Fraud Expert Checklist

Fraud Expert Checklist user guide v.1.0.3

Table of Contents

1 Introduction

The Fraud Expert module allows you to receive an additional opinion and refine your fraud detection. This Global Risk Management module allows you to detect fraud at an earlier stage, and to protect your online business from complex fraud attacks, whilst preventing the rejection of valid orders. This is achieved by means of over 100 transaction scoring parameters, and over 20,000 cross-parameter rules, specific to your industry.

Fraud Expert also enables you to save time and resources by outsourcing the manual review of dubious transactions. In addition, you will be able to freeze the most dubious transactions (credit cards and direct debits) that you prefer to review by yourself.

Fraud Expert is to be used in combination with our Advanced Fraud Detection modules; FDMA "Checklist" and "Scoring". Therefore this guide should be read in conjunction with the relevant FDMA guide.

2 Features

2.1 Automatic

Depending on the activity sector you defined in your Ingenico ePayments Account, various scoring rules and criteria are applied. Based on the transaction analysis through these global and industry specific rules, *Fraud Expert Automatic* generates three possible scorings: Low Risk, Medium Risk, or High Risk.

The transaction score of *Fraud Expert Automatic* is combined with the rating of the FDMA module, to generate a *Global Fraud score* (cf. Global Fraud Score decision process).

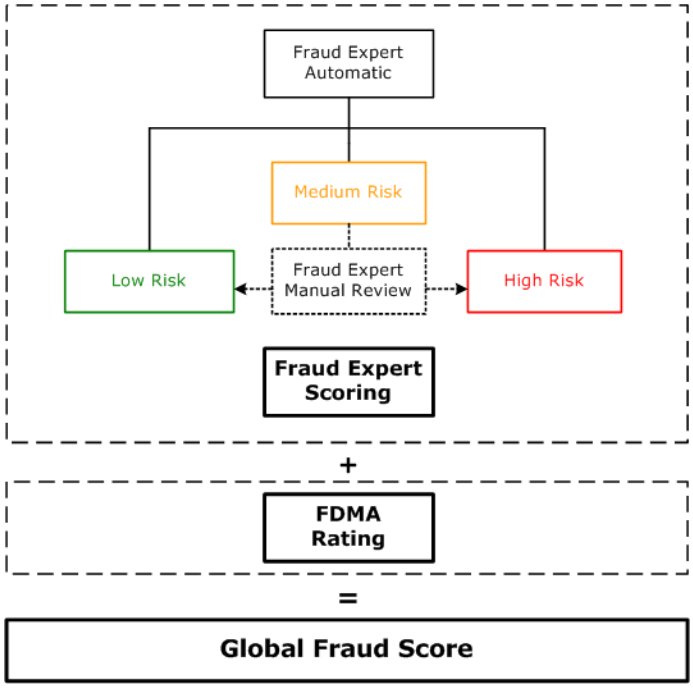
2.2 Manual review

Thanks to the *Manual Review* option, Medium Risk transactions may be manually reviewed by our fraud experts. The review is performed within hours, 24/7.

The Fraud Expert Manual Review will refine the Fraud Expert scoring.

The Fraud Expert scoring is combined with the rating of the FDMA module to generate a Global Fraud Score (cf. Global Fraud Score decision process).

Schematic presentation of how the *Global Fraud Score* is generated:



3 Integration

3.1 Parameters

In order to have your transactions reviewed in the best way, it is strongly recommended to submit as many parameters as possible.

In any case, we strongly recommend you to submit at least the following parameters:

Parameter	Format	Explanation	Example
EMAIL	AN (50)	Customer's email address	John.Doe@test.com
OWNERTELNO	AN (30)	Customer's phone number	+32123456789
OWNERCTY	AN (2)	Customer's country (ISO)	BE
REMOTE_ADDR (via DirectLink*)	AN	Customer's IP address	212.23.45.96

* not for e-Commerce integrations

If you work with travel data, it is important to send the travel data with the relevant travel parameters (cf. FDMA documentation for more information).

If you work with delivery data, it is important to send the delivery data with the relevant delivery ("ECOM_SHIPTO...") parameters.

Important

For the best reviewing, please make sure to always send the correct data with the relevant parameters. E.g. ECOM_SHIPTO_POSTAL_NAME_LAST should contain the customer's last name, the ECOM_SHIPTO_POSTAL_NAME_FIRST his first name.

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

3.2 Data Controller privacy notice request

Based on GDPR article 12, 13 & 14, a Data Controller has the obligation to inform its end-customers about the future processing of their personal data. Such information should be made specific based on the type of personal data to be filled-in for a specific transaction (e.g.: selected payment method, controller/processor, acquirer, fraud). The result should be available and visible at the moment of the data collection and the cardholder should be offered with a printable and downloadable version of it.

Per the GDPR policy, you need to display the information to your customer before they validate their transaction. This information should ideally be displayed on the same page as where your customer fills in their card/account credentials.

