

# Module de Détection de Fraude

Guide de Configuration pour le Module de Détection de Fraude v.4.2.3

## Table des matières

<b>1</b>	<b>Qu'est-ce le Module de Détection de Fraude?</b>	<b>4</b>
1.1	Avantages	4
1.2	Accès	4
1.3	Contenu	4
<b>2</b>	<b>Activation et configuration de la détection des fraudes</b>	<b>5</b>
2.1	Cartes de crédit	5
2.1.1	Règles de blocage	5
2.1.1.1	Pays de l'adresse IP	5
2.1.1.2	Cohérence de pays (pour Visa, MasterCard, American Express et Diners Club seulement)	5
2.1.1.3	3-D Secure (Pour Visa/MasterCard/JCB/AmEx seulement)	6
2.1.2	Limites	6
<b>3</b>	<b>3-D Secure</b>	<b>7</b>
3.1	Général	7
3.1.1	Demande d'affiliation	7
3.1.2	Procédé de transaction du 3-D Secure standard	7
3.2	Options de configuration	8
3.2.1	Problème technique	8
3.2.2	Service d'identification temporairement indisponible	8
3.2.3	Échec de l'identification (MasterCard seulement)	8
3.2.4	Activer/Désactiver le 3-D Secure	8
3.2.5	Désactiver le 3-D Secure pour un BIN spécifique	8
<b>4</b>	<b>Liste noire / liste blanche</b>	<b>9</b>
4.1	Cartes de crédit	9
4.1.1	Liste noire des cartes	9
4.1.2	Liste noire des BIN	9
4.1.3	Liste noire des adresses IP	10
4.1.4	Liste blanche des adresses IP	10
<b>5</b>	<b>Dispute</b>	<b>11</b>
5.1	Ajouter des données de transaction à une liste noire et blanche	11
<b>6</b>	<b>Retour sur le Module de Détection de Fraude</b>	<b>14</b>

---

6.1	Aperçu des transactions dans le module de gestion.....	14
6.1.1	Critères de sélection avancés .....	14
6.1.2	3-D Secure dans la liste des transactions .....	14
6.1.3	Renseignements concernant la transaction .....	14
6.1.4	Codes erreurs .....	15
6.2	Paramètres de transaction supplémentaires.....	15
7	<b>Annexe: CVC2 et AAV</b> .....	18
7.1	CVC2 .....	18
7.2	AAV .....	18

# 1 Qu'est-ce le Module de Détection de Fraude?

En matière de vente par correspondance, la lutte contre la fraude nécessite un savoir faire, de la rapidité et de la flexibilité. Pour vous aider à mettre en œuvre l'application efficace de la gestion du risque, le module de détection de fraude vous offre un service en temps réel qui vous propose toutes les informations d'analyse nécessaires et les offres de protection personnalisées pour traiter les transactions douteuses.

Cependant, l'utilisation du module de détection de fraude ne garantit pas l'élimination de toutes les fraudes ; il vous aide seulement à les combattre. Le module de détection de fraude peut être configuré selon les risques ou les problèmes de fraude vécus par le passé au sein de votre entreprise.

## 1.1 Avantages

Le module de détection de fraude vous permet de :

- Détecter des anomalies pendant les transactions
- Faire immédiatement opposition à toutes les tentatives effectuées par des fraudeurs connus
- Protéger contre les risques spécifiques à un pays
- Définir et appliquer des politiques de sécurité personnalisées
- Bénéficier d'une garantie de paiement conditionnelle (voir la section 2.1.2) selon les politiques d'acquéreur à titre individuel (3-D Secure).

## 1.2 Accès

Vous pouvez accéder au module de détection de fraude via le lien « Fraud detection » dans le menu de votre compte.

## 1.3 Contenu

Le module de détection de fraude comprend trois parties distinctes et fonctionnelles : «Activation et configuration de la détection des fraudes», « 3-D Secure » et « Liste noire / liste blanche ».



Nous allons maintenant regarder de plus près et voir comment configurer le *modus operandi* et les critères de 3-D Secure pour les cartes de crédit VISA et MasterCard.

### Important

Les critères des cartes VISA et MasterCard décrits dans cette documentation ne sont pas nécessairement disponibles pour toutes les méthodes de paiement. La disponibilité de la « Sélection multicritères » dépend de la méthode de paiement. Pour certaines méthodes de paiement, la configuration est limitée aux options de « Limites ». Nous recommandons la vérification des critères de sélection spécifiques pour vos méthodes de paiement individuelles en cliquant sur le bouton « Éditer » près de la méthode de paiement dans le tableau « Sélection multicritères des méthodes de paiement » dans votre module de détection de fraude.

## 2 Activation et configuration de la détection des fraudes

Dans le tableau « Activation et configuration », vous distinguerez les cartes de crédit et les autres méthodes de paiement.

Il y a les règles de blocage et les limites offerts comme options. « Non » indique que rien n'a été configuré dans la page option concernée. Lorsqu'une page a déjà été configurée, le statut sera donc « Oui »

Nous allons maintenant regarder de plus près pour voir comment configurer les options de détection de fraude pour les cartes de crédit.

### 2.1 Cartes de crédit

Pour configurer les options de détection de fraude pour une carte de crédit spécifique, cliquez sur le bouton « Editer » près de la méthode de paiement. Vous entrerez alors sur la page configuration avec les onglets pour les règles de blocage et les limites.

#### 2.1.1 Règles de blocage

Les règles de blocage sont applicables dès que le client entre les données de sa carte de crédit et clique sur le bouton procéder.

Si la transaction ne respecte pas les règles que vous avez entrées, nous retiendrons cette transaction et fixerons son statut à « Autorisation refusée ».

