Departure airport not in trusted list" criterion in the risk evaluation page.

The departure country is also taken into account for the "number of different countries" item.

### 9.2.4 IP country / airport list

The IP country / airport list allows you to configure a list of airports of which at least one must be included in the itinerary if the reservation is made in a specific IP country.

To configure the IP country / airport list, select one or more IP countries in the list and enter the airports in the text fields next to the IP country.

*Examples*

IP address: AT Airport list: GRZ, INN, KLU, LNZ, SZG, VIE

If a customer makes a reservation in Austria (i.e. the customer's country/IP country is “AT” for Austria), his flight itinerary must include either Graz Airport, Innsbruck Airport, Klagenfurt Airport, Linz Airport, Salzburg Airport, or Vienna International Airport.

IP address: BE Airport list: BRU, AMS, CDG

If a customer makes a reservation in Belgium (i.e. the customer's country/IP country is “BE” for Belgium), his flight itinerary must include either Brussels Airport, Amsterdam Schiphol Airport or Paris - Roissy Charles de Gaulle Airport.

## 9.3 American Express: Enhanced Authorization

The Enhanced Authorization tool of American Express helps travel merchants to reduce fraud and fraud chargebacks, by submitting various transaction parameters and shipping information that American Express holds against positive and negative data. This way AmEx can provide an improved authorisation response.

If a merchant submits travel details, not all required fields are submitted to the AmEx authorisation host. Therefore the merchant must submit the following parameters:

| Parameter | Explanation |
|---|---|
| CN | Card holder name |
| OWNERTELNO | Telephone number |
| EMAIL | Email address |
| IP | IP address |

Enhanced Authorization is a service that is free to all American Express merchants. It is active by default if the merchant's UID (affiliation number) is configured with the AmEx GCAG specifications. The merchant must check with AmEx whether or not that is the case.

To be able to make use of the Enhanced Authorization tool via ePDQ, the merchant must have a flag enabled in his ePDQ account. Therefore the merchant must contact our Customer Care.

## 9.4 Time to departure

A ticket bought for a departure in two days is far riskier than a ticket bought for a departure in a month. You can configure the time to departure criterion in the risk evaluation page to add an extra risk for three different times to departure.

Always start with the shortest time to departure (adding a higher risk).

# 10 Appendix: Parameters vs. Checks/Rules

| ePDQ parameter | Description | Rules/Checks in FDMA |
|---|---|---|
| CN | The cardholder name can contain a maximum of 35 characters. This parameter can be sent via ePDQ e-Commerce, DirectLink and Batch. Please note that for ePDQ e-Commerce the cardholder's name will also be captured via the ePDQ payment page, where the cardholder's name is a mandatory field. | • Name blacklist<br>• Name greylist<br>• Passenger name different from cardholder name. |
| OWNERADDRESS | Customer's address may contain a maximum of 35 characters | • Invoicing address is a P.O. Box |
| ADDRMATCH | Whether the billing address is considered different from the delivery address is based on the value of the extra field "ADDRMATCH" the merchant sends us in the order details. If the value is "1" the billing and shipping address will be considered identical. If the value is "0" they will be considered different one from the other.<br>(the parameter "ADDMATCH" can alternatively be used) | • Billing address different from shipping address |
| OWNERZIP | Customer's zip/postal code may contain a maximum of 10 characters. | • Risky zip/postcodes<br>• Advanced address verification check for specific card brands only |
| OWNERTELNO | Customer's telephone number may contain a maximum of 30 characters for all ePDQ modules with the exception of ePDQ Batch which has a maximum of 20 characters. Special characters ("+" or "/" for instance) are allowed in this field. It's best to be consistent in the way you send the phone numbers. | • Telephone number greylist<br>• Telephone number blacklist |
| OWNERCTY | Customers invoicing country may contain a maximum of 2 characters. Country in ISO 3166-1-alpha-2 code as can be found on http://www.iso.org/iso/en/prodsservices/iso3166ma/02iso-3166-code-lists/list-en1.html. | • Number of different countries |
| EMAIL | Customer's email address may contain a maximum of 50 characters. | • Email in blacklist<br>• Email in greylist<br>• Free email<br>• Utilisation limits |
| Generic_BL | Generic blacklist may contain a maximum of 50 characters. | • Generic blacklist<br>• Generic greylist |
| REMOTE_ADDR | IP address of customer.<br>This only needs to be sent when making use of ePDQ DirectLink. For ePDQ e-Commerce the IP-address is automatically detected and registered. | • IP White list<br>• IP greylist<br>• IP blacklist<br>• Utilisation limits<br>• IP country groups<br>• Anonymous proxy<br>• Unauthorised card country/IP country combination<br>• IP country different from Card country |
| CUID | Client Unique Identifier. May contain a maximum of 50 characters. | • Client Unique Identifier White list |
| CARDNO | Card number or account number may contain a maximum of 21 characters. This only needs to be sent when making use of ePDQ DirectLink. | • Card greylist<br>• Card blacklist<br>• BIN blacklist |

