

# Fraud Expert Checklist

Fraud Expert Checklist guide de l'utilisateur v.1.0.3

## Table des matières

1	Introduction .....	3
2	Fonctionnalités.....	4
2.1	Mode automatique.....	4
2.2	Examen manuel.....	4
3	Intégration .....	5
3.1	Paramètres .....	5
3.2	Empreinte numérique des matériels.....	5
4	Configuration.....	6
5	Processus de décision relatif à la notation globale des fraudes.....	7
5.1	Comment ça marche.....	7
5.2	Exemples .....	8
5.3	Gel des transactions .....	9
5.4	Default scoring if Fraud Expert is not available.....	9
6	Contrôle et examen des transactions.....	10
6.1	Généralités .....	10
6.1.1	Notation globale des fraudes .....	10
6.2	Examen avancé : Détails de la notation.....	11
6.2.1	Résumé des données des transactions .....	11
6.2.2	Détails et données .....	11
6.2.3	Résumé de la notation des transactions .....	12
6.2.4	États Contestations / Litige / Faux positif et actions .....	13
6.2.5	Résumé de l'historique corrélé des transactions .....	14
7	Annexe : Empreinte numérique des matériels via DirectLink.....	16
8	Annexe : Secteurs d'activité.....	17

# 1 Introduction

Le module Fraud Expert permet de recevoir un avis supplémentaire et d'affiner la grille de détection des fraudes. Ce module de gestion du risque global vous permet de détecter les fraudes plus rapidement, de mieux vous protéger des attaques frauduleuses complexes tout en empêchant que soient rejetées les commandes valides grâce à plus de 100 paramètres de notation de transaction et à plus de 10 000 règles d'application conjointe des paramètres basées sur votre secteur d'activité spécifique.

Fraud Expert vous permet également d'économiser du temps et des ressources en externalisant l'examen manuel des transactions douteuses. En outre, vous êtes en mesure de geler les transactions les plus douteuses (par carte de crédit et par prélèvement automatique) pour les examiner vous-même.

Fraud Expert est destiné à être utilisé en combinaison avec nos modules de détection des fraudes avancés, la « liste de contrôle » et la « notation » FDMA. Il convient donc de lire ce guide en parallèle avec le guide FDMA ad hoc.

## 2 Fonctionnalités

### 2.1 Mode automatique

En fonction du [secteurs d'activité](#) que vous avez défini dans votre compte Ingenico ePayments s'appliquent différentes règles et différents critères de notation. L'analyse des transactions reposant sur ces règles générales et spécifiques du secteur conduit le *mode automatique de Fraud Expert* à générer trois notes possibles : Risque faible, Risque moyen ou Risque élevé.

La note affectée à la transaction par le *mode automatique de Fraud Expert* est combinée à la notation du module FDMA afin de générer une *Global Fraud Score* (voir [Processus de décision relatif à la notation globale des fraudes](#)).

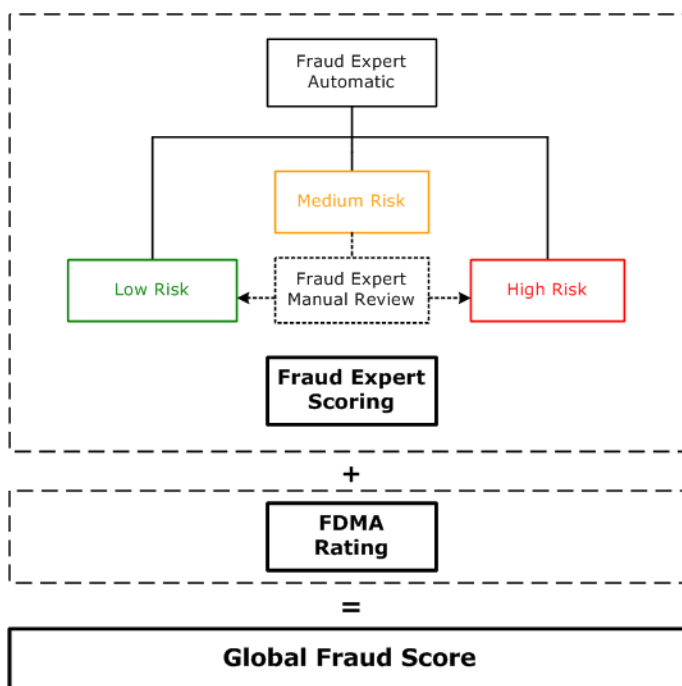
### 2.2 Examen manuel

Avec l'option *Manual Review (Examen manuel)*, les transactions à risque moyen peuvent être examinées manuellement par nos experts en fraude. Cet examen est effectué en quelques heures (24h/24 et 7j/7).