##### 2.1.1.1 Pays de l'adresse IP

Tous les pays de l'adresse IP sont acceptés par défaut. Notre système peut identifier le pays d'une adresse IP selon l'adresse IP d'un client (bien que, dans tous les cas, cette vérification donne des résultats positifs à 94%, elle est basée sur des listes IP fournies extérieurement, donc il existe tout de même un léger risque puisque nous dépendons de l'exactitude de cette liste). Si vous voulez établir une liste de pays pour l'adresse IP, vous pouvez sélectionner ceux-ci à partir de la liste située à la droite de votre écran et cliquer sur le bouton « Ajouter ».

#### IMPORTANT

Les codes A1 (proxy anonyme), AP (région pacifique de l'Asie), EU (réseau européen) et A2 (Provider satellite) font référence aux adresses IP pour lesquelles le pays d'origine est inconnu.

EU, par exemple, signifie que le pays exact de l'adresse IP est inconnu mais qu'il appartient à l'Europe. Accepter EU comme pays d'adresse IP ne signifie pas que vous acceptez les paiements provenant de tous les pays d'Europe ; cela signifie que vous acceptez les paiements provenant des adresses IP gérées par des institutions européennes. Si vous voulez accepter des paiements provenant des pays d'Asie ou d'Europe, vous devez ajouter les pays un par un sur votre liste.

Les proxys anonymes sont des fournisseurs d'accès Internet qui permettent aux utilisateurs Internet de dissimuler leur adresse Internet. Nous vous recommandons de ne pas accepter de paiements provenant d'un proxy anonyme !

Au-dessus de la liste des pays de l'adresse IP sélectionnés, vous avez le choix d'établir votre liste pour les pays acceptés (*Accepter uniquement les paiements des pays de la liste*) ou pour les pays refusés (*Refuser les paiements originaux des pays de la liste*).

Vous pouvez toujours supprimer un pays dans la liste en cliquant sur la boîte « Del » devant le pays et ensuite cliquer sur le bouton « Envoyer » sous la liste.

##### 2.1.1.2 Cohérence de pays (pour Visa, MasterCard, American Express et Diners Club seulement)

Lorsque vous fixez ce paramètre à « Oui », vous permettez aux transactions d'avoir lieu seulement si l'adresse IP du client est dans le même pays que l'émetteur de la carte de crédit, en d'autres termes, seulement si le pays de la carte et le pays de l'adresse IP sont identiques. Cette vérification n'est pas

effectuée si l'adresse IP provient d'un proxy anonyme, du réseau pacifique de l'Asie, du réseau européen ou d'un fournisseur satellite.

### 2.1.1.3 3-D Secure (Pour Visa/MasterCard/JCB/AmEx seulement)

Ce paramètre vous permet de contourner les règles de blocage fixées ci-dessus si le titulaire d'une carte est identifié par le 3-D Secure.

Lorsqu'une carte de crédit est identifiée par le 3-D Secure et que vous avez un contrat de 3-D Secure avec votre acquéreur, vous aurez une garantie de paiement conditionnelle (voir la Section 2.1.2) pour la transaction. De cette façon, même si vous ne souhaitez pas recevoir de paiements d'un pays X en raison d'un haut risque de fraude, vous pouvez tout de même permettre les transactions avec les cartes de crédit 3-D Secure d'un pays X puisque vous ne courez aucun risque concernant les conflits entourant la non-identification du titulaire de la carte (cependant, ceci ne s'applique pas aux conflits qui touchent d'autres questions, voir le chapitre 2).

**CreditCard/VISA**

Blocking rules	Limits														
<p><b>Card country</b></p> <p> <input type="radio"/> Accept only payment from country list  <input checked="" type="radio"/> Reject payment from country list                 </p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10px;">Del</th> <th style="width: 100%;">Selected countries</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/></td><td>ANTARCTICA</td></tr> <tr><td><input type="checkbox"/></td><td>BAHAMAS</td></tr> <tr><td><input type="checkbox"/></td><td>PALAO ISLES</td></tr> <tr><td><input type="checkbox"/></td><td>Select all</td></tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Submit"/></p>	Del	Selected countries	<input type="checkbox"/>	ANTARCTICA	<input type="checkbox"/>	BAHAMAS	<input type="checkbox"/>	PALAO ISLES	<input type="checkbox"/>	Select all	<p>Select (Multiple selection possible)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>AFGHANISTAN</td></tr> <tr><td>ALBANIA</td></tr> <tr><td>ALGERIA</td></tr> <tr><td>ANDORRA</td></tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Add"/></p>	AFGHANISTAN	ALBANIA	ALGERIA	ANDORRA
Del	Selected countries														
<input type="checkbox"/>	ANTARCTICA														
<input type="checkbox"/>	BAHAMAS														
<input type="checkbox"/>	PALAO ISLES														
<input type="checkbox"/>	Select all														
AFGHANISTAN															
ALBANIA															
ALGERIA															
ANDORRA															
<p><b>IP address country</b></p> <p> <input type="radio"/> Accept only payment from country list  <input checked="" type="radio"/> Reject payment from country list                 </p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10px;">Del</th> <th style="width: 100%;">Selected countries</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/></td><td>Anonymous Proxy</td></tr> <tr><td><input type="checkbox"/></td><td>ARUBA</td></tr> <tr><td><input type="checkbox"/></td><td>WALLIS - F.</td></tr> <tr><td><input type="checkbox"/></td><td>Select all</td></tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Submit"/></p>	Del	Selected countries	<input type="checkbox"/>	Anonymous Proxy	<input type="checkbox"/>	ARUBA	<input type="checkbox"/>	WALLIS - F.	<input type="checkbox"/>	Select all	<p>Select (Multiple selection possible)</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>Asia Pacific Network (AP)*</td></tr> <tr><td>European network (EU)*</td></tr> <tr><td>Satellite Provider (A2)*</td></tr> <tr><td>AFGHANISTAN (AF)</td></tr> </tbody> </table> <p style="text-align: right;"><input type="button" value="Add"/></p> <p><small>* Special country codes</small></p>	Asia Pacific Network (AP)*	European network (EU)*	Satellite Provider (A2)*	AFGHANISTAN (AF)
Del	Selected countries														
<input type="checkbox"/>	Anonymous Proxy														
<input type="checkbox"/>	ARUBA														
<input type="checkbox"/>	WALLIS - F.														
<input type="checkbox"/>	Select all														
Asia Pacific Network (AP)*															
European network (EU)*															
Satellite Provider (A2)*															
AFGHANISTAN (AF)															
<p><b>Countries consistency</b></p> <p>Card country and IP address country must be identical:                      This test is not performed if the IP address comes from a region (A1, A2, EU, AP)</p> <p style="text-align: right;"> <input type="radio"/> Yes  <input checked="" type="radio"/> No  <input type="button" value="Submit"/> </p>															
<p><b>3DSecure</b></p> <p>Accept all countries if the 3DSecure/SPA ucaf authentication is successful</p> <p style="text-align: right;"> <input checked="" type="radio"/> Yes  <input type="radio"/> No  <input type="button" value="Submit"/> </p>															

