# Module de Détection de Fraude Avancé - Checklist

Guide de Configuration pour le Module de Détection de Fraude Avancé - Checklist v.4.4.7

# Table of Contents

# 1 Qu'est-ce que le module de détection des fraudes ?

Contrairement au module de détection des fraudes de base, le module de détection des fraudes avancé permet au marchand de configurer le comportement effectif des listes noires, grises et blanches, ainsi que les règles et les limites dans la liste « Risk Evaluation (Évaluation du risque) ».

## 1.1 Avantages

Le module de détection des fraudes vous permet de réaliser les opérations suivantes :

- Détecter les anomalies en temps réel avant la finalisation de la commande
- Bloquer immédiatement les tentatives des fraudeurs identifiés
- Marquer des risques spécifiques en vue d'un examen
- Prévenir les risques associés à certains pays
- Définir et appliquer des politiques de sécurité entièrement personnalisées
- Bénéficier d'une garantie de paiement conditionnelle (voir ici) conformément aux règles de votre acquéreur (3-D Secure)

## 1.2 Accès

Vous pouvez accéder le module de détection des fraudes par le lien "Fraud detection" dans le menu "Avancé" de votre compte Ingenico ePayments.

## 1.3 Contenu

Le module de détection des fraudes comprend trois espaces fonctionnels distincts :

- Activation et configuration de la détection des fraudes
- 3-D Secure
- Listes noires, grises et blanches

IMPORTANT

Les critères VISA/MasterCard décrits dans cette documentation ne sont pas nécessairement disponibles pour tous les moyens de paiement.

La disponibilité de la configuration des critères dépend du moyen de paiement. Pour certains de ces moyens, la configuration est limitée.

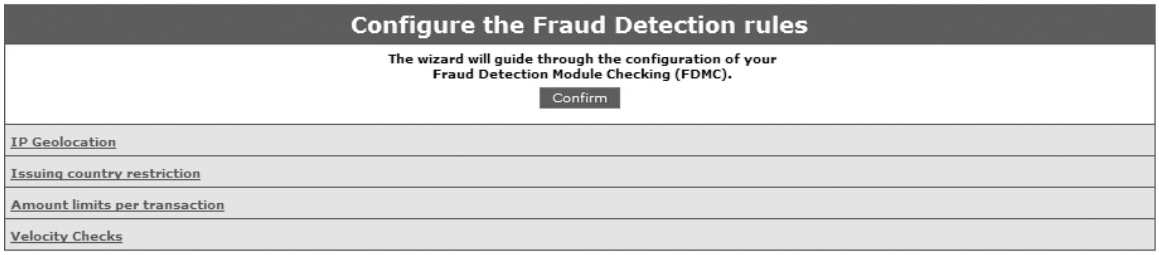
Nous vous recommandons de vérifier la configuration spécifique de vos moyens de paiement en cliquant sur le bouton « Edit (Modifier) » en regard des différents moyens de paiement dans la table « Fraud detection activation and configuration (Activation et configuration de la détection des fraudes) » dans l'écran de configuration de la détection des fraudes.

# 2 Assistant de configuration

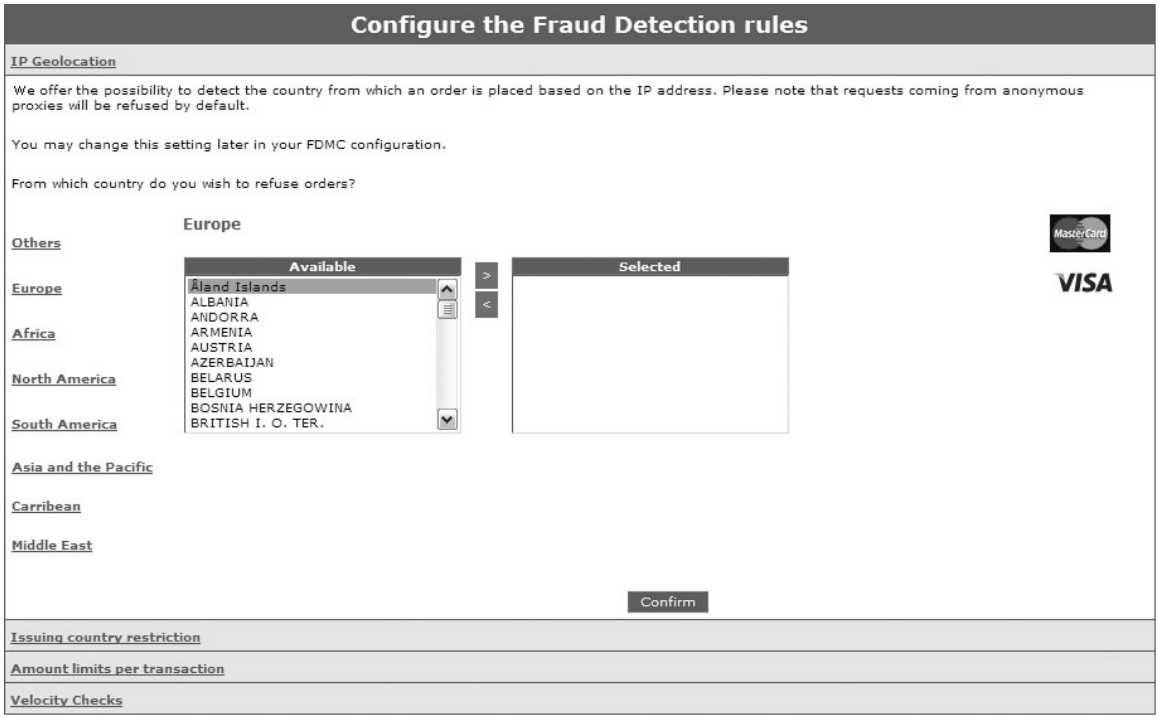
Si le module de détection des fraudes n'est pas encore configuré, le lien « Configure the Fraud Detection rules (Configurer les règles de détection des fraudes) » est visible dans la page d'accueil du marchand.

Un clic sur ce lien permet d'accéder à un assistant de configuration qui vous guide pas à pas à travers la configuration de l'évaluation du risque. Cliquez sur « Confirm (Confirmer) » pour lancer l'assistant.