| ePDQ parameter | Description | Rules/Checks in FDMA |
|---|---|---|
| | For ePDQ e-Commerce the card number is automatically detected and registered. | • BIN greylist<br>• Card country high risk<br>• Card country medium<br>• Utilisation limits |
| ECOM_SHIPTO_POSTAL_POSTALCODE | Delivery postcode. May contain up to 10 alphanumeric characters. | • Risky zip/postcodes |
| ECOM_BILLTO_POSTAL_POSTALCODE | Invoicing Postal Code | • Risky zip/postcodes<br>• Advanced address verification check for specific card brands only |
| | AIRLINE/TRAVEL DATA | |
| AIPASNAME | Primary passenger name. The default value is the name of the credit cardholder. | • Name blacklist<br>• Name greylist<br>• Passenger name different from cardholder's name |
| AIEXTRAPASNAME1 | Name of extra passenger for PNR's with more than one passenger. This field can be repeated up to 5 times (i.e. for 5 extra passengers), changing the digit at the end of the field name. | • Name blacklist<br>• Name greylist<br>• Passenger name different from cardholder's name |
| AIORCITY1 | Departure airport (short) is a mandatory field and may contain a maximum of 5 characters. | • Departure airport not in trusted airport list<br>• Risky itinerary (airport groups)<br>• Unauthorised IP country for itinerary |
| AIORCITYL1 | Departure airport (long) is a mandatory field and may contain a maximum of 20 characters. | • Departure airport not in trusted airport list<br>• Risky itinerary (airport groups)<br>• unauthorised IP country for itinerary |
| AIDESTCITY1 | Arrival airport (short) is a mandatory field and may contain a maximum of 5 characters. | • Risky itinerary (airport groups)<br>• Unauthorised IP country for itinerary |
| AIDESTCITYL1 | Arrival airport (long) is a mandatory field and may contain a maximum of 20 characters. | • Risky itinerary (airport groups)<br>• Unauthorised IP country for itinerary |
| AISTOPOV1 | Stopover allowed for airport.<br>Possible values: the capital letters O and X.<br>O: the passenger is allowed to stop and stay.<br>X: the passenger is not allowed to stay. | • Risky itinerary (airport groups) |
| AIFLDATE1 | Flight date. | • Time to departure 1<br>• Time to departure 2<br>• Time to departure 3 |