## 2.1.2 Limites

Dans le module de détection de fraude, vous pouvez limiter le montant par transaction.

Vous pouvez entrer un montant minimum et un montant maximum. Si le montant de la transaction ne se retrouve pas dans ces limites, nous retiendrons cette transaction et fixerons son statut à « Autorisation refusée ».

La devise de la limite sera la principale devise de votre compte. Si vous avez plusieurs devises et qu'une transaction est effectuée dans une devise autre que la vôtre, notre système convertira la limite dans cette autre devise.

## 3 3-D Secure

Le 3-D Secure offre un niveau élevé de sécurité puisqu'il permet aux clients d'être identifiés sans équivoque grâce à toutes les technologies, comme les mots de passe html, les *digipass*, les lecteurs de cartes, les biométriques et bien d'autres, appliquées par les banques émettrices.

En offrant le 3-D Secure, un marchand bénéficie de la garantie de paiement conditionnelle décrite dans le contrat de 3-D Secure avec son acquéreur. Sous ces conditions, le compte d'un marchand n'est plus débiteur en matière de conflits concernant la « non-identification du titulaire de la carte » (ceci ne s'applique pas aux conflits qui touchent d'autres questions !).

Les brands suivantes ont appliqué le protocole de 3-D Secure :

- Visa sous le nom de [Verified by Visa](#)
- MasterCard sous le nom de [SecureCode](#)
- JCB sous le nom de [J-Secure](#)
- American Express sous le nom de [SafeKey](#)

### 3.1 Général

#### 3.1.1 Demande d'affiliation

Si le 3-D Secure n'est pas activée dans votre compte, vous verrez un bouton « Demander 3DS » dans le tableau « 3-D Secure ».

Si vous cliquez sur le bouton « Demander 3DS », un email sera envoyé à votre acquéreur. Si votre contrat avec l'acquéreur ne vous fournit pas le 3-D Secure, vous pouvez contacter votre acquéreur pour obtenir davantage d'informations concernant l'inscription au 3-D Secure. Indiquez à votre acquéreur que vous désirez avoir l'option de paiement du 3-D Secure.

Remarque : Pour s'enregistrer avec SafeKey, veuillez contacter American Express ou aller sur le portail SafeKey.

Une fois que le 3-D Secure a été activée dans votre compte, vous pourrez voir la date d'activation dans le tableau. Vous pouvez modifier la configuration du 3-D Secure en cliquant sur le bouton « Éditer » situé près des méthodes de paiement.

#### 3.1.2 Procédé de transaction du 3-D Secure standard

1. Lorsque nous recevons les données de carte de crédit de votre client, nos systèmes envoient une demande au répertoire VISA/MasterCard/JCB/AmEx afin de déterminer si la carte est inscrite, c'est-à-dire que le titulaire de la carte a reçu certains moyens d'identification liés à sa carte et, si approprié, a obtenu les données du serveur pour l'identification de l'émetteur.
2. Si la carte est inscrite, nos systèmes redirigent l'acquéreur vers le serveur d'identification de l'émetteur pour débiter l'identification.
3. Nos systèmes reçoivent le résultat de l'identification et procèdent au paiement comme c'est fait habituellement.

Si l'identification est réussie, le marchand peut bénéficier de la garantie de paiement conditionnelle fournie par son acquéreur.

Si la carte n'est pas inscrite, le marchand reçoit un certain niveau de garantie de paiement conditionnelle fournie par son acquéreur.

Donc, dans les deux cas, le marchand possède, sous certaines conditions (définies par VISA, MasterCard et les organismes financiers, et comme décrit dans le contrat 3-D Secure avec son acquéreur), une garantie de paiement, même sans réception des informations identifiant le client. Ces règles concernant la garantie de paiement conditionnelle sont gérées exclusivement entre le marchand et son acquéreur. Ingenico ePayments agit seulement à titre d'intermédiaire technique.

## 3.2 Options de configuration

La section suivante décrit les options de configuration pour Verified by VISA, SecureCode, J-Secure et SafeKey. En fonction de votre acquéreur, certaines (ou toutes) ces options ne seront peut-être pas garanties.

### 3.2.1 Problème technique

Le marchand peut choisir de *continuer* ou d'*interrompre* la transaction si un problème technique empêche la connexion au répertoire VISA/MasterCard/JCB/AmEx pendant la vérification d'une inscription au 3-D Secure.

Si un problème technique empêche notre système de se connecter au répertoire VISA/MasterCard/JCB/AmEx (étape 1 sous 2.1.2), VISA/MasterCard/JCB/AmEx recommandent que le procédé soit poursuivi sans identification (option *continuer*). Dans ce cas, toutefois, le marchand ne bénéficiera pas de la garantie de paiement conditionnelle (voir la section 2.1.2).

### 3.2.2 Service d'identification temporairement indisponible

Le marchand peut choisir de *continuer* ou d'*interrompre* la transaction si le service d'identification du titulaire de la carte est temporairement indisponible.