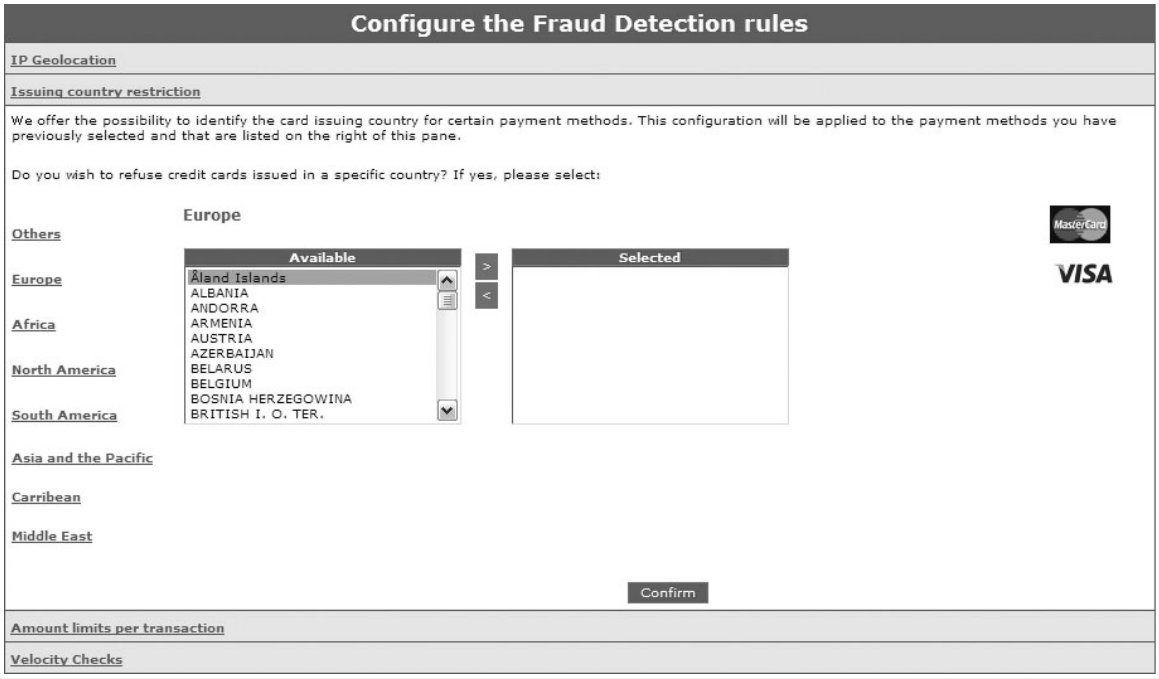
Accueil



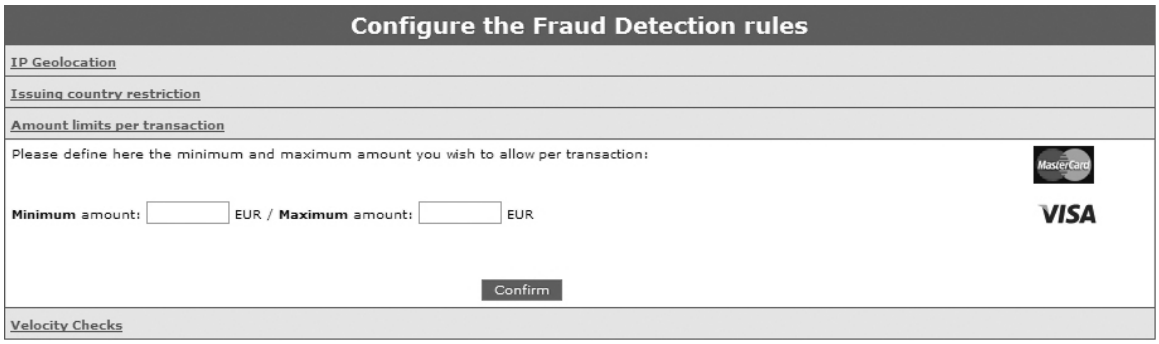

Étape 1 : Géolocalisation de l'adresse IP



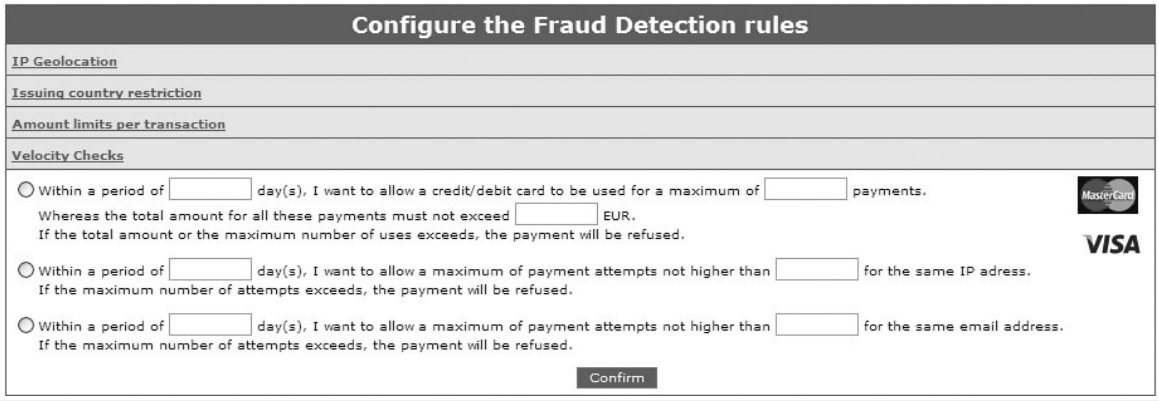

Étape 2 : Restrictions en fonction du pays de la carte



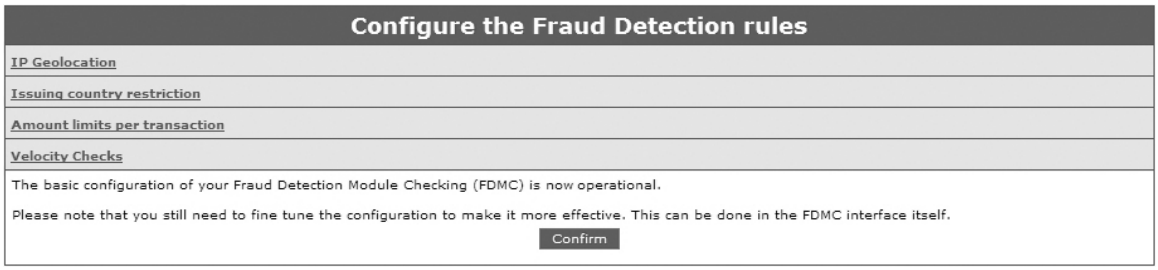

Étape 3 : Limitation du montant par transaction




Étape 4 : Contrôles de vélocité




Terminé !



# 3 Activation et configuration de la détection des fraudes

La table « Activation et configuration de la détection des fraudes » permet de faire la distinction entre les cartes de crédit et les autres moyens de paiement. Cette section se concentre plus particulièrement sur la configuration des options de détection des fraudes pour les cartes de crédit.

Pour configurer les options de détection des fraudes pour une carte de crédit spécifique, cliquez sur le bouton « Editer » en regard du moyen de paiement. Vous pouvez ensuite accéder à la page d'évaluation du risque pour ce moyen de paiement, qui présente des liens vers les pages de configuration des différentes règles, limites et listes.

Le comportement effectif de ces règles (à savoir si elles conduisent ou non à bloquer les transactions) dépend des paramètres que vous définissez dans la page « Risk Evaluation (Évaluation du risque) ».

## 3.1 Groupes de pays de carte

Par défaut, tous les pays d'origine des cartes sont acceptés. Le terme « pays émetteur de cartes » désigne le pays où la carte a été émise. Notre système peut identifier le pays émetteur de cartes sur la base du code BIN de la carte. Le code BIN correspond aux 6 premiers chiffres d'un numéro de carte de crédit. Il est lié à la banque et au pays d'origine de la carte.

Vous pouvez définir un risque déterminé par pays émetteur de cartes. Vous pouvez classer un pays émetteur de cartes selon trois catégories :

- Risque élevé
- Risque moyen
- Risque faible

Les pays émetteurs de cartes à risque élevé peuvent entraîner le blocage des transactions ou l'augmentation de l'évaluation du risque. Les pays émetteurs de cartes à risque moyen peuvent augmenter l'évaluation du risque. Les pays émetteurs de cartes à risque faible ne sont pas pris en considération dans l'évaluation.

Remarque

- Disponible uniquement pour les cartes VISA, MasterCard, American Express et Diners Club

## 3.2 Groupes de pays d'adresse IP

Par défaut, tous les pays d'origine des adresses IP sont acceptés. Notre système peut identifier le pays de l'adresse IP sur la base de l'adresse IP de votre client. (Ce contrôle donne des résultats positifs dans 94 % des cas ; un léger risque d'erreur ne peut être totalement exclu car il se base sur des listes d'adresses IP d'origine extérieure.)

Comme dans le cas des pays des cartes, vous pouvez définir un risque déterminé par pays IP. Vous pouvez classer un pays IP selon trois catégories :

- Risque élevé
- Risque moyen
- Risque faible

Les pays IP à risque élevé peuvent entraîner le blocage des transactions ou l'augmentation de l'évaluation du risque. Les pays IP à risque moyen peuvent augmenter l'évaluation du risque. Les pays IP à risque faible ne sont pas pris en considération dans l'évaluation.

À côté de ces pays IP, il existe également ce que l'on appelle des serveurs proxy anonymes. Les serveurs proxy anonymes sont des fournisseurs d'accès internet qui autorisent les utilisateurs web à masquer leur adresse IP. Nous vous recommandons de bloquer les transactions provenant de serveurs proxy

anonymes dans la page d'évaluation du risque.

IMPORTANT

« Asia Pacific Network (Réseau Asie-Pacifique) », « European Network (Réseau européen) » et « Satellite Provider (Fournisseur satellite) » se rapportent à des adresses IP dont le pays d'origine est incertain.

« European Network (Réseau européen) », par exemple, signifie que le pays IP exact n'est pas déterminé avec certitude, mais qu'il fait bien partie de l'Europe. Accepter « European network (Réseau européen) » comme pays d'adresse IP n'implique pas que vous acceptez les paiements de tous les pays d'Europe, mais que vous acceptez les paiements en provenance d'adresses IP gérées par des établissements européens (p. ex. un fournisseur d'accès internet actif dans plusieurs pays européens, la Commission européenne, etc.).

La plupart du temps, le pays de l'adresse IP est identique au pays de l'adresse de livraison. Les régions et pays de livraison généralement considérés comme risqués chez les acquéreurs sont l'Europe de l'est, l'Asie, l'Indonésie, l'Afrique et les Etats Unis. Cependant, si vous vendez régulièrement dans ces régions ou pays, ou si vous avez mis en place des procédures de livraison ou de commande spécifiques afin de vérifier l'identité de vos clients, vous ne devez pas définir un niveau de risque élevé pour ces régions ou pays.

## 3.3 Combinaisons risquées de pays IP et pays émetteurs de cartes

Par défaut, toutes les combinaisons pays IP et pays émetteur de cartes sont acceptées.

Pour configurer une combinaison pays IP et pays émetteur de cartes, sélectionnez un pays IP et un pays émetteur de cartes à combiner dans les listes déroulantes.

De la même façon que pour les pays émetteurs de cartes et les pays IP, vous pouvez définir un risque déterminé par combinaison pays IP et pays émetteur de cartes. Vous pouvez classer une combinaison pays IP et pays émetteur de cartes selon trois catégories :

- Risque élevé
- Risque moyen
- Risque faible

Les combinaisons à risque élevé peuvent entraîner le blocage des transactions ou l'élévation de l'évaluation du risque. Les combinaisons à risque moyen peuvent augmenter l'évaluation du risque. Les combinaisons à risque faible ne sont pas prises en considération dans l'évaluation.

Remarque

- Disponible uniquement pour les cartes VISA, MasterCard, American Express et Diners Club

## 3.4 Limite de montant

Vous pouvez limiter le montant par transaction en saisissant un montant minimal et maximal. La devise de la limite doit correspondre à la devise principale de votre compte. Si vous gérez plusieurs devises et qu'une transaction est réalisée dans une autre devise que celle qui est définie par défaut, notre système convertit la limite dans cette autre devise.

## 3.5 Limites d'utilisation

### 3.5.1 Utilisation de la carte

Vous pouvez définir l'utilisation maximale par carte et par période sur la base du montant total des transactions par carte et du nombre de transactions par carte.

Vous devez configurer cette limite en fonction de vos activités et de vos produits. Ainsi, si vous vendez un produit qu'une personne n'achète pas plus d'une fois par semaine, vous pouvez limiter l'utilisation de la carte à une fois par semaine.

*Exemple*

Si vous ne souhaitez pas accepter plus de deux transactions le même jour pour une certaine carte de crédit ou si vous ne souhaitez pas accepter un montant de plus de 250 EUR pour cette carte le même jour, vous pouvez procéder à la configuration suivante :

- *Utilisation maximale par carte et par période 1 jour(s)*
- *Montant total des transactions par carte, seuil haut : 250 EUR*
- *Nombre de transactions par carte, seuil haut : 2*

Vous pouvez également mettre à profit cette règle pour définir un seuil bas et un seuil haut pour marquer une transaction en vue d'un examen (seuil bas) ou la bloquer complètement (seuil haut).