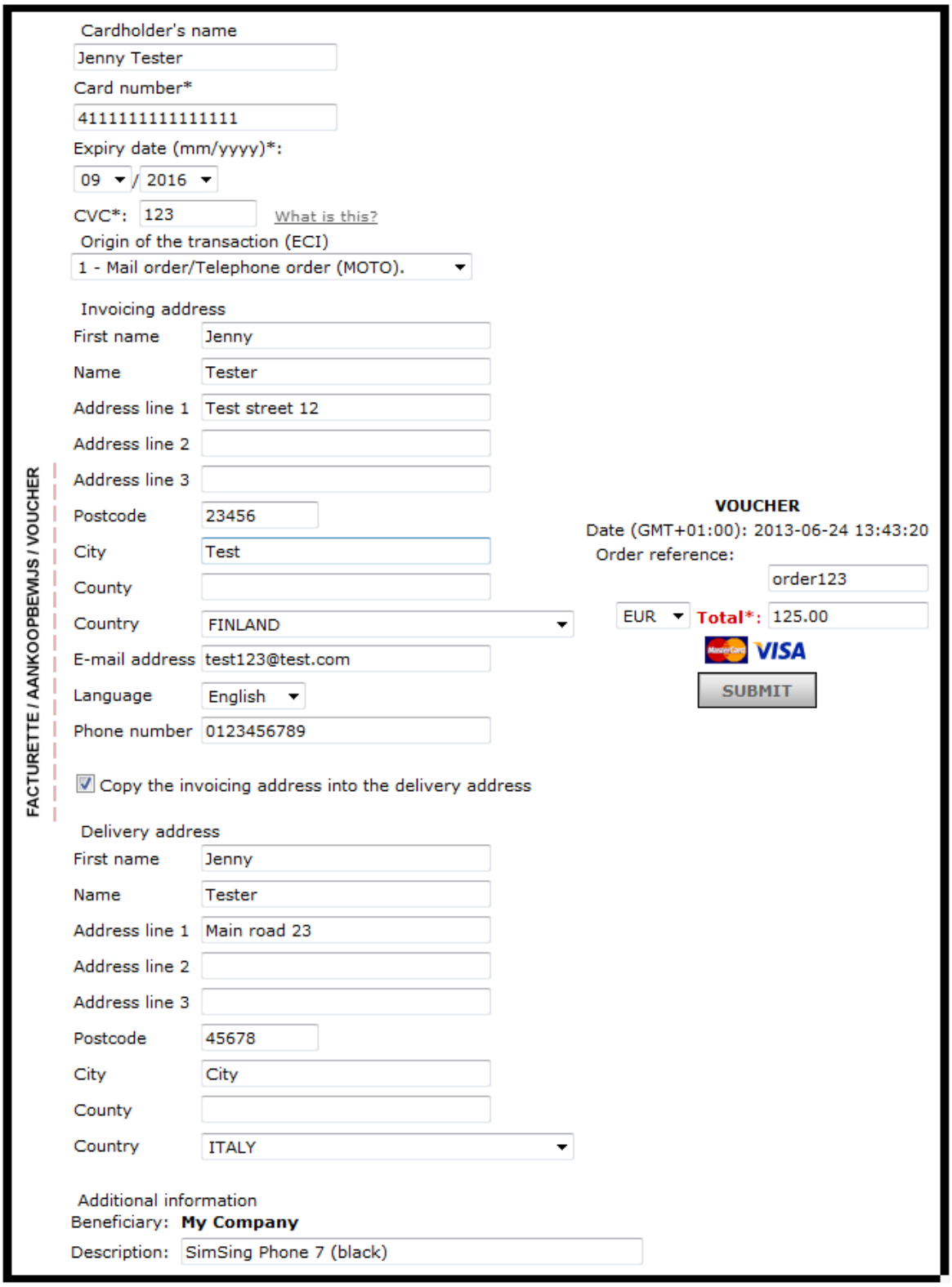
*The above list of travel parameters only contains the parameters that are linked to rules/checks in the FDMA module. For the full list of mandatory travel parameters, please check the Special Travel Format Appendix in our DirectLink or Advanced e-Commerce guide.*

# 11 Appendix: Additional data via e-Terminal

If you are using our MOTO solution e-Terminal, in addition to the default order data you can also enter contact/address details. This data will be taken into account in your fraud detection tool, thus improving your fraud prevention possibilities.

In your back office, under "Operations" select "New transaction"; you will see the voucher where the default details (name, card number, CVC, etc.) can be entered.

You will see the additional Invoicing and Delivery address details:



# 12 Appendix: CVC2 and AAV

## 12.1 CVC2

CVC2 is an authentication procedure established by credit card companies to assist in preventing fraudulent credit card use for internet transactions. Depending on the brand, this code has a different name (CVC2 or Card Validation Code for MasterCard, CVV2 or Card Verification Value for VISA, CID or Card Identification Number for American Express). However, the code is generally referred to as the “CVC”. The functionality of the CVC2 is the same for all brands.

