Fraud Detection Module Advanced: Scoring

Configuration Guide for the Advanced Fraud Detection Module: Scoring v.4.4.7

ingenico

ePayments

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, in the Advanced Fraud Detection Module, the merchant configures the actual behaviour of the blacklists, whitelists and greylists, along with the rules and limits in the scoring list.

The Basic Fraud Detection Module and the Advanced Fraud Detection Module are both upwards compatible, meaning that an upgrade to the advanced module doesn't actually impact the blocking behaviour you configured in the Basic Fraud Detection Module. For example:

- All blacklists entries will still be present, and the corresponding criteria in the scoring page will be configured as "blocking".

- The credit card and IP countries you configured not to accept payments from will be considered as "High-risk" countries and will be configured as "blocking" in the scoring page.

- IP address whitelist entries will still be present, and the corresponding behaviour (trust) will be set in the scoring page.

Of course, once you have upgraded to the Advanced Fraud Detection Module, you can benefit from further features and nuances in the criteria used to assess the risk of the transactions.

1.1   Benefits

The Fraud Detection Module allows you to:

- Detect anomalies during transactions
- Immediately block attempts by recognised fraudsters
- Assign a score to specific risks
- 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
- Blacklist/Greylist/Whitelist

Fraud detection activation and configuration

Payment methods	FDM	
CreditCard		
MasterCard	Yes	EDIT
VISA	Yes	EDIT

3D-Secure

About Verified By Visa, AMEX Safekey and SecureCode (3-D Secure)

Credit card		Acquirer	Card status	3-D Secure activation date	3-D Secure status	
MasterCard	Mastercard SecureCode Learn more	Barclays	Active	2017-12-07	Active	EDIT
VISA	Verified by VISA	Barclays (Mult. cur.)	Active	-	REQUEST 3-D SECURE	

Blacklist / whitelist / greylist

Card blacklist	Yes	EDIT
BIN blacklist	No	EDIT
IP blacklist	No	EDIT
IP address whitelist	No	EDIT

Important

- The VISA/MasterCard criteria described in this documentation are not necessarily available for all payment methods.
  The availability of the multi-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.

- In Batch mode (file upload), only the following functionalities of the fraud detection module are supported:
  o Card country: medium/high risk (Card country groups)
  o Card blacklist
  o Card greylist
  o BIN blacklist
  o BIN greylist

2   Fraud detection activation and configuration

In the "Fraud detection activation and configuration" table you will see the distinction between 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 can then enter the scoring page for this payment method with links to the configuration pages for the various rules, limits and lists.

The actual behaviour of these rules (i.e. whether they actually block transactions) depends on your settings in the "Scoring" page.

2.1   Card country groups

All card countries are accepted by default. Here, the term 'card country' means the country where the card was issued. Our system can identify the card country based on the card's BIN code, i.e. 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 heightened scoring; medium-risk card countries can lead to a heightened scoring; and low-risk card countries will not be taken into account for scoring.

> Note
> - Only available for VISA, MasterCard, American Express and Diners Club

2.2   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, so there is a slight risk of error, as we rely on the accuracy of this list).

As with 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 blocked transactions or adding to scoring, medium-risk IP countries can add to scoring and low-risk IP countries will not be taken into account for scoring.

Apart from these IP countries, there are also anonymous proxies. Anonymous proxies are internet access providers that allow internet users to hide their IP address. We recommend you block transactions originating from anonymous proxies in the Scoring 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 the 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 (e.g. an internet provider operating 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 risky 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.

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

Note
- Only available for VISA, MasterCard, American Express and Diners Club

2.4   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.

2.5   Utilisation limits

2.5.1   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. For example you can limit the card utilisation to once per week for products which will not be sold for more than once.

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 medium and a high threshold which allows you to set two different scores. With a medium threshold you can only raise the risk scoring; with a high threshold you can also raise the risk scoring or block directly.

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.

2.5.2   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 from this IP address in this 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 medium and a high threshold which allows you to set two different scores. With a medium threshold you can only raise the risk scoring; with a high threshold you can also raise the risk scoring or block directly.