Si le serveur d'identification de l'émetteur est temporairement indisponible (étape 2 sous 2.1.2), l'identification du titulaire de la carte ne sera pas possible. Dans ce cas, VISA/MasterCard/JCB/AmEx recommandent que le procédé soit poursuivi (option *continuer*). Dans ce cas, toutefois, le marchand ne bénéficiera pas de la garantie de paiement conditionnelle (voir la section 2.1.2).

### 3.2.3 Échec de l'identification (MasterCard seulement)

Le marchand peut choisir de *continuer* ou d'*interrompre* la transaction s'il y a échec lors de l'identification.

S'il y a échec lors de l'identification du titulaire de la carte (étape 3 sous 2.1.2), MasterCard recommande que le procédé soit interrompu (option *interrompre*). Si la transaction est poursuivie, le marchand ne bénéficiera pas de la garantie de paiement conditionnelle (voir la section 2.1.2).

### 3.2.4 Activer/Désactiver le 3-D Secure

Ici, le marchand peut activer ou désactiver le 3-D Secure pour les cartes VISA/MasterCard/JCB/AmEx. Important : si le 3-D Secure est invalide, le marchand ne bénéficiera pas de la garantie de paiement conditionnelle (voir la section 2.1.2).

### 3.2.5 Désactiver le 3-D Secure pour un BIN spécifique

Le marchand peut entrer certaines séries de BIN dont il veut désactiver le 3-D Secure si le titulaire de la carte n'est pas inscrit.

Si la carte n'est pas inscrite, le marchand ne bénéficiera pas de la garantie de paiement conditionnelle (voir la section 2.1.2) pour les paiements faits à partir de la carte dont le numéro débute par ces 6 chiffres.



## 4 Liste noire / liste blanche

Dans le module de détection de fraude, vous avez la possibilité de créer vos propres listes noires pour les cartes de crédit à partir du code BIN, les numéros de carte de crédit et les adresses IP dont vous ne désirez pas accepter de transactions. Vous pouvez aussi produire une liste blanche (autorisée) à partir des adresses IP.

« Non » indique que rien n'a été configuré dans la liste noire/liste blanche concernée. Lorsqu'une liste noire/liste blanche a déjà été configurée, le statut sera donc « Oui ».

Si, pour une nouvelle transaction effectuée dans votre compte, le BIN, le numéro de carte de crédit ou l'adresse IP ont été inscrits dans votre liste noire, nous retiendrons cette transaction et fixerons son statut à « Autorisation refusée ».

### 4.1 Cartes de crédit

Un maximum de 50 entrées est possible par liste.

Vous pouvez ajouter un commentaire pour toute information enregistrée dans vos « listes noires » et « listes blanches ».

Vous pouvez l'insérer immédiatement dans le champ « Commentaire: ». Vous pouvez également en insérer de nouveaux où en effacer en cliquant sur le lien « ... » de la colonne commentaire.

Pour chaque entrée, vous pouvez choisir la raison pour laquelle vous désirez faire opposition : Fraude avérée ou Différend commercial.

**IMPORTANT**

Ne sélectionnez Actual fraud (Fraude effective) que si vous recevez un rejet de débit avec un code de motif de fraude.

#### 4.1.1 Liste noire des cartes

Dans la liste noire de votre carte de crédit, vous devez entrer le numéro complet de la carte de crédit. Vous pouvez toujours supprimer des numéros de cartes de crédit qui ont été entrés dans votre liste.

Si vous avez activé les méthodes de paiement Direct Debit NL, Direct Debit DE ou Direct Debit AT dans votre compte, la liste noire de numéros de cartes servira également de liste noire de numéros de comptes.

Cards	BIN	IP addresses	Trusted IP addresses																								
<p><b>Cards blacklist</b> This list contains 2 items.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Delete</th> <th>Card number</th> <th>BRAND</th> <th>Payid</th> <th>Fraud type</th> <th>Date</th> <th>Encoded By</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>XXXXXXXXXXXX9999</td> <td>MasterCard</td> <td></td> <td>COM</td> <td>02/10/2007</td> <td>GFR2oec/GFR2oec/PSPID</td> <td>...</td> </tr> <tr> <td><input type="checkbox"/></td> <td>XXXXXXXXXXXX1111</td> <td>VISA</td> <td></td> <td>COM</td> <td>27/03/2008</td> <td>GFR2oec/GFR2oec/PSPID</td> <td>...</td> </tr> </tbody> </table> <p>Enter a new item: <input style="width: 150px;" type="text"/></p> <p> <input type="radio"/> Actual fraud  <input checked="" type="radio"/> Commercial dispute                 </p> <p>Comment: <input style="width: 100px;" type="text"/></p> <p style="text-align: center;"><input type="button" value="Submit"/></p>				Delete	Card number	BRAND	Payid	Fraud type	Date	Encoded By	Comment	<input type="checkbox"/>	XXXXXXXXXXXX9999	MasterCard		COM	02/10/2007	GFR2oec/GFR2oec/PSPID	...	<input type="checkbox"/>	XXXXXXXXXXXX1111	VISA		COM	27/03/2008	GFR2oec/GFR2oec/PSPID	...
Delete	Card number	BRAND	Payid	Fraud type	Date	Encoded By	Comment																				
<input type="checkbox"/>	XXXXXXXXXXXX9999	MasterCard		COM	02/10/2007	GFR2oec/GFR2oec/PSPID	...																				
<input type="checkbox"/>	XXXXXXXXXXXX1111	VISA		COM	27/03/2008	GFR2oec/GFR2oec/PSPID	...																				