La limite « Maximum utilisation per card, per period (Utilisation maximale par carte et par période) » s'applique uniquement aux cartes qui ont été utilisées dans le cadre de transactions qui ont entraîné les statuts suivants : 9, 91, 92, 5, 51, 52.

### 3.5.2 Utilisation de l'adresse IP

Vous pouvez définir la limite « Maximum utilisation per IP address, per period (Utilisation maximale par adresse IP et par période) » sur la base du nombre de transactions qui se sont déroulées correctement par adresse IP et du nombre total de transactions (acceptées et rejetées) par adresse IP.

Les fraudeurs utilisent souvent une liste de cartes de crédit volées qu'ils essaient l'une après l'autre. En conséquence, plusieurs transactions impliquant différentes cartes proviennent de la même adresse IP. Pour détecter un tel agissement, vous pouvez limiter le nombre de transactions (acceptées et rejetées) par adresse IP. Si une utilisation abusive vous est signalée, il est également important de se reporter à l'historique de l'adresse IP. De cette façon, vous pouvez arrêter la livraison de vos marchandises si vous observez un trop grand nombre de transactions transitant par la même adresse IP avec différentes cartes au sein d'une période de temps définie.

*Exemple*

Si vous ne souhaitez pas accepter plus d'une transaction provenant de la même adresse IP dans les 3 jours et que vous ne souhaitez pas accepter plus de 3 tentatives sur cette adresse IP au sein de cette période, vous pouvez réaliser la configuration suivante :

- *Utilisation maximale par adresse IP et par période 3 jour(s)*
- *Nombre de transactions réussies par adresse IP, seuil haut : 1*

*Nombre de transactions (acceptées ou rejetées) par adresse IP, seuil haut : 3*

Vous pouvez également mettre à profit cette règle pour définir un seuil bas et un seuil haut pour marquer une transaction en vue d'un examen (seuil bas) ou la bloquer complètement (seuil haut).

« Maximum utilisation per email address, per period limit » s'applique uniquement aux adresses IP utilisées dans le cadre de transactions qui ont entraîné les statuts suivants :

- Transactions réussies : 9, 91, 92, 5, 50, 51, 52
- Toutes les autres transactions : 9, 91, 92, 5, 50, 51, 52, 2

### 3.5.3 Utilisation de l'adresse électronique

Vous pouvez définir la limite d'utilisation maximale par adresse électronique et par période (« Maximum utilisation per e-mail address, per period »). Vous déterminez ainsi le nombre maximal de fois qu'une adresse électronique donnée peut être utilisée au cours d'une période définie.

Vous pouvez également mettre à profit cette règle pour définir un seuil bas et un seuil haut pour marquer une transaction en vue d'un examen (seuil bas) ou la bloquer complètement (seuil haut).

La limite « Maximum utilisation per e-mail address, per period (Utilisation maximale par adresse électronique et par période) » s'applique aux transactions de tous statuts.

« Maximum utilisation per email address, per period limit » s'applique uniquement aux adresses e-mail utilisées dans le cadre de transactions qui ont entraîné les statuts suivants : 9, 91, 92, 5, 50, 51, 52, 2.

# 3.6 Données risquées

## 3.6.1 Codes postaux et adresses risqués

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des codes postaux et adresses risqués s'applique à tous les moyens de paiement. Sont incluses les adresses de facturation et de livraison.

Vous pouvez définir un risque déterminé par code postal / adresse. Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les codes postaux/adresses à risque élevé peuvent entraîner le blocage des transactions ou l'élévation de la notation. Les codes postaux/adresses à risque moyen peuvent augmenter la notation. Les codes postaux/adresses à risque faible ne sont pas pris en considération dans la notation.

Pour configurer votre liste, sélectionnez le pays, saisissez le code postal et la rue, cliquez sur le bouton « Ajouter » et définissez le risque. Pour terminer, cliquez sur le bouton « Envoyer ». Afin d'évaluer la règle, le code pays devra lui aussi être inclus.

Pour utiliser cette fonctionnalité, assurez-vous d'envoyer les paramètres suivants pour les adresses de facturation et de livraison, avec les valeurs associées dans la demande de commande issue de votre site Web.

### Adresse de facturation

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| OWNERCTY | AN (2) | Pays du client | UK |
| OWNERZIP | AN (10) | Code postal du client | 75420 |
| OWNERADRESSE | AN (35) | Adresse du client, première ligne | Rue Baker 221B |
| OWNERADRESSE2 | AN (35) | Adresse du client, deuxième ligne | 2ème étage |

ou

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ECOM_BILLTO_POSTAL_COUNTRYCODE | AN (2) | Pays de facturation | UK |

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ECOM_BILLTO_POSTAL_POSTALCODE | AN (10) | Code postal - adresse de facturation | 75420 |
| ECOM_BILLTO_POSTAL_STREET_LINE1 | AN (35) | Adresse de facturation, première ligne | Rue Baker 221B |
| ECOM_BILLTO_POSTAL_STREET_LINE2 | AN (35) | Adresse de facturation, deuxième ligne | 2ème étage |

Adresse de livraison

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ECOM_SHIPTO_POSTAL_COUNTRYCODE | AN (2) | Code du pays de livraison | UK |
| ECOM_SHIPTO_POSTAL_POSTALCODE | AN (10) | Code postal - adresse de livraison | 75420 |
| ECOM_SHIPTO_POSTAL_STREET_LINE1 | AN (35) | Adresse de livraison, première ligne | Rue Baker 221B |
| ECOM_SHIPTO_POSTAL_STREET_LINE2 | AN (35) | Adresse du client, deuxième ligne | 2ème étage |

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

### 3.6.2 Périodes risquées (dates et heures de commande)

IMPORTANT

- Vous ne devez configurer cette page qu'une seule fois. La configuration des périodes risquées s'applique à tous les moyens de paiement.
- Le fuseau horaire utilisé est l'heure d'Europe centrale CET !

Vous pouvez définir un risque déterminé par période de commande. Il existe trois catégories possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les périodes à risque élevé peuvent entraîner le blocage des transactions ou l'élévation de l'évaluation du risque. Les périodes à risque moyen peuvent augmenter l'évaluation du risque. Les périodes à risque faible ne sont pas prises en considération dans l'évaluation.

Pour configurer la table, sélectionnez le risque au bas de celle-ci, cochez les cases des lignes auxquelles affecter ce risque et cliquez sur le bouton « Apply (Appliquer) ».

## 3.6.3 Modes d'expédition risqués

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des modes de livraison risqués s'applique à tous les moyens de paiement.

Vous pouvez définir un risque déterminé par mode de livraison. Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les modes de livraison à risque élevé peuvent entraîner le blocage des transactions ou l'augmentation de l'évaluation du risque. Les modes de livraison à risque moyen peuvent augmenter l'évaluation du risque. Les modes de livraison à risque faible ne sont pas pris en considération dans l'évaluation.

Pour configurer votre liste, saisissez le mode d'expédition, définissez le risque et cliquez sur le bouton « Add (Ajouter) ». Pour terminer, cliquez sur le bouton « Submit (Soumettre) ».

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ECOM_SHIPMETHODTYPE | Nombre entier 1-9 | Mode de livraison<br>Vous pouvez définir et envoyer une valeur selon le mode d'expédition. | 1 : Enlèvement chez le marchand<br>2 : Point de collecte (bureau de poste, point Kiala, etc.)<br>3 : Collecte dans un aéroport, une gare, une agence de voyage<br>4 : Transporteur (DHL, UPS, etc.)<br>5 : Téléchargement<br>6: Fournisseur à faible coût<br>7: Collecte aux casiers<br>8: militaire<br>9: électronique<br>91: Marchand défini 1<br>92: Marchand défini 2<br>93: Marchand défini 3<br>94: Marchand défini 4<br>95: Marchand défini 5<br>96: Marchand défini 6<br>97: Marchand défini 7<br>98: Marchand défini 8<br>99: Marchand défini 9 |

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

## 3.6.4 Détails des modes d'expédition risqués

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des détails des modes de livraison risqués s'applique à tous les moyens de paiement.

Vous pouvez définir un risque déterminé par entrée. Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen

- Risque faible

Les détails des modes de livraison à risque élevé peuvent entraîner le blocage des transactions ou l'augmentation de la notation. Les détails des modes de livraison à risque moyen peuvent augmenter la notation. Les détails des modes de livraison à risque faible ne sont pas pris en considération dans la notation.

Pour configurer votre liste, sélectionner la valeur Détails du mode d'expédition dans la liste déroulante, définissez le risque et cliquez sur le bouton « Add (Ajouter) ». Pour terminer, cliquez sur le bouton « Submit (Soumettre) ».

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ECOM_SHIPMETHODDETAILS | Texte libre (maximum 50 car.) | Identification du point de collecte | Bureau de poste KR124 |

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

## 3.6.5 Catégories de produits risquées

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des catégories de produits risquées s'applique à tous les moyens de paiement. Les catégories de produits à risque s'appliquent uniquement à e-Commerce et DirectLink.

Vous pouvez définir un risque déterminé par catégorie de produits. Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les catégories de produits à risque élevé peuvent entraîner le blocage des transactions ou l'élévation de la notation. Les catégories de produits à risque moyen peuvent augmenter la notation. Les catégories de produits à risque faible ne sont pas prises en considération dans la notation.

Pour utiliser cette fonctionnalité, envoyez uniquement le paramètre ITEMFDMPRODUCTCATEGx et les valeurs qui lui sont associées.