The maximum utilisation per IP address, per period limit only applies to IPs that were used in transactions resulting in the following two statuses:

- Successful transactions: 9, 91, 92, 5, 50, 51, 52
- All transactions (including successful and rejected transactions): 9, 91, 92, 5, 50, 51, 52, 2

2.5.3   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.

You can also set a medium and a high threshold for the email utilisation which allows you to set two different scores. With a medium threshold you can only raise the risk scoring; with a high threshold you can also raise the risk scoring or block directly.

The maximum utilisation per email address, per period limit only applies to email addresses that were used in transactions resulting in any of the following statuses: 9, 91, 92, 5, 50, 51, 52, 2.

2.6   Risky data

2.6.1   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. Please note that the addresses include billing and shipping addresses.

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

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. In order for the rule to be evaluated, the country code will also need to be included.

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

Billing Address

Related input parameter	Format	Explanation	Example
OWNERCTY	AN (2)	Customer's country	UK
OWNERZIP	AN (10)	Customer's ZIP/ postcode	75420
OWNERADDRESS	AN (35)	Customer's address first line	Baker Street 221B
OWNERADDRESS2	AN (35)	Customer's address second line	2nd Floor

<u>or</u>

Related input parameter	Format	Explanation	Example
ECOM_BILLTO_POSTAL_ COUNTRYCODE	AN (2)	Invoicing country	UK
ECOM_BILLTO_POSTAL_ POSTALCODE	AN (10)	Invoicing postcode	75420
ECOM_BILLTO_POSTAL_ STREET_LINE1	AN (35)	Invoicing address first line	Baker Street 221B
ECOM_BILLTO_POSTAL_ STREET_LINE2	AN (35)	Invoicing address second line	2nd Floor

Shipping Address

Related input parameter	Format	Explanation	Example
ECOM_SHIPTO_POSTAL _COUNTRYCODE	AN (2)	Shipping country code	UK
ECOM_SHIPTO_POSTAL _POSTALCODE	AN (10)	Shipping postal code	75420
ECOM_SHIPTO_POSTAL _STREET_LINE1	AN (35)	Shipping address first line	Baker Street 221B
ECOM_SHIPTO_POSTAL _STREET_LINE2	AN (35)	Shipping address second line	2nd Floor

2.6.2   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 levels:

- High risk
- Medium risk
- Low risk

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

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.

2.6.3   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 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_SHIPMETHODTYPE	Integer value: 1-9	Delivery method You can define and submit a value for each shipping (delivery) method.	1: Pick up at merchant 2: Collection point (Post office, Kiala point...) 3: Collect at airport, train station or travel agency 4: Transporter (DHL, UPS...) 5: Carrier Merchant Owned 6: Carrier Low Cost 7: Collect at Parcel Lockers 8: Military 9: Electronic 91: Merchant Defined 1 92: Merchant Defined 2

Related input parameter	Format	Explanation	Example
			93: Merchant Defined 3
			94: Merchant Defined 4
			95: Merchant Defined 5
			96: Merchant Defined 6
			97: Merchant Defined 7
			98: Merchant Defined 8
			99: Merchant Defined 9

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

2.6.4   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, select the Shipping Method Details value from the drop-down list, 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 Ogone account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

2.6.5   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. Risky product categories only apply to e-Commerce and DirectLink.

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 can lead to a positive scoring.

To use this functionality, you should only send the ITEMFDMPRODUCTCATEGx parameter with its associated values.

Related input parameter	Format	Explanation	Example
ITEMFDMPRODUCTCATEG x	Free text (max. 50)	Product category	Travel Food Sports

Note:

Replace "x" with a number to send multiple items: ITEMFDMPRODUCTCATEG1, ITEMFDMPRODUCTCATEG2, etc.

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

2.6.6   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 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
ECOM_SHIPMETHODSPE ED	Integer value	The number of hours required for the delivery	24

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

2.6.7   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.

2.7   Duplicate settings

Next to 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

3   3-D Secure

3-D Secure offers an additional level of security, as it allows customers to be identified unambiguously through technologies, e.g. 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) 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 apply 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

The blocking and review rules can be overridden when customers are successfully identified via 3-D Secure. For more information about the overriding mechanism, please refer to Appendix: Overriding mechanism.