#### 4.1.2 Liste noire des BIN

Le code BIN est représenté par les six premiers chiffres d'un numéro de carte de crédit. Un code BIN est lié à une banque d'un pays spécifique. Par conséquent, vous pouvez entrer toutes les cartes de crédit émises d'une banque X provenant d'un pays Y dans votre liste noire, simplement en ajoutant le code BIN. Vous pouvez toujours supprimer des codes BIN qui ont été entrés dans votre liste :

Cards	BIN	IP addresses	Trusted IP addresses														
<p><b>BIN blacklist</b> This list contains 1 item.</p> <table border="1"> <thead> <tr> <th>Delete</th> <th>BIN</th> <th>BRAND</th> <th>Fraud type</th> <th>Date</th> <th>Encoded By</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Sel. All</td> <td>111111</td> <td></td> <td><input checked="" type="checkbox"/></td> <td>28/03/2007</td> <td>GFR2oec/GFR2oec/PSPID</td> <td>...</td> </tr> </tbody> </table> <p>Enter a new item: <input type="text"/></p> <p> <input type="radio"/> Actual fraud      <input type="text" value="Comment:"/>   <input checked="" type="radio"/> Commercial dispute                 </p> <p align="center"><input type="button" value="Submit"/></p>				Delete	BIN	BRAND	Fraud type	Date	Encoded By	Comment	<input type="checkbox"/> Sel. All	111111		<input checked="" type="checkbox"/>	28/03/2007	GFR2oec/GFR2oec/PSPID	...
Delete	BIN	BRAND	Fraud type	Date	Encoded By	Comment											
<input type="checkbox"/> Sel. All	111111		<input checked="" type="checkbox"/>	28/03/2007	GFR2oec/GFR2oec/PSPID	...											

### 4.1.3 Liste noire des adresses IP

Dans votre liste noire des adresses IP, vous pouvez non seulement entrer une adresse IP spécifique, mais aussi une série d'adresses IP qui utilisent les formats suivants : a.b.c-d.0-255 ou a.b.c-d.\* ou a.b.c.d-e. Vous pouvez toujours supprimer des adresses IP qui ont été entrées dans votre liste.

Afin que notre système vérifie l'adresse IP du client, les marchands qui travaillent via DirectLink doivent envoyer l'adresse IP dans le champ « REMOTE\_ADDR ».

Cards	BIN	IP addresses	Trusted IP addresses														
<p>You may enter a range of IP addresses. The acceptable format is a.b.c-d.0-255 or a.b.c-d.* or a.b.c.d-e.</p> <p><b>IP blacklist</b> This list contains 1 item.</p> <table border="1"> <thead> <tr> <th>Delete</th> <th>IP addresses</th> <th>Payid</th> <th>Fraud type</th> <th>Date</th> <th>Encoded By</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Sel. All</td> <td>1.12.1.123</td> <td></td> <td>FRA</td> <td>24/09/2008</td> <td>GFR2oec/GFR2oec/PSPID</td> <td>...</td> </tr> </tbody> </table> <p>Enter a new item: <input type="text"/></p> <p> <input type="radio"/> Actual fraud      <input type="text" value="Comment:"/>   <input checked="" type="radio"/> Commercial dispute                 </p> <p align="center"><input type="button" value="Submit"/></p>				Delete	IP addresses	Payid	Fraud type	Date	Encoded By	Comment	<input type="checkbox"/> Sel. All	1.12.1.123		FRA	24/09/2008	GFR2oec/GFR2oec/PSPID	...
Delete	IP addresses	Payid	Fraud type	Date	Encoded By	Comment											
<input type="checkbox"/> Sel. All	1.12.1.123		FRA	24/09/2008	GFR2oec/GFR2oec/PSPID	...											

### 4.1.4 Liste blanche des adresses IP

Si, vous avez fait opposition pour certains pays ou certaines adresses IP dans les règles de blocage, vous avez fait opposition à un client spécifique dont vous aimeriez accepter des commandes, vous pouvez entrer son adresse IP dans la liste blanche des adresses IP. De cette façon, vous autorisez les transactions à partir de cette adresse IP même si elles proviennent d'un pays bloqué. Vous pouvez toujours supprimer des adresses IP qui ont été entrées dans votre liste.

Afin que notre système vérifie l'adresse IP du client, les marchands qui travaillent via DirectLink doivent envoyer l'adresse IP sur le champ « REMOTE\_ADDR ».

Cards	BIN	IP addresses	Trusted IP addresses												
<p>You may enter a range of IP addresses. The acceptable format is a.b.c-d.0-255 or a.b.c-d.* or a.b.c.d-e.</p> <p><b>IP addresses whitelist</b> This list contains 1 item.</p> <table border="1"> <thead> <tr> <th>Delete</th> <th>Trusted IP addresses</th> <th>Payid</th> <th>Date</th> <th>Encoded By</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> Sel. All</td> <td>1.12.1.123</td> <td></td> <td>24/09/2008</td> <td>GFR2oec/GFR2oec/PSPID</td> <td>...</td> </tr> </tbody> </table> <p>Enter a new item: <input type="text"/></p> <p>Comment: <input type="text"/></p> <p align="center">Don't apply the blocking rules if the buyer's IP address is in the IP addresses whitelist.</p> <p align="center"><input type="button" value="Submit"/></p>				Delete	Trusted IP addresses	Payid	Date	Encoded By	Comment	<input type="checkbox"/> Sel. All	1.12.1.123		24/09/2008	GFR2oec/GFR2oec/PSPID	...
Delete	Trusted IP addresses	Payid	Date	Encoded By	Comment										
<input type="checkbox"/> Sel. All	1.12.1.123		24/09/2008	GFR2oec/GFR2oec/PSPID	...										

## 5 Dispute

L'acceptation de transaction, quel que soit l'environnement, implique des risques inhérents, comme celui de rejet de débit. Lors du traitement dans un environnement CNP (Carte non présente), les risques de rejet de débit sont toujours présents.

Ingenico ePayments permet aux clients d'accéder à une page de litige, permettant aux marchands d'ajouter des données de transaction à des listes noires et blanches, avec la raison du litige. Les marchands sont ainsi protégés de nouvelles fraudes et de torts répétés. La base de données Ingenico ePayments Fraud Expert est ainsi améliorée et ses performances sont accrues.