L'examen manuel réalisé à l'aide de Fraud Expert affine la notation de Fraud Expert.

La notation de Fraud Expert est combinée à celle du module FDMA pour générer une notation globale des fraudes (voir [Processus de décision relatif à la notation globale des fraudes](#)).

Présentation schématique du processus de *génération de la notation globale* des fraudes :



### 3 Intégration

#### 3.1 Paramètres

Pour que vos transactions soient examinées au mieux, il est fortement recommandé de soumettre autant de paramètres que possible.

Dans tous les cas, nous vous conseillons vivement de soumettre au minimum les paramètres suivants :

Paramètre	Format	Explication	Exemple
EMAIL	AN (50)	Adresse électronique du client	jean.dupont@test.com
OWNERTELNO	AN (30)	Numéro de téléphone du client	+32123456789
OWNERCTY	AN (2)	Pays du client (code ISO)	BE
REMOTE_ADDR (via DirectLink*)	AN	Adresse IP du client	212.23.45.96

\*pas nécessaire pour les intégrations e-Commerce

Si vous traitez des données de voyage, il est important que vous envoyiez ces informations de voyage avec les paramètres de voyage correspondants (Veuillez consulter le guide FDMA pour les détails).

Si vous traitez des données de livraison, il est important que vous envoyiez ces informations de livraison avec les paramètres de livraison correspondants (« ECOM\_SHIPTO », etc.).

**IMPORTANT**  
 Pour que l'examen soit le meilleur possible, veillez à toujours envoyer les données appropriées avec les paramètres correspondants. Ainsi, « ECOM\_SHIPTO\_POSTAL\_NAME\_LAST » doit contenir le nom de famille du client, et « ECOM\_SHIPTO\_POSTAL\_NAME\_FIRST » son prénom, par exemple.

*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 Empreinte numérique des matériels

*Device fingerprinting (Empreinte numérique des matériels)* est une technologie qui nous permet d'identifier de manière unique un appareil de telle sorte que, si un fraudeur utilise une seconde fois un même appareil, notre système puisse le détecter. C'est le paramètre DEVICEID qui sert à identifier l'appareil que le fraudeur utilise.

Cette technologie est intégrée dans la page de paiement Ingenico ePayments au moyen d'un script Java. Si vous utilisez DirectLink ou Alias Gateway, vous devez intégrer le script Java vous-même. (Voir [Appendix: Device fingerprinting via DirectLink](#))

Remarque : La fonctionnalité Empreinte numérique de l'appareil s'applique uniquement en présence de Fraud Expert et, par conséquent, d'une catégorie Expert.

## 4 Configuration

Les fonctionnalités Fraud Expert mentionnées ci-dessus peuvent être activées et configurées par moyen de paiement. Cette configuration peut être effectuée en sélectionnant « Fraud detection (Détection des fraudes) », sous « Advanced (Avancé) » dans le menu Back Office :

### Fraud detection

#### Fraud detection activation and configuration

Your activity sector: Ticketing  — Configure "Your activity sector" and activate Fraud Expert Automatic and Manual

Un clic sur le bouton « Edit (Modifier) » de la zone « Your activity sector (Votre secteur d'activité) » permet de changer de secteur d'activité et d'activer les fonctionnalités *Fraud Expert Automatic (mode automatique)* et *Fraud Expert Manual Review (examen manuel)* par moyen de paiement :

Payment methods	FDMAc	Fraud Expert Automatic	Fraud Expert Manual Review
<b>CreditCard</b>			
MasterCard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VISA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Un clic sur le bouton « Edit (Modifier) » d'un moyen de paiement permet de configurer les fonctionnalités FDMA et Fraud Expert pour le moyen de paiement en question. Cette configuration est expliquée en détail au [chapitre suivant](#).

Payment methods	FDMAc	Fraud Expert Automatic	Fraud Expert Manual Review	
<b>CreditCard</b>				
MasterCard	Yes	Yes	No	<input type="button" value="Edit"/>
VISA	Yes	Yes	Yes	<input type="button" value="Edit"/>

— Configure FDMA and Fraud Expert settings per payment method

## 5 Processus de décision relatif à la notation globale des fraudes

La notation globale des fraudes qui apparaît dans les rapports de transaction constitue le résultat de votre propre notation (FDMAc) et de celle de Fraud Expert conformément aux paramètres de la matrice que vous pouvez configurer dans votre Back Office via « Fraud detection > Fraud detection activation and configuration > Payment method > Edit (Détection des fraudes > Activation et configuration > Mode de paiement > Modifier) » :

VISA FDMAc
VISA Fraud Expert

### Fraud Expert configuration

Receive a second expert opinion and refine your fraud detection with Fraud Expert. This Global Risk Management module allows you to detect fraud earlier, protect yourself from complex fraud attacks whilst preventing the rejection of valid orders, by means of over 100 transaction scoring parameters and over 10,000 cross-parameter rules based on your specific industry. This module 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 that you want to review yourself.