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ITEMFDMPRODUCTCATEGx | Texte libre (max. 50) | Catégorie de produits | Voyage<br>Aliments<br>Sports |

Remarque:

Remplacez « x » par un nombre pour envoyer plusieurs éléments: ITEMFDMPRODUCTCATEG1, ITEMFDMPRODUCTCATEG2, etc.

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

## 3.6.6 Délais de livraison risqués

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des délais de livraison risqués s'applique à tous les moyens de paiement.

Vous pouvez définir un risque déterminé par délai (nombre d'heures). Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les délais de livraison à risque élevé peuvent entraîner le blocage des transactions ou l'augmentation de la notation. Les délais de livraison à risque moyen peuvent augmenter la notation. Les délais de livraison à risque faible ne sont pas pris en considération dans la notation.

Pour configurer votre liste, saisissez la catégorie de produits, définissez le risque et cliquez sur le bouton « Add (Ajouter) ». Pour terminer, cliquez sur le bouton « Submit (Soumettre) ».

| Paramètre d'entrée lié | Format | Explication | Exemple |
|---|---|---|---|
| ECOM_SHIPMETHODSPEED | Nombre entier | Nombre d'heures à compter pour la livraison | 24 |

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

## 3.6.7 Sous-marques risquées

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des sous-marques risquées s'applique à tous les moyens de paiement.

Vous pouvez définir un risque déterminé par sous-marque. Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les sous-marques à risque élevé peuvent entraîner le blocage des transactions ou l'élévation de la notation. Les sous-marques à risque moyen peuvent augmenter la notation. Les sous-marques à risque faible ne sont pas prises en considération dans la notation.

Pour configurer votre liste, saisissez la sous-marque, définissez le risque et cliquez sur le bouton « Add (Ajouter) ». Pour terminer, cliquez sur le bouton « Submit (Soumettre) ».

## 3.6.8 Numéros d'émetteur risqués

IMPORTANT

Vous ne devez configurer cette page qu'une seule fois. La configuration des numéros d'émetteur risqués s'applique à tous les moyens de paiement.

Vous pouvez définir un risque en fonction de l'identifiant des banques émettrices. Il existe trois niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

Les numéros d'émetteur à risque élevé peuvent entraîner le blocage des transactions ou l'augmentation

de l'évaluation du risque. Les numéros d'émetteur à risque moyen peuvent augmenter l'évaluation du risque. Les numéros d'émetteur à risque faible ne sont pas pris en considération dans l'évaluation.

Pour configurer votre liste, saisissez le numéro d'émetteur, définissez le risque et cliquez sur le bouton « Add (Ajouter) ». Pour terminer, cliquez sur le bouton « Submit (Soumettre) ».

# 3.7 Dupliquer paramètres

En regard de chaque mode de paiement de la vue d'ensemble Fraud detection activation and configuration se trouve le bouton Duplicate. Ce bouton permet de copier les paramètres d'un mode de paiement pour les appliquer à un ou plusieurs autres modes de paiement de la liste. Ainsi, si votre compte comporte plusieurs modes de paiement, vous n'avez pas besoin de créer la même configuration plusieurs fois.

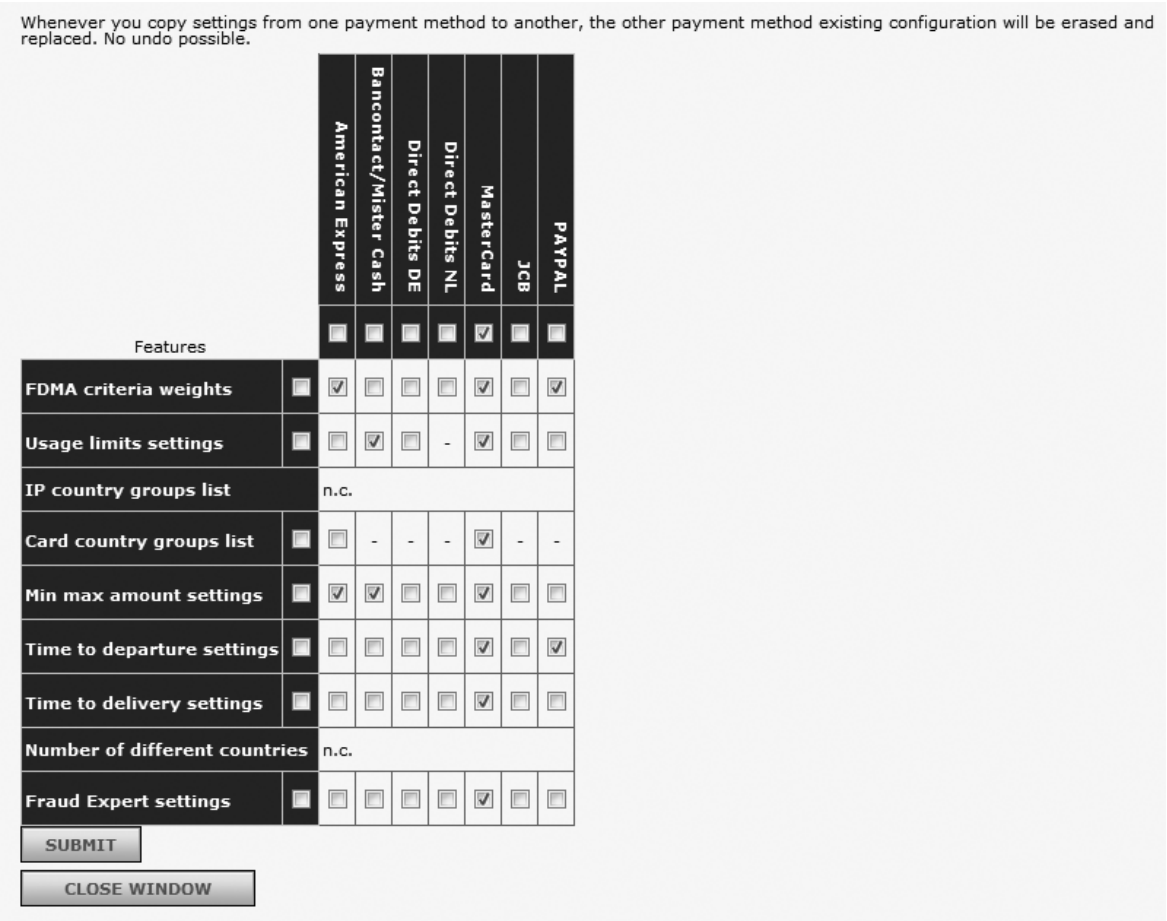
**Important**

Si vous avez déjà configuré le module de détection de fraudes pour un mode de paiement auquel vous souhaitez appliquer les paramètres d'un autre mode de paiement, les paramètres d'origine seront remplacés par les paramètres copiés.

Les paramètres suivants peuvent être copiés, à la condition que le mode de paiement de destination les prenne en charge :

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

*Exemple*



# 4 3-D Secure

La fonctionnalité 3-D Secure offre un niveau supplémentaire de sécurité car elle permet d'identifier les clients sans ambiguïté par des moyens technologiques (mots de passe HTML, Digipass, lecteurs de carte, biométrie, etc.) mis en œuvre par les banques émettrices.

S'il offre 3-D Secure, le marchand bénéficie d'une garantie de paiement conditionnelle (voir ici), décrite dans le contrat 3-D Secure avec son acquéreur. Dans ces conditions, le marchand n'est plus sujet aux litiges qui résulteraient de la « non-identification du titulaire de la carte », où son compte se voit débité d'autorité. (Cela ne l'immunise cependant pas contre les litiges d'un autre ordre.)

Le protocole 3-D Secure est implémenté chez les marques suivantes, au minimum :

- 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

Les règles de blocage et de vérification peuvent être ignorées si les clients sont identifiés via 3-D Secure. Pour en savoir plus sur la fonction Ignorer, voir l'Annexe : Fonction Ignorer.

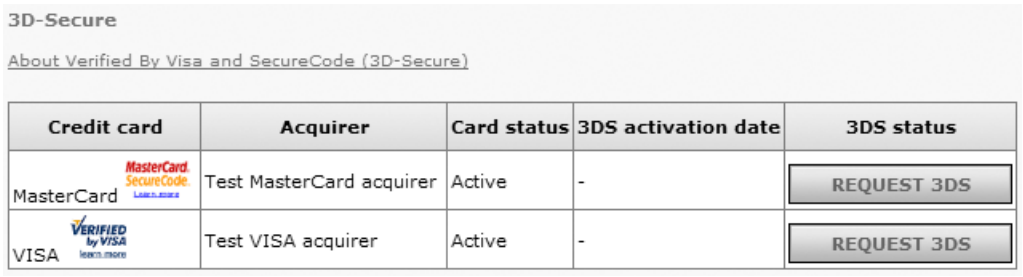
## 4.1 Généralités

### 4.1.1 Demande d'affiliation

Si 3-D Secure n'est pas activé pour votre compte, la table « 3-D Secure » comprend un bouton intitulé « Request 3DS (Demander 3DS) ».

Un clic sur ce bouton « Request 3DS (Demander 3DS) » a pour effet d'envoyer un courriel à votre acquéreur. Si votre contrat avec votre acquéreur ne prévoit rien concernant 3-D Secure, vous pouvez contacter votre acquéreur pour de plus amples informations sur l'inscription au service 3-D Secure si vous souhaitez qu'il propose l'option de paiement 3-D Secure.

Une fois 3-D Secure activé dans votre compte, la table affiche la date d'activation. Vous pouvez modifier la configuration de la fonctionnalité 3-D Secure en cliquant sur le bouton « Edit (Modifier) » en regard des moyens de paiement.