### IMPORTANT

Ne sélectionnez Actual fraud (Fraude effective) que si vous recevez un rejet de débit avec un code de motif de fraude.

<b>Ref.: 722004653</b>			
<b>Order reference: order_123</b>			
<b>Total charge: 84 EUR</b>			
<b>Status: 9</b>			
<b>Order date : 2013-06-06 11:53:31</b>			
Data	Value	Comment	Add to the blacklist
Card/Account number	670397-XXXXXXXX-09		<input type="checkbox"/>
IP address	84.193.187.225		<input type="checkbox"/>
			<input checked="" type="radio"/> Commercial dispute <input type="radio"/> Actual fraud
			<b>DISPUTE</b>

### 5.1 Ajouter des données de transaction à une liste noire et blanche

1. Cliquez sur PAYID dans l'aperçu des transactions afin de rechercher les transactions que vous souhaitez dénoncer comme différends commerciaux, fraudes effectives ou suspicions de fraude.

**Currencies**

Selected currencies	
<input type="checkbox"/>	British Pound
<input type="checkbox"/>	EURO
<input type="checkbox"/>	US Dollar

REMOVE SELECTED ITEMS

EURO  
British Pound  
US Dollar

ADD SELECTED ITEMS

SELECT ALL

**Country**  
The country filter will apply only to the e-commerce interface and if the country code (ISO) is transmitted in the hidden field "ownercy". This country can be changed by the buyer.

Selected countries	
<input type="checkbox"/>	AUSTRIA
<input type="checkbox"/>	BELGIUM
<input type="checkbox"/>	FRANCE
<input type="checkbox"/>	GERMANY
<input type="checkbox"/>	NETHERLANDS
<input type="checkbox"/>	UNITED KINGDOM
<input type="checkbox"/>	UNITED STATES OF AMERICA

REMOVE SELECTED ITEMS

AFGHANISTAN (AF)  
Åland Islands (AX)  
ALBANIA (AL)  
ALGERIA (DZ)

ADD SELECTED ITEMS

SELECT ALL

2. Cliquez sur le bouton DISPUTE (litige) afin de répertorier les données reçues pour la transaction qui peuvent être ajoutées à la liste noire et blanche.

3. Accédez à la page des litiges et choisissez la liste à laquelle vous souhaitez ajouter les données de transaction (liste noire ou liste blanche). Sélectionnez ensuite le motif du litige.

Vous pouvez marquer la transaction comme suit :

- Les litiges commerciaux couvrent entièrement les rejets de débit reçus par le marchand et qui ne sont pas liés à des fraudes.
- La fraude effective est un refus de débit frauduleux.
- La suspicion de fraude a pour but d'empêcher une transaction frauduleuse.

La sélection d'un ou plusieurs boutons impacte différemment la base de données des fraudes.

Remarque : La fraude effective ne s'applique qu'au rejet de débit frauduleux.

**Currencies**

Selected currencies	
<input type="checkbox"/>	British Pound
<input type="checkbox"/>	EURO
<input type="checkbox"/>	US Dollar

REMOVE SELECTED ITEMS

EURO  
British Pound  
US Dollar

ADD SELECTED ITEMS

SELECT ALL

**Country**  
The country filter will apply only to the e-commerce interface and if the country code (ISO) is transmitted in the hidden field "ownercy". This country can be changed by the buyer.

Selected countries	
<input type="checkbox"/>	AUSTRIA
<input type="checkbox"/>	BELGIUM
<input type="checkbox"/>	FRANCE
<input type="checkbox"/>	GERMANY
<input type="checkbox"/>	NETHERLANDS
<input type="checkbox"/>	UNITED KINGDOM
<input type="checkbox"/>	UNITED STATES OF AMERICA

REMOVE SELECTED ITEMS

AFGHANISTAN (AF)  
Åland Islands (AX)  
ALBANIA (AL)  
ALGERIA (DZ)

ADD SELECTED ITEMS

SELECT ALL

4. Sauvegardez et confirmez l'ajout des données à la liste appropriée. La vérification de fraude prend immédiatement effet.

**Currencies**

Selected currencies	
<input type="checkbox"/>	British Pound
<input type="checkbox"/>	EURO
<input type="checkbox"/>	US Dollar

REMOVE SELECTED ITEMS

EURO  
British Pound  
US Dollar

ADD SELECTED ITEMS

SELECT ALL

**Country**  
The country filter will apply only to the e-commerce interface and if the country code (ISO) is transmitted in the hidden field "ownership". This country can be changed by the buyer.

Selected countries	
<input type="checkbox"/>	AUSTRIA
<input type="checkbox"/>	BELGIUM
<input type="checkbox"/>	FRANCE
<input type="checkbox"/>	GERMANY
<input type="checkbox"/>	NETHERLANDS
<input type="checkbox"/>	UNITED KINGDOM
<input type="checkbox"/>	UNITED STATES OF AMERICA

REMOVE SELECTED ITEMS

AFGHANISTAN (AF)  
Åland Islands (AX)  
ALBANIA (AL)  
ALGERIA (DZ)

ADD SELECTED ITEMS

SELECT ALL

À partir de la page des litiges, vous pouvez également sélectionner les données (appartenant à votre Centre d'appel, VIP client, etc.) à ajouter à la liste blanche. Si vous sélectionnez des données préalablement incluses dans la liste noire, ces dernières seront automatiquement ajoutées à la liste blanche. La vérification de fraude prend immédiatement effet.

## 6 Retour sur le Module de Détection de Fraude


### 6.1 Aperçu des transactions dans le module de gestion


#### 6.1.1 Critères de sélection avancés

Lorsque vous cherchez une transaction via le lien « Gestion transactions » ou « Historique financier » dans le menu de votre compte, vous aurez un choix de plus dans le « Critère de sélection avancé » : l'adresse IP. Vous pouvez utiliser le champ de l'adresse IP pour chercher toutes les transactions qui proviennent de la même adresse IP ou qui proviennent d'adresses IP commençant par les mêmes chiffres.