3.1   General

3.1.1   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 about 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.

3.1.2   Standard 3-D Secure transaction processing

1. When we receive your customer's credit card details, 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, gets 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. Ogone only acts as a technical intermediary.

3.2   Configuration options

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

3.2.1   Technical problem

The merchant can choose to *continue* or *interrupt* the transaction, should a technical problem prevent connection with 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 (option *continue*). In this case, however, the merchant will not benefit from the conditional payment guarantee (see here).

3.2.2   Identification service temporarily unavailable

Should the cardholder identification service be temporarily unavailable, the merchant can choose to *continue* or *interrupt* the transaction.

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).

3.2.3   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 (*interrupt* option). If the transaction continues, the merchant will not benefit from the conditional payment guarantee (see here).

3.2.4   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).

4   Blacklist, greylist, and whitelist configuration

In the advanced Fraud Detection Module, you can generate your own blacklist and greylist 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 three whitelists based on IP addresses, Client unique identifier, and a customer email.

The actual behavior of these lists (i.e. whether they're blocking or not) depends on your settings in the "Scoring" page.

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

4.1   General list functionalities

4.1.1   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 ticking the boxes in the "Delete" column and clicking the "Submit" button.

4.1.2   Comments

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

You can either enter it at the time of submission by entering the comment in the "Comment" field. All items you entered in that submission will then have the same comment.

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

4.1.3   Reason

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

> Important
>
> Only select "actual fraud" when you've received a chargeback with a fraud reason code

4.1.4   Filter

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

To remove a filter, click "Remove filter" button.

4.1.5   List downloads

You can download the list content in a spreadsheet (e.g. 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.

4.1.6   Blacklist hit warning

In the blacklist, you can enable a radio button in order to send a warning email when a blacklist is hit. The warning email will be sent to the email address(es) configured in the "Email address(es) for transaction

---

related emails" in the Technical information page of your account.

> **Important**
>
> You only need to enable/disable this option once. The configuration of this option applies to all blacklists.

4.2 Whitelist

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

4.2.1 IP address whitelist

You can enter IP addresses of customers you'd like to receive orders from in the trusted IP address list. If a customer's unique IP address is in this whitelist, this will override all IP-related blocking and review rules (depending on the merchant's scoring settings). For more information about the overriding mechanism, please refer to Appendix: Overriding mechanism.

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.

You may enter ranges of IP addresses, in the format "a.b.c-d.0-255", "a.b.c-d.*" or "a.b.c.d-e".

4.2.2 Unique customer identifier whitelist

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

If a customer's unique CUI is in this whitelist, this will override almost all other blocking and review rules (depending on the merchant's scoring settings). For more information about the overriding mechanism, please refer to Appendix: Overriding mechanism.

4.2.3 Email whitelist

You can whitelist a customer email by adding the email on the whitelist. In order for our system to check the customer's email address, you must also send the email address in the order details. If this is already done, the check will be done automatically.

If a customer email is in this whitelist, it will override almost all other blocking and review rules (depending on the merchant's settings). For more information about the overriding mechanism, please refer to Appendix: Overriding mechanism.

4.3 Blacklist / Greylist

Blacklist allows you to (based on your setup of rules) block transactions, force review transactions, and add risk scoring to transactions. Greylist allows you to (based on your setup of rules) force review transactions and add risk scoring to transactions.

Example: You have had issues with transactions originating from a specific IP address, but are not sure whether this IP address is a dedicated IP address, belonging to one individual. The IP address might also represent a whole company/building or may in future 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 about either moving it to your IP address blacklist or deleting it from the greylist.

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

4.3.1   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 account numbers.

4.3.2   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 on your list, simply by adding the BIN code.

4.3.3   IP address

In your IP address blacklist or greylist, you can not only enter 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.

4.3.4   Email address

The e-mail address can be a fixed address or a whole range of addresses (domain) using an asterisk ('*') before the "@" sign. The e-mail address entered by the merchant will appear in the "e-mail" column. Based on this e-mail address, our system will generate the "Partial match".