The below privacy policy request allows you to retrieve all the information you need to display to your customer about our services in order to be compliant with the GDPR regulation.

3.2.1 Query request

3.2.1.1 Request URL

- The request URL in the TEST environment is https://secure.ogone.com/ncol/test/privacy-policy.asp
- The request URL in the PRODUCTION environment is https://secure.ogone.com/ncol/prod/privacy-policy.asp

3.2.1.2 Request parameter

The following table contains the mandatory request parameters to be sent to your customer regarding the usage of their privacy information:

Field	Format	Description
USERID	String	Your API-user
PSWD	String	Your API-user password
PSPID	String	Your account PSPID
BRAND	String (e.g. Visa)	Optional: Payment method brand You can send this field multiple times to get the result of several brands at once. • Sending no brand is the same as sending all your active brands. • Empty/wrong formatted brands are ignored.
LANGUAGE	ISO 639-1: Two-letter codes (e.g. FR)	Optional: The language in which you want to retrieve the text. If not provided, the text will be returned into the merchant configured language.

3.2.1.3 Test page

You can test direct query requests here: https://secure.ogone.com/ncol/test/privacy-policy.asp

3.2.2 Query response

The following is a list of XML elements and the returned XML responses examples for different outcomes.

Name	Format	Description
Response	Complex	Root node, always present
Response.Status	String, possible values : Success, SuccessWithWarnings, Error	Always present
Response.Body	Complex	Present only when Response.Status = Success or SuccessWithWarnings
Response.Body.Html	String / html	Empty if Response.Status = SuccessWithWarnings & Response.Warnings.Warning.Code = NoContent
Response.Errors	Complex	Present only when Response.Status = Error
Response.Errors.Error	Complex	Can occur multiple times inside an <Errors> node
Response.Warnings	Complex	Present only when Response.Status = SuccessWithWarnings or Error
Response.Warnings.Warning	Complex	Occurs multiple times inside a <Warnings> node
Response.Errors.Error.Code Response.Warnings.Warning.Code	String, possible values : Inside an <Error> node : Unauthorized, InternalServerError Inside a <Warning> node : NoContent	Always present in an <Error> or <Warning> node
Response.Errors.Error.Message Response.Warnings.Warning.Message	String	Optional

If you face Response.Status=Error, please refer to the Response.Errors.Error to fix it.

The following are two successful examples:
1. Example of an XML response for success with warnings. This example displays if no privacy information needs to be disclosed to the customer.

```
<?xml version="1.0" encoding="utf-8"?>
<Response>
<Status>SuccessWithWarnings</Status>
<Warnings>
<Warning>
<Code>NoContent</Code>
</Warning>
</Warnings>
<Body>
<Html/>
</Body>
</Response>
```

2. Example of an XML response for success with content. The example shows a 2 section display.

```
<?xml version="1.0" encoding="utf-8"?>
<Response>
<Status>Success</Status>
<Body>
<Html><![CDATA[<ul><li><h2>Title 1</h2><p>Content 1</p></li><li><h2>Title 2 (VISA,
</Body>
</Response>
```

3.3 Device fingerprinting

Device fingerprinting is a technology that enables us to uniquely identify a device, so that if a fraudster uses the same device twice, for different transactions, it can be detected by our system. The parameter DEVICEID is used to identify the device that the fraudster uses.

The technology is integrated in the Ingenico ePayments payment page by means of a Java Script. If you're using DirectLink and/or Alias Gateway you need to integrate the Java Script yourself. (See Appendix: Device fingerprinting via DirectLink)

Note: The Device Fingerprinting functionality applies only when a Fraud Expert scoring category (Green, Orange or Red) is successfully returned by Fraud Expert

4 Configuration

The aforementioned Fraud Expert features can be activated and configured per payment method. This can be done by selecting "Fraud detection" under "Advanced" in the back-office menu:

Clicking the "Edit" button for "Your activity sector" will allow you to change your activity sector, and to enable *Fraud Expert Automatic* and *Fraud Expert Manual Review* per payment method:

Payment methods	FDMAc	Fraud Expert Automatic	Fraud Expert Manual Review
CreditCard			
MasterCard	☑	☑	☑
VISA	☑	☑	☑