**Fraud Expert Automatic Risk Scoring**

Not active
  Active

The Global Fraud Score you will see in your transaction reports will be the combination of your own rating (FDMA) and the Fraud Expert Scoring in accordance with the settings in the table below.

**Your activity sector**

Used to select 10.000+ predefined rules corresponding to your activity sector

**Fraud Expert additional Manual Review of Medium Risk transactions**

Not active
  Active

Review performed within hours. See technical user guide on how you will be notified of the Manual Review result.

**Global Fraud Score (combined results of FDMA/Fraud Expert modules)**

Colour in the table will replace colour of the FDMA Scoring result in the report.

FDMA rating result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	<input type="checkbox"/>			
Green	<input checked="" type="checkbox"/>		Expert manual review *	Merchant review *
Orange	<input checked="" type="checkbox"/>	Merchant review *	Expert manual review *	Merchant review *
Red	<input checked="" type="checkbox"/>	Merchant review *	Expert manual review *	
Red "black list"	<input type="checkbox"/>			

**Transaction Freeze of orange transactions**

Not active
  Active

If not active, transactions are not blocked and will be processed as usual. If active, orange transactions will stay in status 50, no automatic datacapture will take place until the Merchant selects to "unfreeze" or after a delay of 5 days.

Si toutes les actions concernant les règles FDMA ont la valeur "none" (aucune), le résultat de Fraud Expert déterminera le résultat de la transaction:

- Si le résultat de Fraud Expert est "low risk" (risque faible), la transaction sera envoyée pour autorisation.
- Si le résultat de Fraud Expert est "medium risk" (risque modéré), la transaction sera envoyée pour autorisation.
- Si le résultat de Fraud Expert est "high risk" (risque élevé), la transaction sera bloquée et l'état "2 - autorisation declined" (autorisation refusée) s'affichera.

### 5.1 Comment ça marche

Vous pouvez configurer la matrice de la notation globale des fraudes pour chaque moyen de paiement. Cette configuration permet de déterminer l'issue accordée à chaque transaction sur la base du résultat de la notation FDMA et de celle de Fraud Expert.

La combinaison des notations FDMA et Fraud Expert se traduit par une action prédéfinie :

- A. OK : Autorisation (vert)
  - B. Merchant review (Examen par le marchand) : Gel de la transaction au statut 50, autorisation manuelle requise par le marchand (orange) \*
- OU
- C. Expert Manual Review (Examen manuel par un expert) : Gel de la transaction au statut 50, attente de l'examen de la transaction par un expert (orange / seulement si l'option « Manual Review (Examen manuel) » est activée) \*
  - D. BLOCAGE : Rejet (rouge)

(\* Les actions B et C s'appliquent uniquement lorsque l'option « Gel des transactions » est activée. Si elle ne l'est pas, les transactions sont autorisées. Dans tous les cas, les transactions restent identifiables car marqués comme Orange.)

## 5.2 Exemples

Cette section propose des exemples de configuration concrets de la matrice de notation FDMA/Expert.

### Configuration par défaut

Dans la configuration par défaut, la couleur de la notation globale des fraudes est identique à celle de FDMA, sauf lorsque Fraud Expert pointe un risque moyen ou élevé alors que la notation FDMA n'en détecte pas. En pareil cas, les transactions sont marquées en orange « pour examen » afin de veiller à ce que le comportement suspect soit signalé et que vous puissiez l'identifier.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	<input checked="" type="checkbox"/>			
Green	<input checked="" type="checkbox"/>		Merchant review *	Merchant review *
Orange	<input checked="" type="checkbox"/>	Merchant review *	Merchant review *	Merchant review *
Red	<input checked="" type="checkbox"/>	Block	Block	Block
Red "black list"	<input checked="" type="checkbox"/>			

- Vous pouvez définir cette configuration si vous avez déjà un ensemble étendu de règles configurées dans FDMA et que vous souhaitez minimiser la fraude en faisant intervenir Fraud Expert en seconde ligne.