### 4.1.2 Traitement des transactions 3-D Secure standard

1. Lorsque nous recevons les informations de la carte de crédit de votre client, notre système envoie une requête à l'annuaire VISA/MasterCard/JCB pour déterminer si la carte est enregistrée (si le titulaire de la carte bénéficie d'un moyen d'identification quelconque lié à sa carte) et, le cas échéant, obtient les données du serveur d'authentification de l'émetteur.
2. Si la carte est enregistrée, notre système redirige l'acheteur vers le serveur d'authentification de l'émetteur pour lancer l'authentification.
3. Notre système reçoit le résultat de l'authentification et traite le paiement comme habituellement.

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

Si la carte n'est pas enregistrée, le marchand bénéficie d'un certain niveau de garantie de paiement conditionnelle de la part de son acquéreur.

Dans les deux cas, par conséquent, sous certaines conditions (définies par VISA, MasterCard et les établissements financiers, suivant les dispositions du contrat 3-D Secure avec son acquéreur), le marchand bénéficie d'une garantie de paiement, même s'il ne reçoit pas les informations d'identification du client. Les règles de la garantie de paiement conditionnelle sont gérées exclusivement entre le marchand et son acquéreur. Ingenico ePayments agit uniquement à titre d'intermédiaire technique.

## 4.2 Options de configuration

Les sections suivantes présentent les options de configuration des fonctionnalités Verified by Visa, MasterCard SecureCode et J-Secure. Ces options peuvent ne pas être disponibles, car elles dépendent de votre acquéreur.

### 4.2.1 Problème technique

Le marchand peut choisir de *poursuivre* ou d' *interrompre* la transaction si un problème technique empêche la connexion à l'annuaire VISA/MasterCard/JCB au cours du contrôle de l'enregistrement 3-D Secure.

Si un problème technique empêche notre système de se connecter à l'annuaire VISA/MasterCard/JCB (étape 1), VISA/MasterCard/JCB recommande de poursuivre l'opération sans authentification (option*poursuivre* ). En pareil cas, toutefois, le marchand ne bénéficie plus de la garantie de paiement conditionnelle (voir ici).

### 4.2.2 Service d'identification temporairement indisponible

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

Si le serveur d'authentification de l'émetteur est temporairement indisponible (étape 2), l'identification du titulaire de la carte n'est pas possible. Dans cette éventualité, VISA/MasterCard/JCB recommande de continuer l'opération (option*poursuivre* ). En pareil cas, toutefois, le marchand ne bénéficie plus de la garantie de paiement conditionnelle (voir ici).

### 4.2.3 Échec de l'authentification (MasterCard seulement)

Si l'authentification échoue, le marchand peut choisir de *poursuivre* ou d' *interrompre* la transaction.

En cas d'échec de l'authentification du titulaire de la carte (étape 3), MasterCard recommande l'interruption du traitement du paiement (option*interrompre* ). S'il choisit de poursuivre la transaction, le marchand ne bénéficie plus de la garantie de paiement conditionnelle (voir ici).

### 4.2.4 Activation et désactivation de 3-D Secure

Cette option permet au marchand d'activer ou de désactiver 3-D Secure pour toutes les cartes VISA/ MasterCard/JCB.

ATTENTION

Si 3-D Secure est désactivé, le marchand ne bénéficie pas de la garantie de paiement conditionnelle (voir ici).

# 5 Configuration des listes noires, grises et blanches

Dans le module de détection des fraudes avancé (FDMA), vous pouvez créer vos propres listes négatives (noires ou grises) sur la base des codes BIN, des numéros de carte de crédit, des adresses électroniques, des numéros de téléphone, des noms, des informations génériques et des adresses IP dont vous souhaitez ou non accepter les transactions. Il existe également trois listes positives (blanches) qui se fondent sur les adresses IP, les identifiants de client uniques, et adresse e-mail sur liste blanche.

Le comportement effectif de ces listes (à savoir si elles conduisent ou non à bloquer les transactions) dépend des paramètres que vous définissez dans la page d'évaluation du risque.

« No (Non) » dans le menu principal indique que rien n'a été configuré dans la liste noire, grise ou blanche concernée. Si une liste noire, grise ou blanche a déjà été configurée, l'état est « Yes (Oui) ».

## 5.1 Liste générale des fonctionnalités

### 5.1.1 Entrées

Dans le module de détection des fraudes avancé (FDMA), il n'y a pas de limite au nombre d'entrées dans les listes. Vous pouvez entrer jusqu'à 1 000 éléments à la fois dans la zone de texte à soumettre.

Vous pouvez toujours supprimer des entrées de vos listes en cochant les cases en question dans la colonne « Supprimer », puis en cliquant sur le bouton « Soumettre) ».

### 5.1.2 Commentaires

Vous pouvez adjoindre un commentaire à une entrée d'une liste noire, grise ou blanche.

Vous pouvez saisir le commentaire dans le champ « Comment (Commentaire) » au moment où vous soumettez un élément. Tous les éléments saisis lors de cette soumission adoptent alors le même commentaire.

Vous pouvez également ajouter ou effacer un commentaire en cliquant sur le lien « ... » dans la colonne de commentaire.

### 5.1.3 Raison

Vous pouvez sélectionner pour chaque entrée de la liste noire ou de la liste grise la raison pour laquelle vous souhaitez saisir ces données : fraude effective ou litige commercial.

IMPORTANT

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

### 5.1.4 Filtre

Vous pouvez filtrer les données des listes à l'aide du bouton « Filter (Filtre) » au sommet de la table. Vous pouvez filtrer les données par date et par contenu.

Vous pouvez supprimer un filtre par un clic sur le bouton « Remove filter (Enlever le filtre) ».

### 5.1.5 Téléchargement des listes

Vous pouvez télécharger le contenu d'une liste dans un fichier Excel en cliquant sur le bouton « Download list (Télécharger la liste) » au sommet de la table.

Si vous cliquez sur le bouton « Download list (Télécharger la liste) » alors qu'un filtre est appliqué, c'est le contenu filtré qui est téléchargé.

### 5.1.6 Avertissement en cas d'entrée sur liste noire

Dans les listes noires, vous pouvez activer une case d'option pour qu'un courriel d'avertissement soit envoyé lorsqu'une transaction correspond à une entrée de ces listes.

IMPORTANT

Vous ne devez activer ou désactiver cette option qu'une seule fois. Sa configuration s'applique à toutes les listes noires.

## 5.2 Listes blanches

Les listes blanches contiennent les informations des clients privilégiés ainsi que les données utilisées pour ignorer les autres règles (en fonction des paramètres d'évaluation du risque du marchand).

### 5.2.1 Liste blanche des adresses IP

Vous pouvez saisir les adresses IP des clients dont vous souhaitez recevoir les commandes dans la liste des adresses IP de confiance. Si l'adresse IP unique d'un client se trouve dans la liste blanche, toutes les règles de blocage liées à l'adresse IP peuvent être ignorées (selon les paramètres d'évaluation du risque du marchand).

Pour que notre système vérifie l'adresse IP du client, les marchands utilisant DirectLink doivent envoyer l'adresse IP en l'ajoutant au champ « REMOTE_ADDR ».

### 5.2.2 Liste blanche des identifiants de client uniques

L'identifiant unique du client (CUI) est un identifiant affecté par le marchand à son client. Ce peut être un nom, un numéro de client, une adresse électronique, etc. Si le marchand souhaite utiliser cet identifiant unique, il doit envoyer le CUI dans un champ supplémentaire appelé « CUID » (alphanumérique, maximum 50 caractères).

Si l'identifiant unique d'un client se trouve dans la liste blanche, pratiquement toutes les autres règles de blocage et de vérification seront ignorées (selon les paramètres de notation du commerçant). Pour en savoir plus sur la fonction Ignorer, voir l'Annexe : Fonction Ignorer.

### 5.2.3 Liste blanche des adresse e-mails

Vous pouvez ajouter l'adresse e-mail du client sur liste blanche. Pour que notre système puisse vérifier l'adresse e-mail du client, vous devez également mentionner cette adresse dans les détails de la commande. Si vous l'avez déjà fait, la vérification se fera automatiquement.
Si l'adresse e-mail du client figure sur cette liste blanche, presque toutes les autres règles de blocage et de vérification seront ignorées (selon les paramètres de notation du marchand). Pour en savoir plus sur la fonction Ignorer, voir l'Annexe : Fonction Ignorer.

## 5.3 Listes noires et grises

La liste noire permet, en fonction du paramétrage des règles, de bloquer des transactions et de forcer la vérification aux transactions. La liste grise permet, en fonction du paramétrage des règles, de forcer la vérification aux transactions.

*Exemple* : Vous avez rencontré des problèmes avec des transactions provenant d'une adresse IP particulière, mais vous n'êtes pas certain que cette adresse IP est une adresse IP dédiée, qui correspond à une personne bien définie. L'adresse IP peut aussi représenter une société ou un bâtiment, ou pourrait être attribuée sous peu à une autre personne par le fournisseur d'accès.

En pareil cas, il vaut mieux ne pas reprendre directement cette adresse IP dans votre liste noire d'adresses IP, car vous ne voulez pas désavantager ou bloquer d'autres clients potentiels. Vous placez donc l'adresse IP dans la liste grise des adresses IP jusqu'à ce que vous puissiez déterminer s'il convient de la reprendre dans votre liste noire d'adresses IP ou de la supprimer de la liste grise.

Vous pouvez déplacer des données de la liste grise dans la liste noire en cochant les cases correspondantes de la colonne « Move to blacklist (Déplacer dans la liste noire) » de la liste grise, puis en cliquant sur « Submit (Soumettre) ».

### 5.3.1 Numéro de carte

Dans les listes noire et grise des cartes de crédit, les numéros de carte de crédit doivent être saisis intégralement.

Dans la liste noire des cartes, vous pouvez activer une case d'option pour faire passer en liste grise l'adresse IP des transactions correspondant à une entrée dans la liste noire des cartes.