#### 6.1.2 3-D Secure dans la liste des transactions

Lorsque vous affichez votre liste de transactions via « Gestion transactions » ou « Historique financier » dans le module de gestion, vous remarquerez des points et des demi-points de couleur verte dans votre liste (si vous avez activé le 3-D Secure dans votre compte).

Le point complet , là où le pouce est levé, représente une transaction 3-D Secure où le client a payé avec une carte de crédit inscrite au 3-D Secure. Avec ces transactions, votre acquéreur vous propose la garantie de paiement conditionnelle (voir la Section 2.1.2).

Le demi-point  représente une transaction 3-D Secure où le client a payé avec une carte de crédit non-inscrite au 3-D Secure. Ces transactions supposent un certain niveau de garantie de paiement conditionnelle (voir la Section 2.1.2), basée sur les renseignements spécifiques du contrat de 3-D Secure avec l'acquéreur.

Les transactions qui ne possèdent pas de (demi) point sont des transactions qui n'ont pas été traitées sous l'utilisation du 3-D Secure. La garantie de paiement conditionnelle (voir la Section 2.1.2) ne sera pas appliquée pour ces transactions.

Les transactions qui possèdent un point d'exclamation  indiquent des transactions où l'identification du client a échoué. La garantie de paiement conditionnelle (voir la Section 2.1.2) ne sera pas applicable pour les transactions que vous avez décidées de poursuivre (*continuer*) mais dont l'identification a échoué (pour MasterCard, voir la Section 2.2.3).

#### 6.1.3 Renseignements concernant la transaction

Dans les données fournies lors de la transaction (Page financière), vous verrez des informations supplémentaires tel que le résultat du code de vérification de la carte (si le code CVC a été entré par le client), le pays de la carte, le pays de l'adresse IP ainsi que l'adresse IP.



Le bouton « Dispute », se trouvant en haut du tableau avec les informations supplémentaires, vous amènera à une page où vous pourrez ajouter certains renseignements d'une transaction dans vos listes noires à l'aide d'un simple clic. Cette option vous permet d'ajouter à votre liste noire le numéro de la carte utilisée pour la transaction sans avoir à connaître le numéro complet de la carte, par exemple.

Vous pouvez aussi marquer la transaction comme étant un Différend commercial ou une fraude.

**IMPORTANT**  
 Sélectionner « Fraude avérée» seulement si le client a réellement commis une fraude avec sa carte, par exemple, lorsque que le titulaire utilise une carte qui ne lui appartient pas.

**Ref.:** 722004653  
**Order reference:** order\_123  
**Total charge:** 84 EUR  
**Status:** 9  
**Order date :** 2013-06-06 11:53:31

Data	Value	Comment	Add to the blacklist
Card/Account number	670397-XXXXXXXX-09		<input type="checkbox"/>
IP address	84.193.187.225		<input type="checkbox"/>
			<input checked="" type="radio"/> Commercial dispute <input type="radio"/> Actual fraud
			<div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">DISPUTE</div>

### 6.1.4 Codes erreurs

Lorsqu'une transaction a été retenue par notre système selon les règles que vous avez fixées dans le module de détection de fraude, vous trouverez la raison dans le message d'erreur de la transaction. À quelques exceptions près, tous les codes d'erreur liés au module de détection de fraude commencent par 300011, suivi de deux autres chiffres. L'ensemble de ces codes d'erreur peuvent être trouvés dans la liste [La signification des statuts des paiements et des codes d'erreur éventuels](#).

La liste incomplète suivante contient les exemples des raisons les plus pertinentes :

- 3 / 30001100 Pays de l'acheteur non-autorisé
- 3 / 30001120 Adresse IP dans la liste noire du marchand
- 3 / 30001130 BIN dans la liste noire du marchand
- 3 / 30001140 Numéro de carte dans la liste noire du marchand

## 6.2 Paramètres de transaction supplémentaires

Dans vos requêtes post sale, vos redirections avec feedback, vos téléchargements de fichiers et vos réponses XML DirectLink des paramètres supplémentaires relatifs au module de détection de fraude seront renvoyés.

La liste des paramètres supplémentaires est fixée ci-dessous.

Ces champs seront vides si une erreur de validation de format se produit lorsque les détails de la transaction sont fournis.

Paramètre	Valeur
IPCTY	Pays d'origine de l'adresse IP.  Format: 2 caractères alphabétiques de code ISO. Si ce paramètre n'est pas disponible, « 99 » sera reporté dans la réponse.  Cette adresse IP est basée sur des listes IP fournies extérieurement, donc il existe tout de