### Expert en tant que conseil sans impact sur l'état de la transaction

Dans cette configuration, la couleur de la notation globale des fraudes est toujours identique à celle de FDMA. Ainsi, quelle que soit l'appréciation du risque par Fraud Expert, son retour n'influence pas l'état de la transaction.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	<input checked="" type="checkbox"/>			
Green	<input checked="" type="checkbox"/>		OK	OK
Orange	<input checked="" type="checkbox"/>	Merchant review *	Merchant review *	Merchant review *
Red	<input checked="" type="checkbox"/>	Block	Block	Block
Red "black list"	<input checked="" type="checkbox"/>			

- Vous pouvez définir cette configuration si vous souhaitez utiliser Fraud Expert comme source d'information pour examiner les transactions suspectes et ajuster vos propres règles.

### Externalisation complète de l'analyse de la complexité et de la notation du risque à Expert

Dans cette configuration, la couleur de la notation globale des fraudes est toujours identique à celle de Fraud Expert. Ainsi, l'acceptation et le rejet des critères sont déterminés par la notation de Fraud Expert.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	<input checked="" type="checkbox"/>			
Green	<input checked="" type="checkbox"/>		Merchant review *	Block
Orange	<input checked="" type="checkbox"/>	OK	Merchant review *	Block
Red	<input checked="" type="checkbox"/>	OK	Merchant review *	Block
Red "black list"	<input checked="" type="checkbox"/>			

- Vous pouvez définir cette configuration si vous ne disposez pas de la compétence ou des ressources internes nécessaires pour procéder au suivi opérationnel de vos transactions.

### Optimisation du taux d'acceptation avec un haut taux d'examen

Dans cette configuration, les transactions sont considérées comme suspectes (orange) chaque fois que les couleurs FDMA et Fraud Expert diffèrent. Elles peuvent alors être examinées par notre équipe d'experts ainsi



que par vos propres experts.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	<input checked="" type="checkbox"/>			
Green	<input checked="" type="checkbox"/>		Merchant review *	Merchant review *
Orange	<input checked="" type="checkbox"/>	Merchant review *	Merchant review *	Merchant review *
Red	<input checked="" type="checkbox"/>	Merchant review *	Merchant review *	Merchant review *
Red "black list"	<input checked="" type="checkbox"/>			

• Vous pouvez définir cette configuration si vous disposez de suffisamment de ressources internes pour examiner les transactions.

Configuration « prudente »

Cette configuration est très semblable à la configuration par défaut. La seule différence intervient lorsque Fraud Expert renvoie l'état « Risque élevé ». Dans ce cas, la notation globale des fraudes des transactions est rouge, et les transactions sont bloquées.

FDMA scoring result	Launch fraud Expert	Fraud Expert scoring		
		Low-Risk	MediumRisk	High-Risk
Green "white list"	<input checked="" type="checkbox"/>			
Green	<input checked="" type="checkbox"/>		Merchant review *	Block
Orange	<input checked="" type="checkbox"/>	Merchant review *	Merchant review *	Block
Red	<input checked="" type="checkbox"/>	Block	Block	Block
Red "black list"	<input checked="" type="checkbox"/>			

• Vous pouvez définir cette configuration si vous souhaitez minimiser le taux de fraude et si vos propres règles FDMA ne sont pas trop strictes.

### 5.3 Gel des transactions

Pour toutes les transactions orange, vous pouvez activer la fonctionnalité « Transaction freeze (Gel des transactions) » pour mettre de côté les transactions en question (autorisées par l'acquéreur) pendant un certain nombre de jours, jusqu'à ce que vous les ayez examinées. Une fois cette période de gel passée, et dans la mesure où aucune action n'a été entreprise, la capture de données et le paiement sont traités automatiquement, comme habituellement.

Si vous n'activez pas la fonctionnalité « Transaction freeze (Gel des transactions) », le traitement de ces transactions s'effectue automatiquement, comme normalement.

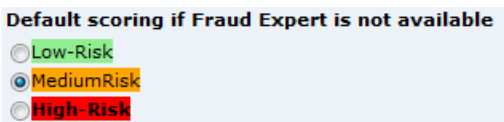
Il est à noter que les acquéreurs peuvent utiliser différentes périodes d'autorisation. Nous vous recommandons par conséquent de vérifier par moyen de paiement la limite pratiquée par votre acquéreur et de configurer la fonctionnalité « Transaction freeze (Gel des transactions) » en correspondance.

**Remarque**

Votre acquéreur peut vous fournir de plus amples informations sur l'expiration des autorisations.