The verification code is uniquely linked to the card number, but is not part of the card number itself. Depending on the card brand, the verification code will be a 3 or 4-digit code on the front or rear of the card, an issue number, a start date or a date of birth. For MasterCard and VISA, for example, a 3-digit code is present on the back of the card in the signature strip, after the full customer account number or the last 4 digits of the customer account number.

It is strictly forbidden for merchants and PSPs to store the customers’ CVC2 codes in a database. When the cardholder is not present in person, i.e. for "card not present" transactions, and is asked to enter the CVC2 code together with his card number, this verification code helps ascertain that the customer placing the order has the actual card at hand and that the card account is legitimate.

## 12.2 AAV/AVS

AAV is an authentication procedure available in some markets to assist in preventing fraudulent credit card use for internet transactions. Depending on the brand, this authentication procedure has a different name (AVS or Address Verification Service/System for VISA/MasterCard; AAV or Automated Address Verification for American Express). However, the functionality of the AAV is the same for all brands.

The address check takes place when the acquirer requests the card issuer to compare the numeric components (house number and postcode / ZIP) of the customer’s (invoicing or delivery) address sent by the merchant with those in the invoicing address provided by the customer to the issuer when applying for the card.

American Express performs this check automatically when it receives address details with a transaction; for other brands, it depends on whether the acquirer performs the address check or not. Under all circumstances, we recommend that the customer’s address details should be sent together with the order details you send to our system.

Although a transaction will not be declined due to the outcome of the address check, the merchant may use this outcome to decide whether to deliver the merchandise or to ask the customer for further information before dispatching.

## 12.3 Adapt rating based on AAV/AVS result

Based on the outcome of the AAV/AVS you can influence the rating of the FDMA. You can select which action you want our system to apply per possible response:

| Response | Action |
|---|---|
| Result OK | *None (only option)* |
| Result KO | Block (Review if in 'Direct Sale' mode) / Review / None |
| ZIP KO, Address OK | Block (Review if in 'Direct Sale' mode) / Review / None |
| ZIP OK, Address KO | Block (Review if in 'Direct Sale' mode) / Review / None |

| Response | Action |
| --- | --- |
| Result not received or unknown | Block (Review if in 'Direct Sale' mode) / Review / None |

**Note**

The "Result not received or unknown" response can be caused if the customer's issuer (bank) does not support the AAV/AVS check while your acquirer does. Please take this into consideration for the configuration of the FDMA.

# 13 Appendix: Fraud Reporting Tips

The fraudulent use of a credit card has to be reported by the cardholder himself to his issuing bank, i.e. the bank where he applied for his credit card.

If a merchant thinks one of his customers is committing fraud, he has to report this to his acquirer.

If a merchant wants to report a fraudster to the police, he doesn't need the credit card number. The information which is useful for the police is the IP address the customer used at the time of the transaction, with the date, time and time zone. If the merchant can include the delivery address(es) with this information, the police have a greater chance of being able to trace the fraudster. Please note, however, that the IP address might be spoofed and the delivery address might only be the address of an intermediary who has to forward the goods to a foreign country; this would make it harder for the police to trace the fraudster.

# 14 Appendix: Group configuration and blacklist sharing

Merchants with a Group account, which places several individual accounts (PSPIDs) under one master account, can benefit from cross-PSPID fraud management possibilities.

These possibilities enable the merchant to:

- Share Blacklists, Greylists and Whitelists between the various PSPIDs that belong to the merchant's group account
- Share the configuration of the FDMA (criteria, rules, limits etc.) and lists (country groups, risky postcodes etc.)

Activation

- If you use Group Manager and you are interested to have Group fraud configuration and sharing enabled, please contact our Customer Care
- In case you don't use Group Manager yet, but you have several PSPIDs you would like to join in one group account, to finally use Group fraud configuration and sharing, please contact our Sales Team for more information.