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

4.3.5   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 that 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 cardholder name, shipping name, and billing name in the order details.

4.3.6   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.

4.3.7   Generic data

The generic data blacklist and greylist allow the merchant to have a fully personalised list to which he can add the data he wishes to take into account for the fraud score of transactions. The data needs to be alphanumeric and must be no longer than 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 with the order (alphanum, max. 50 characters).

5   Scoring

You can find a list of criteria in the Scoring configuration page, which contains all criteria that can be set in the advanced 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 scoring list.

Per criterion, one of the following actions may be configured:

- *Increasing risk weighting*: A weighting from 0 to 5 can be added when the criteria increase the risk.
- *Reducing risk weighting*: A weighting from 0 to 5, 10 or 20 can be subtracted when the criteria reduce the risk.
- *Force review*: For all criteria it's possible to force a review of the transaction. Force review also induces a +3 to the score, in addition to other rules. The transaction will go Orange if the score is Green or Orange, or will remain Red if the total score is above the red threshold and if other blocking criteria were met.
- *Block transaction*: For certain criteria there is also the option to block the transaction. The rules set by the merchant will therefore either block a transaction or influence the global scoring for the transaction. The end score is the total weighting of the various criteria. The higher the score, the higher the risk.
- Override Blocking and Review

The merchant can set a certain score value as an upper limit for intermediate scoring, i.e. before the transaction is authorised. This indicates that all transactions with this score or higher should be blocked prior to the authorisation procedure. The AAV and CVC check take place after we send the transaction to the acquirer (i.e. after authorisation), so these scoring values won't be taken into account therefore for this intermediate scoring limit.

The sum of the values before authorisation and the values of the AAV and CVC scores give the final and overall score. The merchant can decide on scoring categories based on this final scoring value, linked to colours: green (low risk), orange (medium risk) and red (blocked transaction). These colours will be displayed in the feedback to the merchant.

If a transaction is blocked based on your settings, we will set its status to "Authorisation declined".

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

The following is a (non-exhaustive) selection of scoring 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. Therefore 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 address. We recommend that you do not accept payments originating from an anonymous proxies!
- *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 scoring 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 countries*: The merchant can indicate the number of countries that are allowed and can set the scoring action if the number exceeds the set limit based on the following:
    - Credit card country (only available for VISA, MasterCard, American Express and Diners Club)
    - IP country (if available)
    - Invoicing and shipping addresses if sent
    - Departure airports if applicable and sent
- *IP country is different from the CC country* (for VISA, MasterCard, American Express, and Diners Club 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 to the delivery address, based on the value of the extra "addMatch" field 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 to each other.

- *Amount limit, Utilisation limits*

- *CUI whitelist identification*

- *Email whitelist*

- *Trusted IP address*

- *Card/BIN/IP address/email/phone/cardholder name/shipping name/ billing 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 scoring criteria to "Block Transaction" in the Scoring page:

- Card in blacklist

- Anonymous proxy (under IP country)

6 Dispute

Accepting transactions in any environment carries inherent risks, such as the risk of chargebacks. Especially when processing in a Card-Not-Present (CNP) environment, the risks of chargebacks are ever present.

Ogone provides customers with a dispute page that allows merchants to add transaction data in the blacklist, greylist, and whitelist with the appropriate reason behind the dispute. This protects merchants from further fraud exposure and repeated offense. It also enhances Ogone Fraud Expert database and improves its performance.

In the transaction details (Financial page), you can access the "Dispute" button above the table with the additional information. It will take you to a page where you can add certain transaction details to your blacklist, greylist, and whitelist in one click. This option allows you to add the card number used for a transaction to your blacklist, greylist, and whitelist without having to know the full card number, for instance. You can also mark the transaction as a commercial dispute, actual fraud, or suspicion of fraud.

> IMPORTANT
>
> Only select "actual fraud" when you've received a chargeback with a fraud reason code.

Chargeback / Dispute / False Positives status and action
FLAG AS DISPUTE AND FILL BLACKLISTS, GREYLISTS OR WHITELISTS

6.1 Add transaction data in a blacklist, greylist, and whitelist

1. Click the "PAYID" under the transaction view to search for the transactions you want to report for commercial dispute, actual fraud, or suspicion of fraud.