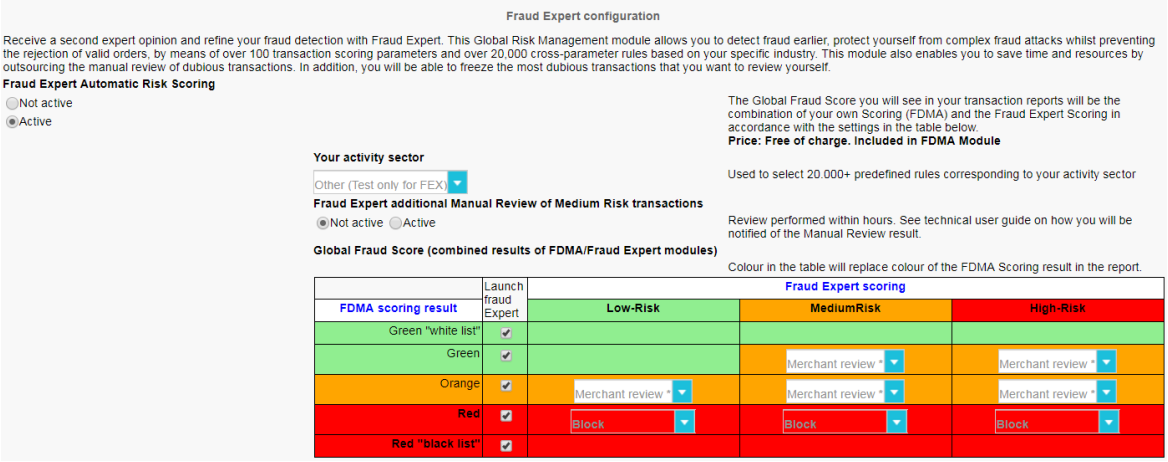
Clicking the "Edit" button for a payment method will allow you to configure FDMA and Fraud Expert for that specific payment method. This is thoroughly explained in the next chapter.

Payment methods	FDMAc	Fraud Expert Automatic	Fraud Expert Manual Review	
CreditCard				
MasterCard	Yes	Yes	No	Edit
VISA	Yes	Yes	Yes	Edit

Configure FDMA and Fraud Expert settings per payment method

5 Global Fraud Score decision process

The Global Fraud Score you will see in your transaction reports will be the combination of your own rating (FDMAc) and the Fraud Expert scoring in accordance with the settings in the matrix that you can configure in your back office via Fraud detection > Fraud detection activation and configuration > Payment method > “Edit”:



If all FDMA rule actions are set to "none", fraud expert’s result will determine the outcome of the transaction:

- If fraud expert output is ‘low risk’ the transaction will be sent further to authorization.
- If fraud expert output is ‘medium risk’ the transaction will be sent further to authorization.
- If fraud expert output is ‘high risk’ the transaction will be blocked and status 2 - authorization declined will be displayed.

5.1 How it works

You can configure the Global Fraud Score matrix for each payment method. It allows you to define the outcome of each transaction, based on the combined result of the FDMA rating and the Fraud Expert scoring.

The combination of the FDMA rating and the Fraud expert scoring will result in a predefined action:

A. OK: Pass (green)

B. Merchant Review: Transaction freeze in status 50 and to be manually approved by the merchant (orange) *

   OR

C. Expert Manual Review: Transaction freeze in status 50 and expert review to be awaited (orange / only if Manual Review is active) *

D. BLOCK: Refuse (red)

(*actions B and C only apply when the transaction freeze option is enabled. If not, the the transactions will pass. In all cases, the transactions are identified labeled Orange.)

5.2 Examples

Hereunder you find concrete configuration examples of the FDMA rating/Expert scoring matrix.

Default configuration

In the default configuration, Global Fraud Score colour is equivalent to your FDMA colour, except when Fraud Expert has flagged a risk as Medium or High, and your FDMA rating didn't give any risk. In this case, transactions will be put in orange "to review", to ensure suspicious behaviour is flagged and you can identify it.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	☑			
Green	☑		Merchant review *	Merchant review *
Orange	☑	Merchant review *	Merchant review *	Merchant review *
Red	☑	Block	Block	Block
Red "black list"	☑			

☛ *You can set this configuration if you already have an extended set of rules configured in the FDMA and you want to ensure minimising fraud thanks to Fraud Expert's second layer of protection.*

Expert as second opinion with no impact on the transaction status

In this configuration, the Global Fraud Score colour is always equivalent to your FDMA colour. This induces that whatever the Fraud Expert risk feedback is, it will not influence your transaction status.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	☑			
Green	☑		OK	OK
Orange	☑	Merchant review *	Merchant review *	Merchant review *
Red	☑	Block	Block	Block
Red "black list"	☑			

☛ *You can set this configuration if you want to use Fraud Expert as feedback to review suspicious transactions and adjust your own rules.*

Fully outsource complexity & risk scoring to Expert

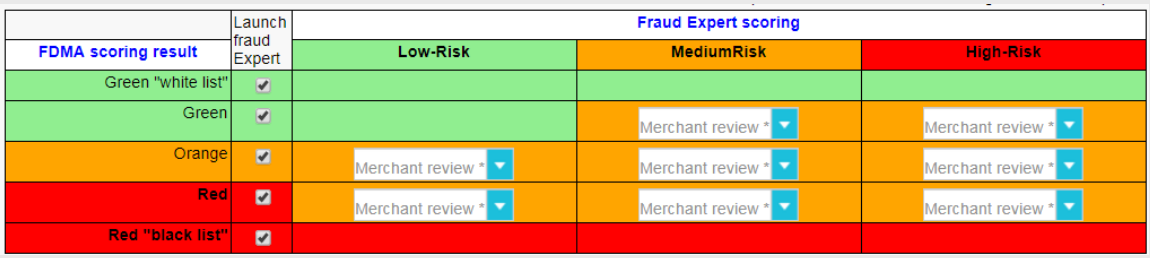
In this configuration, the Global Fraud Score colour is equivalent to the Fraud Expert colour. This induces that rejection and acceptance of criteria will be determined by Fraud Expert scoring.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	☑			
Green	☑		Merchant review *	Block
Orange	☑	OK	Merchant review *	Block
Red	☑	OK	Merchant review *	Block
Red "black list"	☑			