### 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 default value is "Medium Risk".

## 6 Contrôle et examen des transactions

### 6.1 Généralités

Dans votre compte Ingenico ePayments, la page « View transactions (Afficher les transactions) » de la vue générale des transactions affiche trois colonnes dédiées à la détection des fraudes :

- FDMac rating (Notation FDMac) : vert foncé (DG), vert (G), orange (O), rouge (R), rouge foncé (DR)
- Fraud Expert scoring (Notation Fraud Expert) : risque faible, risque moyen, risque élevé (la notation est exprimée sous forme de pourcentage en fonction du niveau du risque ; plus le pourcentage est grand, plus le risque de fraude est élevé)
- Global Fraud Score (notation globale des fraudes) : note résultant de la combinaison de la notation FDMac et de la notation Fraud Expert selon la configuration effectuée dans la matrice de la notation globale des fraudes, vert (G), orange (O) ou rouge (R)

Exemple :

Pay ID	Merch ref	Orders	Status <sup>2</sup>	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%)

#### Astuce

Dans la zone « Advanced selection criteria (Critères de sélection avancés) » du menu « View transactions (Afficher les transactions) », vous pouvez filtrer les résultats sur la base de la notation globale des fraudes (vert/orange/rouge) et du résultat de l'examen manuel réalisé avec Fraud Expert (tous/vert/en suspens/rouge).

#### 6.1.1 Notation globale des fraudes

Le résultat de la notation globale des fraudes est vert (autorisation), rouge (blocage) ou orange.

Lorsque l'option transaction freeze (gel des transactions) est activée et que le résultat est orange, l'icône qui s'affiche représente soit une main, soit un sablier :



Main : en attente de l'examen par le marchand

Sablir : en attente de l'examen manuel par un expert

Pay ID	Merch ref	Orders	Status <sup>2</sup>	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

Dans les deux cas, le statut de la transaction est « 50-Authorised waiting external result (Autorisé en attente d'un résultat extérieur) » (si l'option *Transaction freeze (Gel des transactions)* est activée).

Avec l'option *Merchant review (Examen par le marchand)*, vous devez simplement soit supprimer l'autorisation, soit confirmer la commande.

Avec l'option *Fraud Expert Review (Examen par Fraud Expert)*, vous devez attendre que l'expert en fraude ait donné son appréciation du risque : faible ou élevé. En fonction de la configuration de la matrice, une nouvelle notation globale des fraudes est calculée.

Vous pouvez ignorer l'examen réalisé par l'expert en l'assurant vous-même conformément au processus applicable à l'examen par le marchand.

Pay ID	Merch ref	Status	Authorisation	Payment date	Total	File / line	NCID	Error	Action	Accept in	Charg Meth	Card/ACC no
100744373/0	2012910104322	50-Authorized waiting external result	test123	2012-09-10 10:43:27	12.34 EUR /			0	RES-Authorisation		VISA	XXXXXXXXXXXX1111

Back

Current Selection

Accept Order:100744373/0

Delete authorisation : 100744373/0

Si l'option Gel des transactions est activée, vous pouvez adapter le statut de la transaction dans la page scoring détails (voir [Examen avancé : Détails de la notation](#)).

## 6.2 Examen avancé : Détails de la notation

Pour obtenir une vue d'ensemble détaillée de la notation d'une transaction (*Détails de la notation*), vous pouvez sélectionner « View scoring details (Afficher les détails de la notation) » dans l'aperçu « Financial (Financier) » d'une transaction ou directement dans les résultats des transactions obtenus après une recherche via *View transactions (Gestion des transactions)*.

### 6.2.1 Résumé des données des transactions

Le premier aperçu auquel vous accédez correspond au résumé des données des transactions, qui présente les données générales des transactions correspondant à la notation.

#### Scoring detail

**Transaction data summary**

<p><b>Pay ID :</b> 321789456/0</p> <p><b>Merch ref :</b> Order_1234</p> <p><b>Total charge :</b> 10.00 EUR</p>	<p><b>Order date :</b> 2013-01-30 17:00:46</p> <p><b>Status :</b> 9-Payment requested</p> <p><b>Payment methods :</b> MasterCard</p>
--	--

**Cardholder has been successfully identified!**

**Card verification code :** OK  
**Card country :** FR (FRANCE)  
**IP address country :** FR (FRANCE)  
**Received IP address :** 88.28.211.208

### 6.2.2 Détails et données

Dans la section *Transaction data summary (Résumé des données des transactions)*, vous pouvez sélectionner l'option « Show details (Afficher les détails) » pour voir les données détaillées d'une transaction en particulier :