2. Click the "DISPUTE" button to list the data received for the transaction that can be added to the blacklist, greylist, and whitelist.

3. Go to the dispute page and choose the list which you want to add the transaction data (blacklist, greylist, and whitelist). Then, select the reason for the dispute.

   You can select the transaction as:

   - Commercial dispute covers all the chargeback that the merchant received that are not fraud related.

   - Actual fraud is when you receive a chargeback for fraud.

   - Suspicion of fraud is when you suspect and want to prevent a fraudulent transaction.

   Selecting one or the other buttons impacts the fraud database differently.

4. Save and confirm to add the data to the appropriate List. The fraud check takes into effect immediately.

From the dispute page, you can also select the data (e.g., belonging to your call center, VIP client, etc.) to be added in the whitelist. If you select data that were previously in the blacklist or greylist, they will automatically be added to the white list. The fraud check takes into effect immediately.

7   Feedback

7.1   Transaction view in the back office

7.1.1   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 & IP Address. In the Scoring you can choose between three categories: Red, Orange, Green. 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.

7.1.2   Transaction details

In the transaction details (financial page), you will see additional information such as the card verification code result (if the CVC has been entered by the customer), Card country, IP address country and Received IP address. Apart from this, you will see the end scoring and the scoring category, together with the View scoring details button, should you want more scoring information.

Two buttons are situated above the table with the additional information: "Dispute" and "View transactions from same IP address"

7.1.2.1   View transactions from same IP address

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

7.1.2.2   View scoring details

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

Fraud-trail analysis

In the scoring 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, shipping name, billing name, credit card country and IP address country within a certain period you set.

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 lookup covers all transactions from the moment you start the lookup (not from the original transaction date!).

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 look-up 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.

7.1.3   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 Ogone 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 error codes:

3 / 30001100 Unauthorised customer's country

3 / 30001120 IP address on merchant's blacklist

3 / 30001130 BIN on merchant's blacklist

3 / 30001140 Card on merchant's card blacklist

3 / 30131002 You have reached the total amount allowed

3 / 30001102 Number of different countries too high

3 / 30001141 E-mail on black-list

3 / 30001142 Passenger name on blacklist

3 / 30001143 Name on blacklist

3 / 30001144 Passenger name different to 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

3 / 30001180 Maximum scoring reached

7.2   Supplementary transaction parameters

In your post-sale requests, redirections with feedback, file downloads and DirectLink XML responses, supplementary transaction parameters relating to Scoring 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
AAVCHECK	Result of the automatic address verification. This verification is currently only available for American Express. Possible values: KO The address has been sent but the acquirer has given a negative response for the address check, i.e. the address is wrong. 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 2. The acquirer sent an authorisation code but did not return a specific response for the address check. NO All other cases. For instance, no address transmitted; the acquirer has replied that an address check was not possible; the acquirer declined the authorisation but did not provide a specific result for the address check, etc.
CCCTY	Originating country of credit card. This is only available for VISA, MasterCard, American Express, and Diners Club. This 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.

Parameter	Value
	This credit card country check is based on externally provided listings, so there is a slight risk of error, as we rely on the accuracy of this list. The check gives positive results in 94% of all cases.
CVCCHECK	Result of the card verification code check. Possible values: KO The CVC has been sent but the acquirer has given a negative response to the CVC check, i.e. the CVC is wrong. 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 2. The acquirer sent an authorisation code, but did not return a specific result for the CVC check. 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.
ECI	Electronic Commerce Indicator. The possible ECI values and their meanings are set out below: 1 Manually keyed 2 Recurring payments 3 Instalment payments 5 Cardholder identification successful 6 Merchant supports identification but not cardholder, conditional payment guarantee rules apply (see here) 7 E-commerce with SSL encryption 9 Recurring after first E-Commerce transaction 12 Merchant supports identification but not cardholder, conditional payment guarantee rules apply (see here) (idem 6) 91 Cardholder identification FAILED !!!! (Conditional payment guarantee (see here) may apply. Please check with your acquirer) 92 Issuing bank authentication site temporarily unavailable, but transaction continued
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.
IPCTY	Originating country of IP address. Format: 2-character alphabetic ISO code. If this parameter is not available, "99" will be returned in the response. This IP check is based on externally provided IP listings, so there is a slight risk of error, as we rely on the accuracy of this list. The check gives positive results in 94% of all cases.
VC	Virtual card. Possible values: ECB: For E Carte Bleue ICN: For Internet City Number 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.