Paramètre	Valeur
	même un léger risque puisque nous dépendons de l'exactitude de cette liste. Dans tous les cas, cette vérification donne des résultats positifs à 94%.
CCCTY	<p>Pays d'origine de la carte de crédit.</p> <p>Disponible seulement pour VISA, MasterCard, American Express et Diners Club. Cette valeur sera vide pour toutes les autres méthodes de paiement/brands. Format: 2 caractères alphabétiques de code ISO. Si ce paramètre n'est pas disponible, « 99 » sera reporté dans la réponse.</p> <p>Cette adresse IP est basée sur des listes IP fournies extérieurement, donc il existe tout de même un léger risque puisque nous dépendons de l'exactitude de cette liste. Dans tous les cas, cette vérification donne des résultats positifs à 94%.</p>
ECI	<p>Indicateur de commerce électronique (ECI). Les valeurs possibles pour l'ECI ainsi que leur signification sont fixées ci-dessous :</p> <ul style="list-style-type: none"> <li>1 Vente à distance classique (MOTO)</li> <li>2 Paiements périodiques provenant de VAD</li> <li>3 Paiements étalés</li> <li>5 Identification du titulaire de la carte réussie</li> <li>6 Identification supporté par le marchand mais pas par le titulaire de la carte, les règles de la garantie de paiement conditionnelle s'appliquent (voir la Section 2.1.2)</li> <li>7 E-commerce avec encryption SSL</li> <li>9 Paiements périodiques provenant de commerce électronique</li> <li>12 Identification supporté par le marchand mais pas par le titulaire de la carte, les règles de la garantie de paiement conditionnelle s'appliquent (voir la Section 2.1.2) (idem 6)</li> <li>91 L'identification du titulaire de la carte A ÉCHOUÉ !!!! (garantie de paiement conditionnelle (voir la Section 2.1.2) peut être appliquée, vérifiez avec votre acquéreur)</li> <li>92 Site d'identification de la banque émettrice temporairement indisponible, mais la transaction a été poursuivie</li> </ul>
CVCCheck	<p>Résultat de la vérification de la carte. Valeurs possibles :</p> <p>KO: Le CVC a été envoyé mais l'acquéreur a fourni une réponse négative à la vérification CVC, c'est-à-dire que le CVC est incorrect.</p> <p>OK:</p> <ul style="list-style-type: none"> <li>1. Le CVC a été envoyé et l'acquéreur a fourni une réponse positive à la vérification CVC, c'est-à-dire que le CVC est correct. OU</li> <li>2. L'acquéreur a fourni un code d'autorisation, mais il n'a pas renvoyé le résultat spécifique pour la vérification CVC.</li> </ul>



Paramètre	Valeur
	NO: Tous les autres cas. Par exemple, si aucun CVC n'est transmis et que l'acquéreur a répondu qu'une vérification CVC était impossible, l'acquéreur refuse l'autorisation mais ne propose pas un résultat spécifique pour la vérification CVC, ...
AAVCheck	Résultat de la vérification automatique d'une adresse. Actuellement, cette vérification est seulement disponible pour la carte American Express. Valeurs possibles : KO: L'adresse a été envoyée mais l'acquéreur a fourni une réponse négative à la vérification de l'adresse, c'est-à-dire que l'adresse est incorrecte. OK: 1. L'adresse a été envoyée et l'acquéreur a fourni une réponse positive à la vérification de l'adresse, c'est-à-dire que l'adresse est correcte. OU 2. L'acquéreur a fourni un code d'autorisation, mais il n'a pas renvoyé le résultat spécifique pour la vérification de l'adresse. NO: Tous les autres cas. Par exemple, si aucune adresse n'est transmise et que l'acquéreur a répondu qu'une vérification de l'adresse était impossible, l'acquéreur refuse l'autorisation mais ne propose pas un résultat spécifique pour la vérification de l'adresse, ...
VC	Carte virtuelle. Valeurs possibles : ECB: Pour E Carte Bleue ICN: Pour Internet City Number NO: Tous les autres cas. Par exemple, la carte n'est pas une carte virtuelle, la carte est un type de carte virtuelle que nous ne connaissons pas, ...
IP	L'adresse IP du client telle que détectée par notre système dans une intégration 3-tiers ou qui nous a été envoyée par le marchand dans une intégration 2-tiers.

## 7 Annexe: CVC2 et AAV

### 7.1 CVC2

CVC2 est une procédure de vérification établie par les compagnies de cartes de crédit afin de faciliter la prévention des cartes de crédit frauduleuses utilisées pour les transactions Internet. En fonction du brand, ce code peut porter différents noms (CVC2 ou Card Validation Code pour MasterCard, CVV2 ou Card Verification Value pour VISA, CID ou Card Identification Number pour American Express). Cependant, le code mentionné est généralement « CVC ». La fonctionnalité du CVC2 est la même pour tous les brands.

Le code de vérification est uniquement lié au numéro de la carte, mais il ne fait pas partie du numéro de la carte. En fonction du brand de la carte, le code de vérification sera un code de 3 ou 4 chiffres sur le recto ou le verso de la carte, un nombre émis, une date d'émission ou une date de naissance. Pour MasterCard et VISA par exemple, un code de 3 chiffres est présenté sur le verso de la carte dans la bande de la signature, après le numéro de compte complet du client ou les 4 derniers chiffres du numéro de compte du client.

Il est strictement interdit pour les marchands et les PSP (Payment Solution Provider) d'entrer le code CVC2 de leurs clients dans une base de données. Lorsque le titulaire de la carte n'est pas présent, c'est-à-dire pour les transactions dont « la carte n'est pas présente », et qu'il lui est demandé d'entrer son code CVC2 avec son numéro de carte, ce code de vérification aide à s'assurer que le client qui place la commande a bien sa carte en main et que le compte de cette carte est légitime.

### 7.2 AAV

AAV est une procédure de vérification disponible dans certains marchés pour faciliter la prévention des cartes de crédit frauduleuses utilisées pour les transactions Internet. En fonction du brand, ce code peut porter différents noms : (AVS ou Address Verification Service/System pour VISA/MasterCard ; AAV ou Automated Address Verification pour American Express) Cependant, la fonctionnalité du AAV est la même pour tous les brands.

La vérification d'une adresse débute lorsque l'acquéreur demande à l'émetteur d'une carte de comparer les composantes numériques (numéro de maison et code postal) de l'adresse (de facturation ou d'envoi) d'un client que le marchand nous a envoyée avec celles de l'adresse de facturation que le client a donné à l'émetteur lors de l'enregistrement de la carte. American Express exécute cette vérification automatiquement lorsqu'elle reçoit les détails de l'adresse avec une transaction ; pour les autres brands, cela dépend de l'acquéreur. Quel que soit le cas, nous recommandons que les détails de l'adresse du client soient envoyés avec les données de la commande faites à notre système.

Bien qu'une transaction ne soit pas refusée en raison du résultat de la vérification de l'adresse, le marchand peut utiliser ce résultat pour décider s'il livre la marchandise ou s'il demande au client des informations supplémentaires avant expédition.

Remarque: Les simulations des vérifications AAV/AVS ne fonctionnent pas comme prévu en environnement de test.