Data	
<b>Pay ID :</b> 321789456/0	<b>Merch ref :</b> Order_1234
<b>Action :</b> SAS-	<b>Order date :</b> 2013-01-30 17:00:46
<b>Status :</b> 9-Payment requested	<b>Description :</b>
<b>Authorized amount :</b> 10.00 EUR	<b>Authoriz. Number :</b> 395367
<b>Authorisation date :</b> 2013-01-30 17:02:28	<b>Payment date :</b> 2013-01-31 16:06:37
<b>Order amount :</b> 0.00 EUR	<b>Net with discount/premium :</b> 10.00 EUR
<b>Total charge :</b> 10.00 EUR	<b>Card/Account number :</b> XXXXXXXXXXXXX0638 :09/15
<b>Payment methods :</b> MasterCard	<b>Cardholder's name :</b> J. Cash
<b>Structured communication :</b> 032178945663	<b>Payment file :</b> /
<b>Authorisation code :</b> 395367	<b>AUMODE :</b> ONLINE
<b>NCMODE :</b> STD	<b>NC ID :</b> 955815532
<b>Transaction date :</b> 2013-01-31 16:06:37	<b>TID :</b> 45678654
<b>UID :</b> 1234567	<b>encoded by :</b> ../PSPID
<b>Invoicing customer :</b> J. Cash	<b>Reference :</b>
<b>Request's IP address :</b> [REDACTED]	<b>VAT number :</b>
<b>? NC ST/ER :</b> 0/0	<b>Invoicing customer :</b> J. Cash
<b>E-mail :</b> jcash@mail.com	
<b>Company name :</b>	
<b>Delivery customer :</b>	
<b>encoded by :</b> ../PSPID	

[Hide details](#)

### 6.2.3 Résumé de la notation des transactions

L'aperçu *Transaction scoring summary* (*Résumé de la notation des transactions*) présente les critères précis qui ont été satisfaits pour obtenir la notation globale des fraudes :

Transaction scoring summary		
Criteria	Weight	Comment
<b>FDMA</b>	70	<b>Category: Green (G)</b>
<b>Fraud Expert Scoring</b>	70	<b>High Risk</b> Ogone expert manual review status : reviewed on the: 2013-01-30 16:27:17 <b>Result: Rejected</b> <b>Comment: Research process, Same customer(s) has attempted to make the payment by using various country cards</b>
<b>Global Fraud Score</b>	Orange	<input type="checkbox"/> Change score to green <input type="checkbox"/> Change score to red Reviewer comment: <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div> <input type="button" value="Submit"/>

[Show details](#)

Vous pouvez modifier la couleur du score global de fraude si celui-ci est Orange. Si l'option Gel des transactions (Transaction freeze) est activé, cela modifiera automatiquement le statut de la transaction.

Si le score devient vert, alors la transaction est autorisée et puis capturée.

Si le score devient rouge, alors la transaction est en statut d'annulation d'autorisation.

Un clic sur le bouton « Show details (Afficher les détails) » permet d'accéder à des informations plus détaillées encore sur la notation :

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
<b>FDMA</b>		<b>Category: Green (G)</b>
Rule20067		Device Transaction Count exceeded threshold 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 successfully
<b>Fraud Expert Scoring</b>	<b>70</b>	<b>High Risk</b> 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
<b>Global Fraud Score</b>	<b>Orange</b>	<input type="checkbox"/> Change score to green <input type="checkbox"/> Change score to red Reviewer comment: <input type="text"/> <input type="button" value="Submit"/>
<input type="button" value="Hide details"/>		

Vous pouvez modifier la couleur du score global de fraude (Global Fraud Score) si celui-ci est Orange. Si l'option Gel des transactions (Transaction freeze) est activé, cela modifiera automatiquement le statut de la transaction.

Si le score devient vert, alors la transaction est autorisée puis capturée.

Si le score devient rouge, alors la transaction est en statut d'annulation d'autorisation.

### 6.2.4 États Contestations / Litige / Faux positif et actions

La section *États Contestations / Litige / Faux positif et actions* vous permet de réaliser les opérations suivantes :

- Marquer une transaction en tant que litige et sélectionner les données à placer dans les listes noires ou grises
- Compléter des listes blanches avec des données telles que les adresses IP

**Astuce**  
Pensez à marquer la transaction comme "fraude avérée" si l'acquéreur vous informe d'une fraude. Cela vous permette d'avoir une meilleure prévention grâce à Fraud Expert.