☛ *You can set this configuration if you don't have internal expertise or resources to do the operational follow-up of your transactions.*

Optimise acceptance rate with high review rate

In this configuration, whenever the FDMA and Fraud Expert colours are not similar, the transactions are considered as suspicious (Orange) and can then be reviewed by our team of Experts and your own experts.

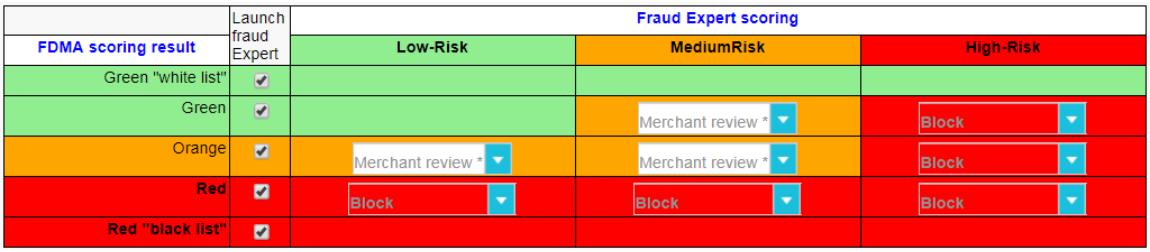


FDMA scoring result	Launch fraud Expert	Fraud Expert scoring: Low-Risk	MediumRisk	High-Risk
Green "white list"	☑			
Green	☑		Merchant review *	Merchant review *
Orange	☑	Merchant review *	Merchant review *	Merchant review *
Red	☑	Merchant review *	Merchant review *	Merchant review *
Red "black list"	☑			

☛ *You can set this configuration if you have enough internal resources to review transactions.*

The "safe way" configuration

This configuration is very similar to the default configuration. The only difference is when Fraud Expert returns “High Risk”. In that case, transactions’ Global Fraud Score is Red, which induces transactions are blocked.



FDMA scoring result	Launch fraud Expert	Fraud Expert scoring: Low-Risk	MediumRisk	High-Risk
Green "white list"	☑			
Green	☑		Merchant review *	Block
Orange	☑	Merchant review *	Merchant review *	Block
Red	☑	Block	Block	Block
Red "black list"	☑			

☛ *You can set this configuration if you want to minimise the fraud rate and if your own FDMA rules are not too strict.*

5.3 Transaction freeze

For all orange transactions, the Transaction freeze feature allows you to put the relevant transactions (authorised by the acquirer) on hold during a certain number of days, until you have reviewed them. Once this freeze period is over, if no action has been taken, the data capture and payment will automatically be processed, as usual.

If you do not activate the Transaction freeze feature, transactions will be processed automatically, as usual.

Be aware that acquirers have distinct authorisation period limits. We therefore recommend you to check per payment method what your acquirer’s limit is, and configure the Transaction freeze module accordingly.

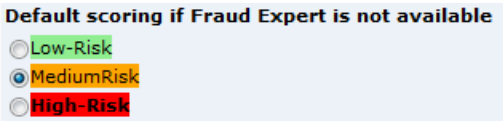
Note

Your acquirer can provide you more information about the expiration of an authorisation.

5.4 Default scoring if Fraud Expert is not available

It may happen that Fraud Expert is temporarily unavailable or doesn't provide an answer in a timely manner.

In the rare occasions this happens you can define a default scoring in the Fraud Expert configuration screen of the payment method.



If you haven't changed the configuration, the defaut value is "Medium Risk".

6 Transaction monitoring and review

6.1 General

In your Ingenico ePayments back office, via View transactions, on the transaction overview page, you can find three columns for fraud detection:

- FDMAc rating: Dark Green (DG), Green (G), Orange (O), Red (R), Dark Red (DR)
- Fraud Expert scoring: Low Risk, Medium Risk, High Risk (scoring is expressed in a percentage depending on the risk level. The higher the percentage, the higher the risk of fraud)
- Global Fraud Score: the result based on the combination of FDMAc rating and Fraud Expert scoring as configured in the Global Fraud Score matrix: G/O/R

Example:

Pay ID	Merch ref	Orders	Status	Authorisation	Total	Global Fraud Score	FDMAc rating	Fraud Expert scoring
100747608	20129271805	2012-09-27 18:00:10	2-Authorisation declined		23.45 EUR	(G)	(G)	n/a
100747609	201292718027	2012-09-27 18:00:40	50-Authorized waiting external result	test123	23.45 EUR		(G)	(41 %)
100747610		2012-09-27 18:02:13	5-Authorised	test123	11.00 EUR	(G)	(G)	(0 %)
100747656		2012-09-28 10:40:03	50-Authorized waiting external result	test123	651.00 EUR		(G)	(61 %)
100745270	2012911123336	2012-09-11 12:33:37	5-Authorised	test123	23.45 EUR	(G)	(O)	(41 %)
100745272	2012911123432	2012-09-11 12:34:32	5-Authorised	test123	77.77 EUR	(G)	(O)	(61 %)
100745273	2012911123528	2012-09-11 12:35:29	5-Authorised	test123	12.34 EUR	(G)	(WL)	(0 %)

Tip

In the "Advanced selection criteria" of the "View transactions" menu, you can filter results with the Global Fraud Score (Green/Orange/Red), and the Fraud Expert Manual Review (All/Green/Pending/Red).

6.1.1 Global fraud score

The result of the Global Fraud Score will be Green (pass), Red (blocked), or Orange.

When the Transaction freeze option is activated and the the result is Orange, either a hand or a sandglass icon will be displayed:

Hand: Waiting merchant review

Sandglass: Waiting expert manual review

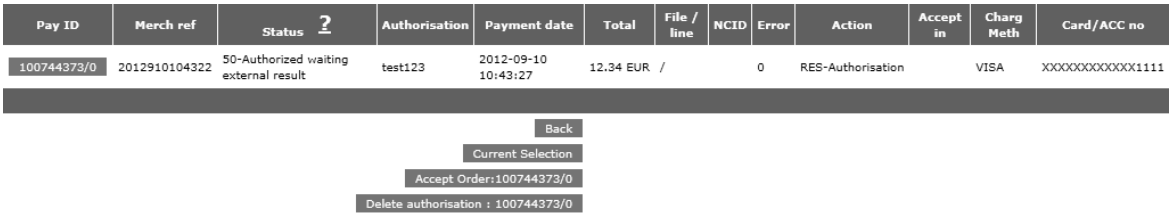
Pay ID	Merch ref	Orders	Status	Authorisation	Payments	Total	Global Fraud Score	FDMAc rating	Fraud Expert scoring	Name	Method
100744373	2012910104322	2012-09-10 10:43:21	50-Authorized waiting external result	test123		12.34 EUR		(O)	(0 %)	Jane Doe	VISA
100744375	2012910104419	2012-09-10 10:44:18	50-Authorized waiting external result	test123		23.45 EUR		(O)	(41 %)	S. Peeters	VISA

In both cases the status of the transaction is “50-Authorised waiting external result” (if the *Transaction freeze* option is enabled).

In the case of *Merchant review*, you only have to either delete the authorisation or confirm the order.

With the *Fraud Expert Review* option activated, you have to wait until the fraud expert has given his scoring: low or high risk. Based on the matrix configuration, a new global fraud score will be calculated.

You can bypass the Expert review by doing the review yourself, following the same process as Merchant review.



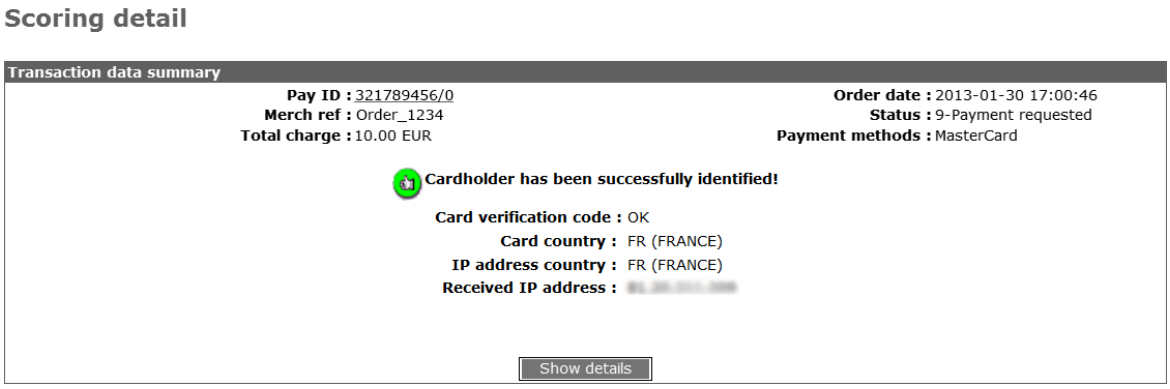
If the Transaction freeze option is activated, you can change the transaction status on the Scoring details page (cf. Advanced reviewing: Scoring detail).

6.2 Advanced reviewing: Scoring detail

To obtain a detailed overview of the transaction scoring (*Scoring detail*), you can select “View scoring details” in the "Financial" overview of a transaction, or directly in the transaction results after you made a search via *View transactions*.