Advanced Fields

NBREMAILUSAGE	Number of times an e-mail address has been used during a certain period. (when the "maximum utilisation per e-mail address, per period" rule is configured.)

NBRIPUSAGE	Number of times an IP address has been used for successful transactions during a certain period.
	(when the "maximum utilisation per IP address, per period" rule is configured.)
NBRIPUSAGE_ALL TX	Number of times an IP address has been used for accepted and refused transactions during a certain period.
	(when the "maximum utilisation per IP address, per period" rule is configured.)
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.)
SCO_CATEGORY	The colour of the category the final score belongs to, based on the settings in the scoring page (Multi-criteria selection of payment methods > Scoring).
	The possible values are G (for green), O (for orange) and R (for red).
SCORING	The end score for the transaction, i.e. the total of the scores given to each item described in the scoring list

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

8   Appendix: Parameters vs. Checks/Rules

Ogone parameter	Description	Rules/Checks in FDMA
CN	The cardholder name can contain a maximum of 35 characters. This parameter can be sent via Ogone e-Commerce, DirectLink and Batch. Please note that for Ogone e-Commerce the cardholder's name will also be captured via the Ogone payment page, where the cardholder's name is a mandatory field.	• Name blacklist • Name greylist • 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. (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 • Advanced address verification check for specific card brands only
OWNERTELNO	Customer's telephone number may contain a maximum of 30 characters for all Ogone modules with the exception of Ogone 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 • 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 whitelist • Email blacklist • Email greylist • Free email • Utilisation limits
Generic_BL	Generic blacklist may contain a maximum of 50 characters.	• Generic blacklist • Generic greylist
REMOTE_ADDR	IP address of customer. This only needs to be sent when making use of Ogone DirectLink. For Ogone e-Commerce the IP-address is automatically detected and registered.	• IP White list • IP greylist • IP blacklist • Utilisation limits • IP country groups • Anonymous proxy • Unauthorised card country/IP country combination • 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 Ogone DirectLink. For Ogone e-Commerce the card number is automatically detected and registered.	• Card greylist • Card blacklist • BIN blacklist • BIN greylist • Card country high risk

		• Card country medium • 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 • 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 • Name greylist • 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 • Name greylist • 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 • Risky itinerary (airport groups) • 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 • Risky itinerary (airport groups) • 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) • 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) • Unauthorised IP country for itinerary
AISTOPOV1	Stopover allowed for airport. Possible values: the capital letters O and X. O: the passenger is allowed to stop and stay. X: the passenger is not allowed to stay.	• Risky itinerary (airport groups)
AIFLDATE1	Flight date.	• Time to departure 1 • Time to departure 2 • 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.

9   Appendix: Additional data via e-Terminal (MOTO)

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 for the FDMA and as such improve 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:

10   Appendix: CVC2 and AAV

10.1   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 customers' CVC2 codes in a database. When the cardholder is not present in person, i.e. for "card not present" transactions, and he is asked to enter his 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.

10.2   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.

Note: As expected, the simulations in AAV/AVS checks do not function in TEST environment.

10.3   Adapt scoring based on AAV/AVS result

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

Response	Action
Result OK	None / Subtract "value" from risk scoring
Result KO	None / Add "value" to risk scoring / Force review / Block (Review if in 'Direct sale' mode)
ZIP KO, Address OK	None / Add "value" to risk scoring / Force review / Block (Review if in 'Direct sale' mode)
ZIP OK, Address KO	None / Add "value" to risk scoring / Force review / Block (Review if in 'Direct sale' mode)

Response	Action
Result not received or unknown	None / Add "value" to risk scoring / Force review

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.

11   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.

12   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.