**Chargeback / Dispute / False Positives status and action**

Litige :

## Dispute

**Ref.:** 321789456  
**Order reference:** Order\_1234  
**Total charge:** 10 EUR  
**Status:** 9  
**Order date :** 2013-01-30 17:00:46

Data	Value	Comment	Add to the blacklist	Add to the greylists
Card/Account number	XXXXXXXXXXXX0638		<input checked="" type="checkbox"/>	<input type="checkbox"/>
IP address	85.226.211.209		<input checked="" type="checkbox"/>	<input type="checkbox"/>
customer e-mail	jcash@mail.com		<input type="checkbox"/>	<input checked="" type="checkbox"/>
Cardholder name	J. Cash		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Commercial dispute  
 Actual fraud

Dispute

End

Alimentation de listes blanches :

## Fill Whitelists

**Ref.:** 321789456  
**Order reference:** Order\_1234  
**Total charge:** 10 EUR  
**Status:** 9  
**Order date :** 2013-01-30 17:00:46

Data	Value	Comment	Add to the whitelist
IP address	85.226.211.209		<input type="checkbox"/>
CUI	jcash@mail.com		<input type="checkbox"/>

Submit

End

### 6.2.5 Résumé de l'historique corrélé des transactions

*Transaction correlated history summary (Résumé de l'historique corrélé des transactions)* est un aperçu qui vous permet de rechercher et d'afficher les transactions semblables à celle que vous examinez.

Vous pouvez sélectionner différents critères pour affiner les transactions qui s'affichent :

Transaction correlated history summary	
Search similar transactions from the last <input type="text" value="30"/> days with	
<input checked="" type="checkbox"/> Same Cardholder name	J. Cash
<input checked="" type="checkbox"/> Same E-mail	jcash@mail.com
<input checked="" type="checkbox"/> Same IP address	85.226.211.209
<input type="checkbox"/> Same IP country	FRANCE (FR)
<input type="checkbox"/> Same CC country	FRANCE (FR)
<input checked="" type="checkbox"/> Same Card number	XXXXXXXXXXXX0638
<input checked="" type="checkbox"/> Same Device ID	9fcd95604kl47e324226b20c11029683
<input checked="" type="checkbox"/> Same Pay ID	321789456
<input type="radio"/> AND <input checked="" type="radio"/> OR	
<span style="border: 1px solid gray; padding: 2px 5px;">Start lookup 1</span>	

Aperçu des transactions après la recherche 1 :

Start period : 2013-01-30 End period : 2013-02-27		Number of transactions :	8	Number of different IP addresses :	4
		Number of settled transactions :	4	Number of different card numbers :	8
		Number of transactions already tagged as Fraud/Commercial Dispute :	0	Number of different email addresses :	7
		Percentage of cancelled transactions :	0 %	Number of different Owner :	7
		Percentage of rejected transactions :	44 %	Number of different IP address country :	1
				Number of different CC country :	1
				Number of different DeviceID :	1

Ref.	Total charge	Payment date	Status	NCERROR	Global Fraud Score	FDMAC rating	Fraud Expert scoring	3dSecure	Owner	E-mail	IP address	Device ID	Card no.	Expert Profile Category	IPCTY	CCCTY	Order reference
321789456/0	10.00 EUR	2013-01-30 17:02:26	5		(O)	G	70 %		J. Cash	jcash@mail.com	88.200.100.100	...0c11029683	...X0638	n/a	FR	FR	Order_1234
321799654/0	10.00 EUR	2013-01-30 22:47:13	5		(G)	G	n/a		J. Cash	jcash@mail.com	88.200.100.100	...0c11029683	...X0638	n/a	FR	FR	Order_2163
331432651/0	10.00 EUR	2013-01-31 12:20:42	2	30341005 - Suspicion of fraud (Expert)	(R)	G	100 %		J. Cash	jcash@mail.com	88.200.100.100	...0c11029683	...X0638	n/a	FR	FR	Order_3113
331439523/0	10.00 EUR	2013-01-31 12:31:05	2	40001134 - Authentication failed. Please retry or cancel.	-	G	n/a		J. Cash	psp321456@yahoo.com	88.200.100.100	n/a	...X0638	n/a	FR	FR	Order_3193

Un clic sur le bouton « Ref. (Réf.) » (PAYID) permet d'accéder aux détails de la notation concernant la transaction correspondante.

Dans la page qui affiche les résultats de la « recherche 1 », vous pouvez lancer la recherche 2 pour vérifier les données des transactions corrélées. Il en va de même pour la recherche 3 et pour les suivantes.