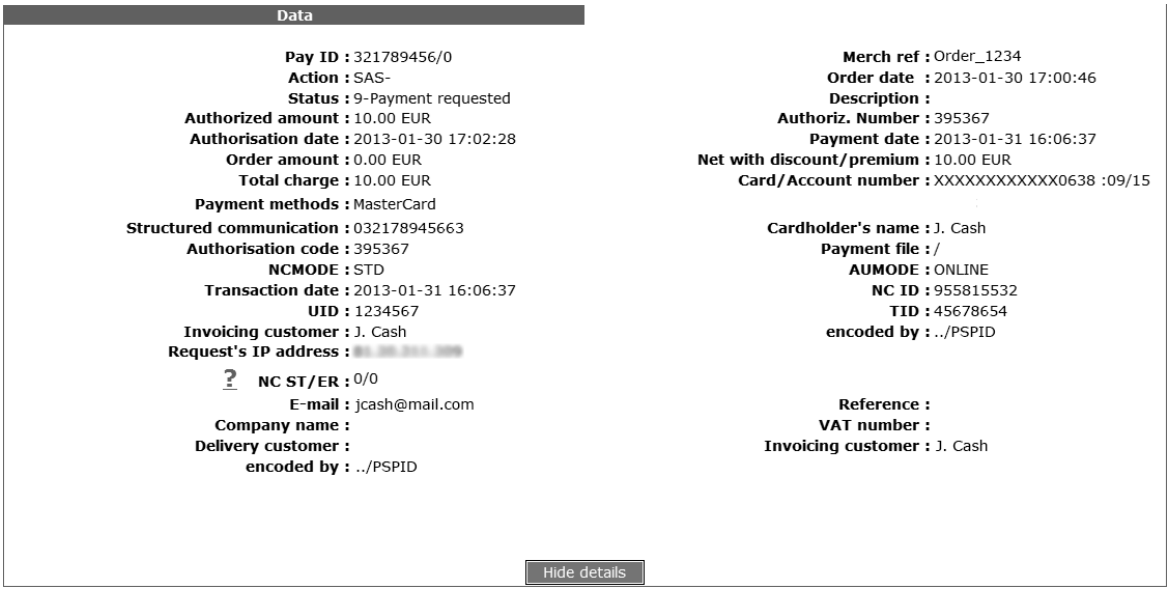
6.2.1 Transaction data summary

The first overview you will see is the Transaction data summary, which shows general transaction data relevant to the scoring.



6.2.2 Details/data

In the *Transaction data summary* you can select “Show details” to get more specific data about a transaction:



6.2.3 Transaction scoring summary

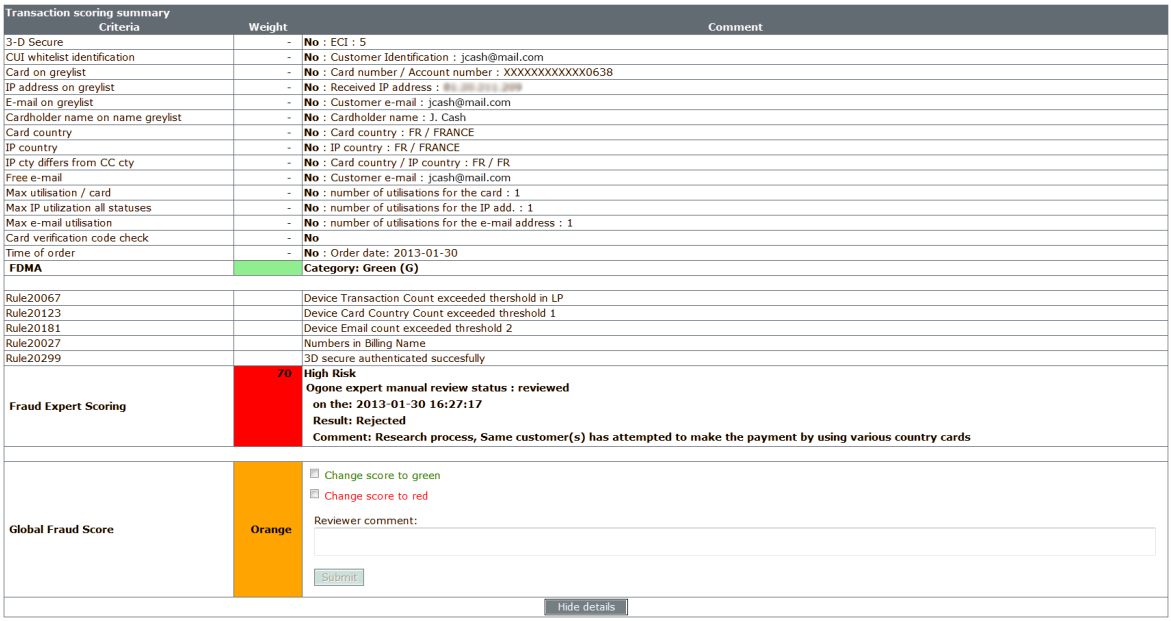
The *Transaction scoring summary* shows exactly which criteria were met to obtain the final transaction score:

You can change the the colour of the Global Fraud Score if the colour is Orange. If the Transaction freeze option is activated, that will automatically change the transaction status.