13   Appendix: Overriding mechanism

The following table contains all the overridable criteria:

Criterion	Overridable by 3-D Secure / CUI whitelist / Email whitelist	Overridable by IP address whitelist
Address is a P.O. Box	✓	
Amount - Higher than range	✓	
Amount - Lower than range	✓	
BIN on blacklist	✓	
BIN on greylist	✓	
Card country - High risk	✓	
Card country - Medium risk	✓	
Card on greylist	✓	
Card subbrand - High risk	✓	
Card subbrand - Medium risk	✓	
Cardholder name on name blacklist - Partial match	✓	
Cardholder name on name blacklist - Perfect match	✓	
Cardholder name on name greylist - Partial match	✓	
Cardholder name on name greylist - Perfect match	✓	
Data in generic blacklist	✓	
Data in generic greylist	✓	
Device Fingerprint not received	✓	
Device Fingerprint not requested - by default	✓	
Device Fingerprint not requested - transac. Level	✓	
Device Fingerprint profile category – High risk	✓	
Device Fingerprint profile category – Suspicious	✓	
E-mail on blacklist - Partial match	✓	
E-mail on blacklist - Perfect match	✓	
E-mail on greylist - Partial match	✓	
E-mail on greylist - Perfect match	✓	
Expert scoring not available	✓	
First departure airport is not in trusted airport	✓	

Criterion	Overridable by 3-D Secure / CUI whitelist / Email whitelist	Overridable by IP address whitelist
Free e-mail	✓	
Invoicing address different to delivery address	✓	
IP address on blacklist	✓	✓
IP address on greylist	✓	✓
IP country - Anonymous proxy	✓	✓
IP country - High risk	✓	✓
IP country - Medium risk	✓	✓
IP country differs from Card country	✓	✓
Max amount / card - High threshold	✓	
Max amount / card - Medium threshold	✓	
Max e-mail utilization - High threshold	✓	
Max e-mail utilization - Medium threshold	✓	
Max IP utilisation all statuses - High threshold	✓	✓
Max IP utilisation all statuses - Medium threshold	✓	✓
Max utilisation / card - High threshold	✓	
Max utilisation / card - Medium threshold	✓	
Max utilisation / IP - High threshold	✓	✓
Max utilisation / IP - Medium threshold	✓	✓
Number of different countries	✓	
One-way ticket	✓	
Passenger name different from cardholder name	✓	
Passenger name on name blacklist - Partial match	✓	
Passenger name on name blacklist - Perfect match	✓	
Passenger name on name greylist - Partial match	✓	
Passenger name on name greylist - Perfect match	✓	
Phone in blacklist - Partial match	✓	
Phone in greylist - Partial match	✓	
Postcode and address - High risk	✓	
Postcode and address - Medium risk	✓	
Product Category - High risk	✓	

Criterion	Overridable by 3-D Secure / CUI whitelist / Email whitelist	Overridable by IP address whitelist
Product Category - Medium risk	✓	
Risky itinerary (airport groups) - High risk airport	✓	
Risky itinerary (airport groups) - Medium risk airport	✓	
Shipping Method - High risk	✓	
Shipping Method - Medium risk	✓	
Shipping Method Details - High risk	✓	
Shipping Method Details - Medium risk	✓	
Time of order - High risk period	✓	
Time of order - Medium risk period	✓	
Time to Delivery - Strictly less than X hours	✓	
Time to Delivery - Strictly less than Y hours	✓	
Time to Delivery - Strictly less than Y hours	✓	
Time to departure - Strictly less than X days	✓	
Time to departure - Strictly less than Y days	✓	
Time to departure - Strictly less than Z days	✓	
Unauthorised card country/IP country combination - High risk	✓	✓
Unauthorised card country/IP country combination - Medium risk	✓	✓
Unauthorised IP country for itinerary	✓	✓

Remark:
- The "Card in blacklist" criterion cannot and will never be overridden.
- The Post-Acquirer rules (AVS/CVC) will not be overridden.
- The scoring category (Block or Review) can be overridden by the 3-D Secure / CUI whitelist criteria / email whitelist.
- Three points are added to the score even if a review rule is overridden.