## 7 Annexe : Empreinte numérique des matériels via DirectLink

Les informations ci-dessous s'adressent aux marchands souhaitant utiliser la fonctionnalité [Device fingerprinting](#) dans le cadre de l'intégration DirectLink.

Il convient d'envoyer un code de suivi en HTML, un code composé à partir d'éléments CSS, JavaScript et Flash. Ce code doit être inséré dans l'en-tête d'une page web à charger au moment où l'ordinateur du client visite le site. Cette page doit idéalement n'être chargée qu'une seule fois au cours de la session de l'utilisateur et correspondre à une page sur laquelle l'utilisateur reste pendant au moins 5 secondes. C'est le plus souvent celle où l'utilisateur entre ses informations de paiement.

Ce code HTML est associé à un identifiant de session temporaire et aléatoire unique (SID) généré par vous de la façon décrite dans le tableau ci-dessous.

Paramètre	Explication	Exemple
SID	Identifiant unique de la session d'un utilisateur.  La concaténation des valeurs du PSPID et de l'ORDERID, respectivement, est calculée dans le format MD5, avec pour résultat une chaîne de hachage hexadécimale à 32 caractères.	<i>ec4dfe7e880e374071e2728c3711c3a8</i>
AID	Identifiant du compte d'application de suivi.  C'est toujours la même valeur (fixe). 10376	

L'exemple ci-dessous illustre comment se présente le fragment de code. Vous devez mettre à jour la chaîne «XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX» dans l'exemple avec un identifiant de session d'utilisateur unique au format MD5.

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



## 8 Annexe : Secteurs d'activité

La liste ci-dessous présente tous les secteurs d'activité (branches industrielles) que vous pouvez sélectionner dans la configuration de l'examen automatique réalisé par Fraud Expert. En fonction du secteur que vous choisissez s'appliquent différentes règles et différents critères de notation prédéfinis.

Description du secteur	Exemple
Voyage & tourisme Secteur d'activité ou industrie qui consiste à fournir des informations, des hébergements, des moyens de transport et d'autres services à des touristes.	Il s'agit d'un secteur très vaste qui inclut les secrétariats d'État au tourisme, les services de l'immigration et des douanes, les agences de voyage, les voyagistes de même que les compagnies aériennes et les services de réservation d'hôtel, etc.
Billetterie Tout ou tous processus impliqués dans la collecte de tarifs et l'émission de tickets pour des événements ou de billets pour toute forme de transport.	Activité impliquant les transports publics tels que les sociétés de transport par autobus ou les compagnies de chemin de fer, mais aussi les films, les événements, les salons professionnels, etc.
Achats Processus par lequel les consommateurs achètent directement des biens ou des services auprès d'un vendeur en temps réel.	Tous les sites web et portails de commerce électronique vendant des produits électroniques tels que des ordinateurs, des ordinateurs portables, des téléphones mobiles, des bijoux, etc.
Cadeaux Transfert volontaire de propriété ou d'un intérêt de propriété d'une personne à une autre, effectué gracieusement au profit du destinataire.	Très commun pour les sites d'achats en ligne, mais s'applique à des produits spécifiques tels que les chocolats, les gâteaux, les fleurs, etc.
Services web Services en ligne fournis à partir d'un site web.	Services d'hébergement, développement d'applications, panier d'achats, enregistrement de nom de domaine, conception et développement de sites web.
Risque élevé Type de secteur plus enclin à faire l'objet de fraudes.	ONG, organisations caritatives, dons, etc.
Recharge Secteur impliqué dans la recharge de tout service de type commercial.	Recharge de cartes de communication mobile postpayées ou prépayées, recharge de services de télévision par satellite, etc.
Services réguliers Toute organisation, parfois privée, fournissant des services au grand public.	Sociétés de distribution d'énergie (électricité, gaz, eau), opérateurs téléphoniques, sociétés de télédistribution, établissements de soin, services conseils, etc.
Centre d'appel Bureau centralisé utilisé dans le but de recevoir ou de transmettre un grand volume de demandes par téléphone.	Téléachat, réservations de type marketing.
Tickets d'avion Activité impliquant la réservation de billets d'avion.	Compagnies aériennes elles-mêmes, agents associés et de réservation.

Description du secteur	Exemple
Hôtels et lieux de séjour Réservation de chambres.	Hôtels et hébergements touristiques, services et agents des plateformes de gestion des réservations (GDS).
Achats à haut risque Activité consistant à vendre des produits facilement revendables.	Articles de luxe ou précieux : bijoux en or, en argent, etc.
Services informatiques Services en ligne fournis via l'internet.	Support et services informatiques, mises à jour de programmes antivirus, logiciels téléchargeables.