Si vous avez activé les moyens de paiement de type prélèvement automatique NL, DE ou AT dans votre compte, les listes noire et grise des cartes se dédoublent également en tant que listes noire et grise de comptes destinées à recevoir les numéros de compte.

### 5.3.2 Code BIN

Le code BIN correspond aux 6 premiers chiffres d'un numéro de carte de crédit. Le code BIN est lié à la banque et au pays d'origine de la carte. Par conséquent, vous pouvez reprendre dans votre liste toutes les cartes de crédit émises par la banque X dans le pays Y en y saisissant le code BIN correspondant.

### 5.3.3 Adresse IP

Dans vos listes noire et grise des adresses IP, vous pouvez non seulement saisir des adresses IP spécifiques, mais aussi des plages d'adresses aux formats suivants : « a.b.c-d.0-255 », « a.b.c-d.* » ou « a.b.c.d-e ».

Pour que notre système vérifie l'adresse IP du client, les marchands utilisant DirectLink doivent envoyer l'adresse IP en l'ajoutant au champ « REMOTE_ADDR ».

### 5.3.4 Adresse électronique

L'adresse électronique peut être une adresse fixe ou une plage d'adresses (un domaine de messagerie) si vous saisissez un astérisque (« * ») avant l'arobase (« @ »). L'adresse électronique saisie par le marchand apparaît dans la colonne « E-mail (Courriel) ». Notre système génère la « correspondance partielle » à partir de cette adresse électronique.

Pour que notre système puisse vérifier l'adresse électronique du client, le marchand doit également envoyer cette adresse dans les informations de la commande.

### 5.3.5 Nom

Le marchand peut saisir le nom des clients dans la liste noire ou la liste grise. Le nom saisi par le marchand apparaît dans la colonne « Name (Nom) ». Sur la base de ce nom, notre système génère deux autres versions du nom : le « nom épuré » et la « correspondance partielle ».

Pour que notre système puisse vérifier le nom du client, le marchand doit également envoyer le nom du titulaire de la carte, nom d'expédition et nom de facturation.

### 5.3.6 Numéro de téléphone

Le marchand peut saisir le numéro de téléphone des clients dans la liste noire ou la liste grise. Le numéro de téléphone saisi par le marchand apparaît dans la colonne « Phone number (N° de téléphone) ». Sur la base de ce numéro de téléphone, notre système génère deux autres versions : le « numéro épuré » et la « correspondance partielle ».

Pour que notre système puisse vérifier le numéro de téléphone du client, le marchand doit également envoyer ce numéro dans les informations de la commande.

### 5.3.7 Données génériques

La liste noire et la liste grise des données génériques permettent au marchand d'avoir des listes entièrement personnalisées dans lesquelles il peut saisir les données qu'il veut voir être prises en considération dans l'évaluation du risque des transactions. Ces données doivent être alphanumériques et contenir au maximum 50 caractères.

Pour que notre système soit en mesure de contrôler ces données génériques, le marchand doit également envoyer les données en les joignant au champ « GENERIC_BL » dans la commande (champ alphanumérique, maximum 50 caractères).

# 6 Évaluation des risques

La page « Risk Evaluation (Évaluation du risque) » présente la liste de tous les critères qui peuvent être définis dans le module de détection des fraudes.

IMPORTANT

Contrairement au module de détection des fraudes de base, où le comportement en matière de blocage est défini dans les listes noires et blanches, les règles de blocage, etc., c'est le marchand qui configure ici le comportement effectif des listes noires, grises et blanches ainsi que les limites et les règles dans la liste d'évaluation du risque.

Il est possible de définir une action pour chaque critère :

- Bloquer
- Examiner
- Aucune
- Ignorer le blocage

Toutes les options ne sont pas disponibles pour tous les critères.

- Si un des critères est associé à une action de blocage, la transaction est bloquée et nous lui attribuons le statut « Authorisation declined (Autorisation refusée) ».
- Si un des critères menant à un examen est rempli, la transaction doit être examinée manuellement.
- Sinon, la transaction est considérée comme non frauduleuse.

Conditions : Comme certaines informations proviennent de listes d'origine extérieure sur lesquelles nous nous fondons pour assurer la précision de l'évaluation, nous ne pouvons pas garantir un résultat correct à 100 %.

La liste qui suit présente une sélection (non exhaustive) de critères d'évaluation :

- *3-D Secure* : Le titulaire de la carte passe avec succès l'authentification 3-D Secure, mais il n'est pas enregistré. Si une carte de crédit est 3-D Secure et si vous avez conclu un contrat 3-D Secure avec votre acquéreur, vous bénéficiez d'une garantie de paiement conditionnelle (voir section 2.1.2) pour la transaction en question. Par conséquent, même si vous ne souhaitez pas recevoir de paiements de certains pays émetteurs de cartes ou IP en raison d'un risque élevé de fraude, vous pouvez autoriser les transactions réalisées au moyen des cartes de crédit 3-D Secure au départ de ces pays, car le risque est beaucoup moins important.
- *Serveur proxy anonyme* : Les serveurs proxy anonymes sont des fournisseurs d'accès internet qui autorisent les utilisateurs web à masquer leur adresse IP. Nous vous recommandons de ne pas accepter les paiements provenant de serveurs proxy anonymes !
- *Compte de messagerie gratuit* : La plupart du temps, les fraudeurs utilisent des comptes de messagerie fictifs créés via des services de messagerie gratuits. Notre système vérifie (sur la base de listes d'origine extérieure) si l'adresse électronique du client correspond ou non à un compte de messagerie gratuit. Le marchand peut décider d'ajouter un degré de risque aux transactions dont l'adresse électronique du client correspond à un compte de messagerie gratuit. Pour que notre système puisse vérifier l'adresse électronique du client, le marchand doit également envoyer cette adresse dans les informations de la commande.
- *Nombre de pays*- Le commerçant peut indiquer le nombre de pays autorisés et définir l'action à entreprendre en matière de notation si ce nombre dépasse la limite fixée, en fonction des éléments suivants :
    - Pays de la carte de crédit (pour VISA, MasterCard, American Express et Diners Club uniquement)
    - IP du pays (si disponible)
    - Adresses d'expédition et de livraison en cas d'envoi
    - Aéroports de départ en cas d'envoi par avion
- *Pays IP différent du pays émetteur de cartes* (pour VISA, MasterCard, American Express et Diners Club uniquement) : lorsque vous définissez ce paramètre à « Block transaction (Bloquer la transaction) », vous autorisez les transactions uniquement si l'adresse IP du client se trouve dans le même pays que l'émetteur de sa carte de crédit, autrement dit si le pays émetteur de cartes et le pays IP sont identiques. Ce contrôle n'est pas effectué si l'adresse IP provient d'un serveur proxy anonyme, du réseau Asie-Pacifique, du réseau européen ou d'un fournisseur satellite.
- *Adresse de facturation différente de l'adresse de livraison* : Le fait que l'adresse de facturation soit considérée comme différente de l'adresse de livraison se fonde sur la valeur du champ supplémentaire «

ADDMATCH » que le marchand nous envoie dans les informations de la commande. Si la valeur est « 1 », les adresses de facturation et de livraison sont considérées comme identiques. Si la valeur est « 0 », ces adresses sont considérées comme différentes.

- *Limite de montant, limites d'utilisation*
- *Identification de l'identifiant de client unique dans la liste blanche*
- *Liste blanche des adresse e-mails*
- *Adresse IP de confiance*
- *Carte, code BIN, adresse IP, adresse électronique, numéro de téléphone, nom du titulaire de la carte ou données génériques sur liste noire ou liste grise*
- *Pays émetteurs de cartes à risque élevé ou moyen, pays IP à risque élevé ou moyen, codes postaux à risque élevé ou moyen, dates et heures de commande à risque élevé ou moyen*

IMPORTANT

Nous vous recommandons vivement de définir les critères d'évaluation du risque suivants à « Block (Bloquer) » dans la page d'évaluation du risque :

- Carte sur liste noire
- Serveur proxy anonyme (sous pays IP)

# 7 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.

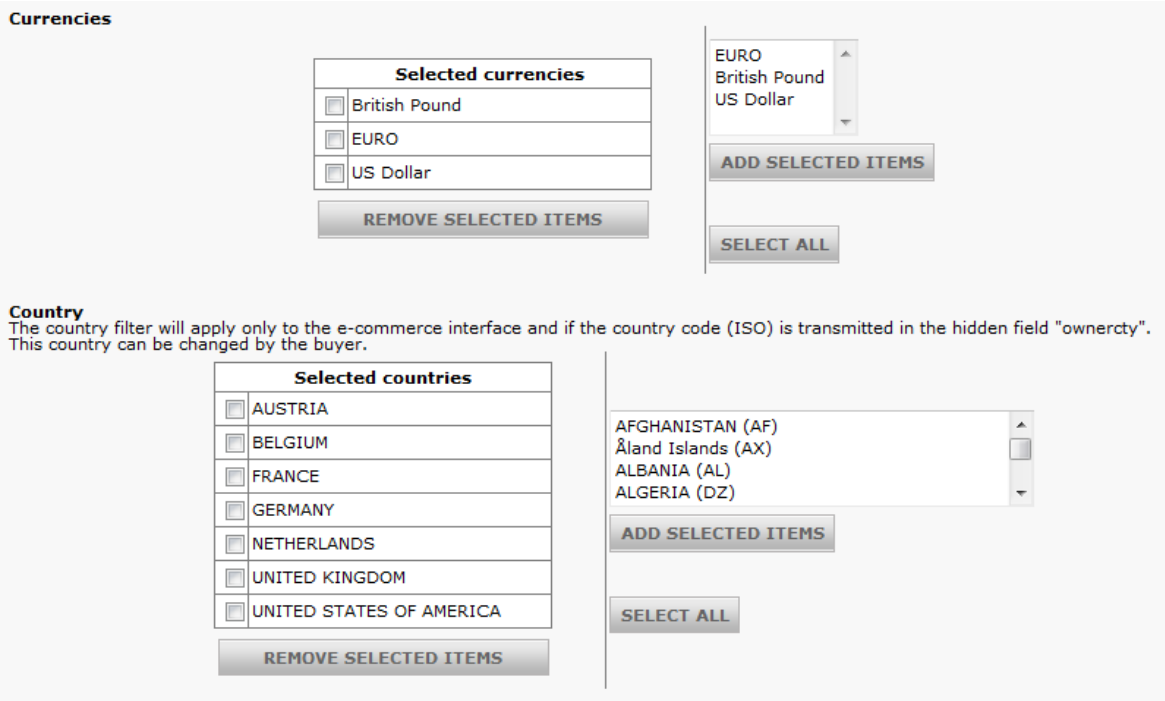
Ingenico ePayments permet aux clients d'accéder à une page de litige, permettant aux marchands d'ajouter des données de transaction à des listes noires et blanches, avec la raison du litige. Les marchands sont ainsi protégés de nouvelles fraudes et de torts répétés. La base de données Ingenico ePayments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


## 7.1 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.




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.