If the score becomes Green, then the transaction is authorised and then captured.

If the score becomes Red, then the transaction gets the "Authorised and cancelled" status.

Clicking the "Show details" button will again give more scoring information:



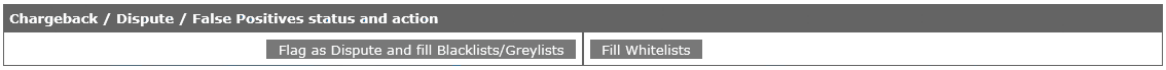
Transaction scoring summary Criteria	Weight	Comment
3-D Secure	-	**No** : ECI : 5
CUI whitelist identification	-	**No** : Customer Identification : jcash@mail.com
Card on greylist	-	**No** : Card number / Account number : XXXXXXXXXXXX0638
IP address on greylist	-	**No** : Received IP address : [redacted]
E-mail on greylist	-	**No** : Customer e-mail : jcash@mail.com
Cardholder name on name greylist	-	**No** : Cardholder name : J. Cash
Card country	-	**No** : Card country : FR / FRANCE
IP country	-	**No** : IP country : FR / FRANCE
IP cty differs from CC cty	-	**No** : Card country / IP country : FR / FR
Free e-mail	-	**No** : Customer e-mail : jcash@mail.com
Max utilisation / card	-	**No** : number of utilisations for the card : 1
Max IP utilization all statuses	-	**No** : number of utilisations for the IP add. : 1
Max e-mail utilisation	-	**No** : number of utilisations for the e-mail address : 1
Card verification code check	-	**No**
Time of order	-	**No** : Order date: 2013-01-30
FDMA		**Category: Green (G)**
Rule20067		Device Transaction Count exceeded thershold in LP
Rule20123		Device Card Country Count exceeded threshold 1
Rule20181		Device Email count exceeded threshold 2
Rule20027		Numbers in Billing Name
Rule20299		3D secure authenticated succesfully
Fraud Expert Scoring	**70**	**High Risk** **Ogone expert manual review status : reviewed** **on the: 2013-01-30 16:27:17** **Result: Rejected** **Comment: Research process, Same customer(s) has attempted to make the payment by using various country cards**
Global Fraud Score	**Orange**	Change score to green Change score to red Reviewer comment: Submit
		Hide details

6.2.4 Chargeback / Dispute / False Positives status and action

In the *Chargeback / Dispute / False Positives status and action* section you can choose to:

- Flag transactions as dispute, and select data to put in the blacklists/greylists
- Fill whitelists, with data such as IP addresses

> Tip
>
> If your acquirer informs you of a fraud case, don't forget to mark the related transaction(s) as "Actual fraud". This allows you to get better prevention with Fraud Expert.



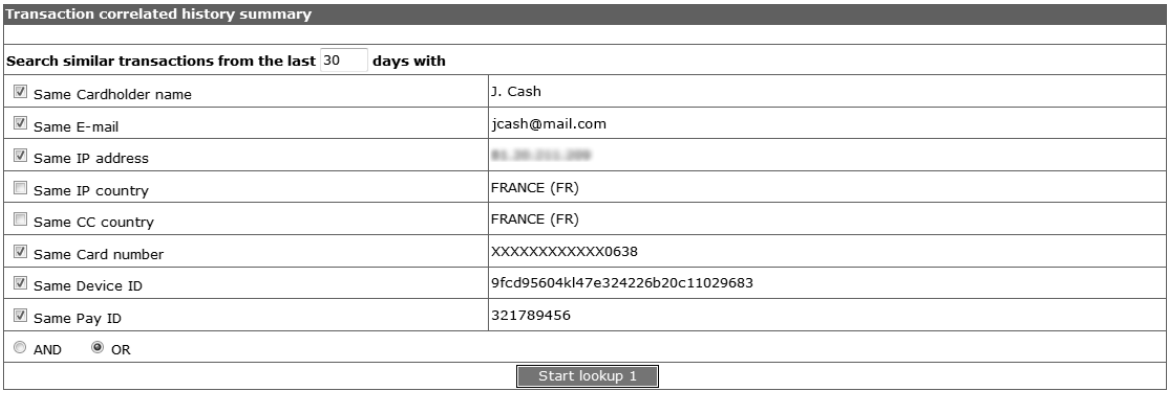
Dispute:

Fill whitelists:

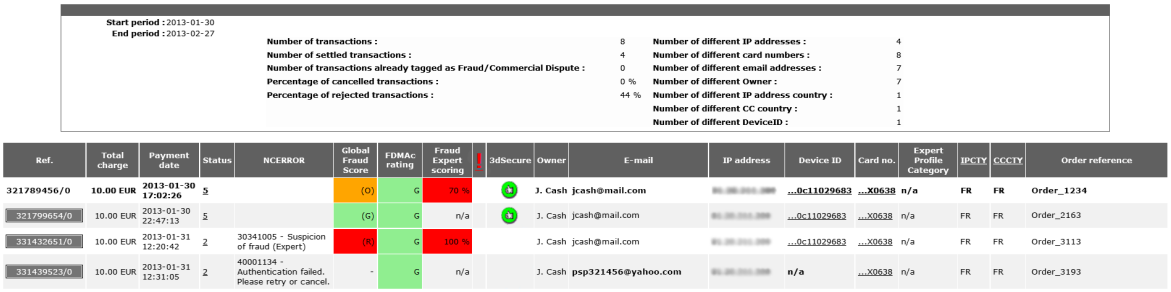
6.2.5 Transaction correlated history summary

The Transaction correlated history summary enables you to look up and browse through transactions that are similar to the one you are checking.

You can select different criteria to refine the resulting transactions:



Transaction overview after lookup 1:



Clicking the "Ref." (PAYID) button will give the scoring details of that specific transaction.

Within the page that shows the results of "lookup 1", you can "Start lookup 2" to check the newly found correlated transactions' data. The same goes for 'lookup 3' etc.

7 Appendix: Device fingerprinting via DirectLink

The below information is for merchants that want to make use of the Device fingerprinting in their DirectLink integration.

A tracking code in HTML, consisting of CSS, JavaScript and flash, must be sent. The code must be inserted into the header of a webpage which will be loaded when the customer's machine visits the site. The page should ideally only be loaded once during a user session, and be a page where the user remains for 5 seconds or more; most probably this will be the page where the user enters his payment details.

This HTML code is associated with a unique temporary and random session identifier (sid), which is generated by you in the way as described in the table below.

Parameter	Explanation	Example
sid	The Unique Identifier of a user session. The concatenation of the values of respectively the PSPID and ORDERID are calculated in the MD5 format, resulting a 32-digit hexadecimal hash string.	*ec4dfe7e880e374071e2728c3711c3a8*
aid	The ID of Tracker Application Account. This is always the same (fixed) value: 10376	

Below is an example of what the code snippet will look like. You will need to update the "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" in the sample below with a unique user session identifier in MD5 format.

```
<script type="text/javascript" async="true" src="https://elistva.com/api/script.js?
aid=10376&sid=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"></script>
<noscript><p style="background:url(//elistva.com/api/assets/clear.png?
aid=10376&sid=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX)"></p></noscript>
<object type="application/x-shockwave-flash" data="//elistva.com/api/udid.swf?
aid=10376&sid=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" width="1" height="1">
    <param name="movie" value="//elistva.com/api/udid.swf?
aid=10376&sid=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" />
</object>
```

8 Appendix: Activity Sectors

In the list below you find the full list of sectors/industries that you can select in the configuration for Fraud Expert Automatic review. Based on the sector name you select, various pre-defined scoring rules and criteria are applied.

Sector description	Example
Travel & Tourism The business or industry of providing information, accommodations, transportation and other services to tourists.	A very wide industry. It includes Government tourism departments, immigration and customs services, travel agencies, tour operators including airlines & hotel bookings, etc.
Ticketing Any or all of the processes involved in collecting fares and issuing tickets for any form of transportation and/or event.	This involves public transport like bus and train industries, movies, events, trade shows, etc.
Shopping The process whereby consumers directly buy goods or services from a seller in real-time.	All e-commerce websites and portals selling electronic products like PC, laptops, mobile phones, garments, etc.
Gifting A voluntary transfer of property or of a property interest from one individual to another, made gratuitously to the recipient.	Quite common to shopping websites, but involves some specific products like chocolates, cakes, flowers, etc.
Web Services Online services delivered from a website.	Hosting services, application development, shopping cart, domain registration, web design and development.
High Risk High-risk segments is a kind of category that is more inclined to encounter fraud.	N.G.O, charities, donations, etc.
Recharge Business that is involved in any recharge of business activities.	Postpaid/Prepaid mobile recharge, DTH recharge, etc.
Regular Service Any organisation providing services to the general public, although it may be privately owned.	This includes electricity, gas, telephone, water, television cable systems, health care, consultancy services, etc.
Call Centre Is a centralised office used for the purpose of receiving or transmitting a large volume of requests by telephone.	Tele-shopping/Marketing bookings.
Air tickets Business that involves flight ticket booking.	Direct airlines, associates and booking agents.
Hotels & Resorts Popular method of booking rooms.	Hotels & Resorts accommodations, GDS services and agents.

Sector description	Example
High-Risk Shopping This category of products are easily resalable.	Luxury/precious items like gold & silver jewellery.
IT Services Online services that are delivered over the internet.	Computer support & services, anti-virus updates and downloadable software.