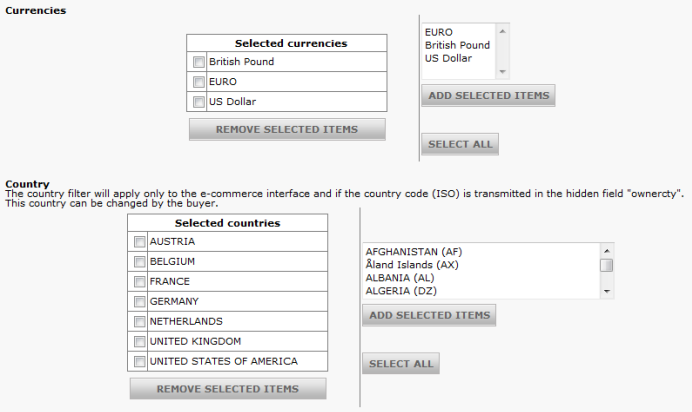
3. Accédez à la page des litiges et choisissez la liste à laquelle vous souhaitez ajouter les données de transaction (liste noire ou liste blanche). Sélectionnez ensuite le motif du litige.

   Vous pouvez marquer la transaction comme suit :

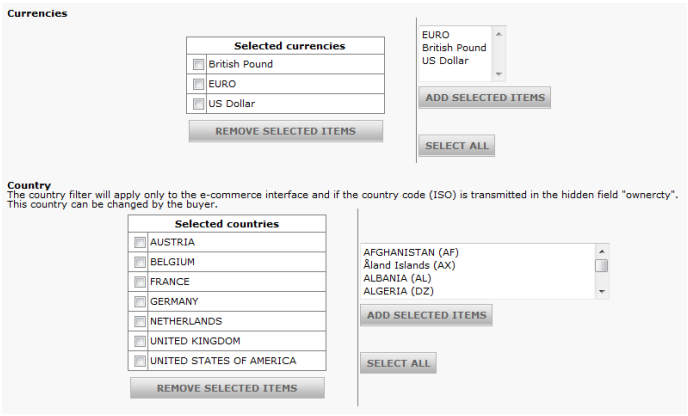
   - Les litiges commerciaux couvrent entièrement les rejets de débit reçus par le marchand et qui ne sont pas liés à des fraudes.
   - La fraude effective est un refus de débit frauduleux.
   - La suspicion de fraude a pour but d'empêcher une transaction frauduleuse.

   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.




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




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.

# 8 Retour d'information

## 8.1 Vue des transactions dans le Back Office

### 8.1.1 Critères de sélection avancés

Lorsque vous recherchez une transaction via le lien « View transactions (Afficher les transactions) » ou « Financial history (Historique financier) » dans le menu de votre compte, vous pouvez accéder à deux critères supplémentaires dans la zone « Advanced selection criteria (Critères de sélection avancés) » : Risk Category (Catégorie du risque) et IP Address (Adresse IP).

Dans la page du lien « Risk category (Catégorie du risque) », vous pouvez sélectionner les transactions d'une couleur déterminée.

Vous pouvez utiliser le champ de l'adresse IP pour rechercher toutes les transactions provenant de la même adresse IP ou d'adresses IP commençant par les mêmes chiffres.

### 8.1.2 Liste des transactions

Lorsque vous affichez la liste de vos transactions via « View transactions (Afficher les transactions) » ou « Financial history (Historique financier) » dans le Back Office, cette liste fait apparaître la catégorie du risque avec la couleur correspondante dans la colonne « Rating (Classement) ». Lorsque vous cliquez sur le risque, vous accédez aux détails de l'évaluation du risque concernant la transaction.

S'il n'existe pas de résultat d'évaluation du risque pour la transaction, par exemple parce que l'autorisation a été refusée, la liste présente des pictogrammes verts et (si la fonctionnalité 3-D Secure est activée dans votre compte) des demi-pictogrammes verts.

Le pictogramme complet  , qui représente un pouce levé, désigne une transaction 3-D Secure lors de laquelle le client a payé avec une carte de crédit enregistrée auprès de 3-D Secure. Votre acquéreur vous fait bénéficier d'une garantie de paiement conditionnelle pour les transactions de ce type.

Le demi-pictogramme  désigne une transaction 3-D Secure lors de laquelle le client a payé avec une carte de crédit qui n'est pas enregistrée auprès de 3-D Secure. Les transactions de ce type bénéficient d'un certain degré de garantie de paiement conditionnelle en fonction des dispositions spécifiques du contrat 3-D Secure avec votre acquéreur.

Les transactions sans (demi-)pictogramme sont celles qui n'ont pas été traitées avec 3-D Secure. La garantie de paiement conditionnelle ne s'applique pas à ces transactions.

Les transactions présentant un point d'exclamation  sont les transactions dont l'authentification du client a échoué. La garantie de paiement conditionnelle ne s'applique pas aux transactions que vous décidez de poursuivre (*poursuivre*) alors que leur authentification a échoué (pour MasterCard, voir ici).

*Pour plus d'informations sur la garantie de paiement conditionnelle, voir ici*

### 8.1.3 Informations de la transaction

Les informations relatives à la transaction (dans la page de l'historique financier) présentent des informations complémentaires, telles que le résultat du code de vérification de la carte (si le code CVC a été saisi par le client), le pays émetteur de cartes, le pays IP et l'adresse IP, de même que la catégorie du risque.

| FDMA | |
|---|---|
| **Risk evaluation:** | Review |
| **Risk category:** | Orange (O) |
| View risk detail | |

#### 8.1.3.1 Litige

Le bouton « Dispute (Litige) » permet d'accéder à une page dans laquelle vous pouvez ajouter différentes informations relatives à la transaction dans vos listes négatives. Vous pouvez ainsi ajouter à la liste noire le numéro de carte utilisé lors de la transaction même si vous ne connaissez pas le numéro entier de la carte, par exemple.

Vous pouvez aussi marquer simplement la transaction en tant que litige commercial ou fraude avérée.

IMPORTANT

Ne sélectionnez « Fraude avérée » que si le client a réellement commis une fraude avec cette carte, par exemple s'il a utilisé une carte qui ne lui appartient pas.


### 8.1.3.2 Affichage des transactions issues de la même adresse IP

Lorsque vous cliquez sur le bouton « View transactions from same IP address (Affichage des transactions issues de la même adresse IP) », la liste qui s'affiche présente toutes les transactions provenant de la même adresse IP au cours d'une période donnée.

### 8.1.3.3 Afficher les détails des risques

Lorsque vous cliquez sur le bouton « View risk details (Affichage des détails du risque) », vous pouvez obtenir de plus amples informations sur le calcul de l'évaluation du risque. Vous pouvez y consulter la liste des critères d'évaluation du risque qui ont été pris en considération dans le calcul, ainsi que le résultat de l'évaluation. Les critères remplis sont mis en évidence en gras dans la liste.

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

Pistage des fraudes

La page des détails de l'évaluation du risque vous permet de comparer la transaction aux transactions qui ont été enregistrées avec des informations identiques : numéro de carte de crédit, code BIN, adresse IP, adresse électronique, nom du titulaire de la carte, pays de la carte de crédit et pays de l'adresse IP, au cours d'une période que vous pouvez définir.

Vous pouvez cocher une ou plusieurs cases de critères de recherche et sélectionner l'opérateur logique que vous souhaitez appliquer aux critères de recherche sélectionnés (AND ou OR). Lorsque vous cliquez sur le bouton « Start lookup (Lancer la recherche) », le système récupère toutes les transactions

correspondant aux critères sélectionnés.

La première recherche se base sur les valeurs de la transaction d'origine. Le système recherche donc une seule valeur pour chaque critère. Si vous lancez la recherche suivante (« Start look-up 2 (Lancer la recherche 2) », « Start lookup 3 (Lancer la recherche 3) », etc.), le système effectue la recherche dans les résultats de la recherche précédente. Dans les recherches successives, les critères peuvent avoir plusieurs valeurs, ce qui multiplie les résultats et permet de détecter les pistes de fraudes potentielles.

### 8.1.4 Codes d'erreur

Lorsqu'une transaction est retenue par notre système sur la base des règles que vous avez définies dans le module de détection des fraudes, le motif est donné dans le message d'erreur de la transaction. À quelques exceptions près, tous les codes d'erreur liés à la détection des fraudes commencent par « 300011 », suivi de deux chiffres.

*Vous trouverez de plus amples informations sur les états et les codes d'erreur dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides de l'Utilisateur > La signification des statuts des paiements et des codes d'erreur éventuels.*

La liste non exhaustive suivante propose quelques exemples des codes d'erreur les plus importants :

3 / 30001100 Pays du client non autorisé

3 / 30001120 Adresse IP sur liste noire du marchand

3 / 30001130 Code BIN sur liste noire du marchand

3 / 30001140 Carte sur liste noire du marchand

3 / 30131002 Montant total autorisé atteint

3 / 30001102 Nombre de pays différents trop élevé

3 / 30001141 Adresse électronique sur liste noire

3 / 30001142 Nom de passager sur liste noire

3 / 30001143 Nom sur liste noire

3 / 30001144 Nom de passager différent du nom du titulaire

3 / 30001145 Heure de départ trop rapprochée

3 / 30001154 Limite d'utilisation autorisée atteinte

3 / 30001155 Limite d'utilisation autorisée atteinte

## 8.2 Paramètres de transaction supplémentaires

Différents paramètres de transaction supplémentaires liés à l'évaluation du risque sont renvoyés dans vos requêtes après-vente, redirections avec retour d'information, téléchargements de fichier et réponses XML DirectLink.

La liste de ces paramètres supplémentaires est présentée ci-dessous.

Les champs correspondants sont vides si une erreur de validation de format s'est produite pour les informations de la transaction.

| Paramètre | Valeur |
|---|---|
| IPCTY | Pays d'origine de l'adresse IP.<br>Format : code ISO à 2 caractères alphabétiques. Si ce paramètre n'est pas disponible, « 99 » est renvoyé dans la réponse.<br>Ce contrôle de l'adresse IP s'appuie sur des listes d'adresses IP d'origine extérieure. Il existe donc un léger risque puisque nous nous fions à leur exactitude. Cette vérification donne des résultats positifs dans 94 % des cas. |
| CCCTY | Pays d'origine de la carte de crédit.<br>Ce paramètre est disponible uniquement pour VISA, MasterCard, American Express et Diners Club. Sa valeur est vide pour toutes les autres marques et tous les autres moyens de paiement. Format : code ISO à 2 caractères alphabétiques. Si ce paramètre n'est pas |

| Paramètre | Valeur |
|---|---|
| | disponible, « 99 » est renvoyé dans la réponse.<br>Ce contrôle du pays de la carte de crédit s'appuie sur des listes d'origine extérieure. Il existe donc un léger risque puisque nous nous fions à leur exactitude. Cette vérification donne des résultats positifs dans 94 % des cas. |
| ECI | Indicateur de commerce électronique (Electronic Commerce Indicator). Les valeurs ECI possibles et leur signification sont présentées ci-dessous :<br>1 Saisie manuelle<br>2 Paiements périodiques<br>3 Paiements échelonnés<br>5 Identification du titulaire de la carte réussie<br>6 Identification prise en charge par le marchand, mais pas par le titulaire de la carte, application des règles de la garantie de paiement conditionnelle (voir ici)<br>7 Commerce électronique avec cryptage SSL<br>9 Paiements périodiques après la première transaction de commerce électronique<br>1 Identification prise en charge par le marchand, mais pas par le titulaire de la carte,<br>2 application des règles de la garantie de paiement conditionnelle (voir ici) (idem 6)<br>9 ÉCHEC de l'identification du titulaire de la carte !!! (Application possible de la garantie<br>1 de paiement conditionnelle (voir ici). Vérifier avec votre acquéreur)<br>9 Site d'authentification de la banque émettrice temporairement indisponible, mais<br>2 poursuite de la transaction |
| CVCCHECK | Résultat du contrôle du code de vérification de la carte. Valeurs possibles :<br>KO Le code CVC a été envoyé mais l'acquéreur a donné une réponse négative à la vérification du CVC ; le code CVC est erroné.<br>OK 1. Le code CVC a été envoyé et l'acquéreur a donné une réponse positive à la vérification du CVC ; le code CVC est correct. OU<br>2. L'acquéreur a envoyé un code d'autorisation, mais n'a pas renvoyé de résultat spécifique pour la vérification du CVC.<br>NO Tous les autres cas. Par exemple, aucun CVC transmis ; l'acquéreur a répondu qu'une vérification du CVC était impossible ; l'acquéreur a refusé l'autorisation mais n'a pas fourni de résultat particulier pour la vérification du CVC, etc. |
| AAVCHECK | Résultat de la vérification automatique de l'adresse. Cette vérification est actuellement disponible uniquement pour American Express. Valeurs possibles :<br>KO L'adresse a été envoyée mais l'acquéreur a donné une réponse négative à la vérification de l'adresse ; l'adresse est erronée.<br>OK 1. L'adresse a été envoyée et l'acquéreur a renvoyé une réponse positive à la vérification de l'adresse ; l'adresse est correcte. OU<br>2. L'acquéreur a envoyé un code d'autorisation, mais n'a pas renvoyé de résultat spécifique pour la vérification de l'adresse.<br>NO Tous les autres cas. Par exemple, aucune adresse transmise ; l'acquéreur a répondu qu'une vérification de l'adresse était impossible ; l'acquéreur a refusé l'autorisation mais n'a pas fourni de résultat particulier pour la vérification de l'adresse, etc. |
| VC | Carte virtuelle. Valeurs possibles :<br>ECB : E Carte Bleue.<br>ICN : Internet City Number.<br>NO : Tous les autres cas. Par exemple, la carte n'est pas une carte virtuelle, la carte |

| Paramètre | Valeur |
|---|---|
| | correspond à un type de carte virtuelle qui ne nous est pas connu, etc. |
| IP | Adresse IP du client qui est détectée par notre système dans une intégration de niveau 3 ou qui nous est envoyée par le marchand dans une intégration de niveau 2. |

Champs avancés

| | |
|---|---|
| NBRUSAGE | Nombre de fois qu'une carte de crédit a été utilisée au cours d'une période donnée (lorsque la règle « Maximum utilisation per card, per period (Utilisation maximale par carte et par période) » est configurée). |
| NBRIPUSAGE | Nombre de fois qu'une adresse IP a été utilisée au cours d'une période donnée (lorsque la règle « Maximum utilisation per IP address, per period (Utilisation maximale par adresse IP et par période) » est configurée). |
| SCO_CATEGORY | Couleur de la catégorie à laquelle le risque final appartient en fonction des paramètres de la page d'évaluation du risque (Multi-criteria selection of payment methods > Risk evaluation (Sélection multicritère des moyens de paiement > Évaluation du risque)).<br>Les valeurs possibles sont « G » (vert), « O » (orange) et « R » (rouge). |

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

# 9 Annexe : Voyage

Si vous gérez un compte comportant des fonctionnalités de voyage, vous pouvez configurer des règles et des critères supplémentaires dans la page d'évaluation du risque.

## 9.1 Nom du passager

Tous les noms de passager (au maximum 6) sont pris en considération dans l'évaluation du risque, pas seulement celui du passager principal. Le marchand peut définir un degré de risque pour trois critères liés aux noms des passagers :

- Nom de passager sur liste noire
- Nom de passager sur liste grise
- Nom de passager différent du nom du titulaire de la carte

Les listes noire et grise utilisées pour les noms des passagers sont les listes noire et grise des noms.

## 9.2 Itinéraire

### 9.2.1 Groupes d'aéroports (itinéraire risqué)

Vous pouvez définir une catégorie de risque par aéroport. Nous en tiendrons compte lors du calcul du risque de l'itinéraire de votre client (si vous avez configuré le critère Risky Itinerary (Itinéraire risqué) dans la page d'évaluation du risque).

Vous pouvez classer un aéroport selon trois catégories :

- Risque élevé
- Risque moyen
- Risque faible

Les pays à risque élevé et à risque moyen peuvent augmenter l'évaluation du risque. Les pays à risque faible ne sont pas pris en considération dans l'évaluation. Ne définissez que les aéroports à risque moyen ou élevé. Les aéroports à faible risque ne sont pas pris en considération et ne sont pas listés.

Pour configurer votre liste, saisissez l'aéroport (p. ex. « VIE » pour Vienne), définissez le risque et cliquez sur le bouton « Submit (Soumettre) ».

Vous pouvez également indiquer s'il convient de prendre en considération les escales dans le calcul de l'itinéraire risqué.

### 9.2.2 Billet aller

Comme les billets aller simple présentent un risque plus élevé que les billets aller-retour, vous pouvez ajouter un degré de risque supplémentaire pour ce critère.

### 9.2.3 Aéroport de départ

Vous pouvez indiquer les aéroports de départ qui présentent un risque faible pour vous et affecter un degré de risque supplémentaire à tous les autres en configurant le critère « Departure airport not in trusted list (Aéroport de départ non repris dans la liste de confiance) » dans la page d'évaluation du risque.

Le pays de départ est également pris en considération dans l'élément « Number of different countries (Nombre de pays différents) » .

### 9.2.4 Liste des aéroports selon le pays IP

La liste des aéroports selon le pays IP permet de configurer une liste d'aéroports dont au moins un doit être compris dans l'itinéraire si la réservation est effectuée dans un pays IP spécifique.

Pour configurer la liste des aéroports selon le pays IP, sélectionnez un ou plusieurs pays IP dans la liste et saisissez les aéroports dans les champs de texte situés à côté des pays IP.

*Exemples*

Adresse IP : AT Liste des aéroports : GRZ, INN, KLU, LNZ, SZG, VIE

Si un client effectue une réservation en Autriche (c.-à-d. le pays du client, le pays IP est « AT » pour « Autriche »), son itinéraire de vol doit comprendre l'aéroport de Graz, celui d'Innsbruck, celui de Klagenfurt, celui de Linz, celui de Salzbourg ou l'aéroport international de Vienne.

Adresse IP : BE Liste des aéroports : BRU, AMS, CDG

Si un client effectue une réservation en Belgique (c.-à-d. le pays du client, le pays IP est « BE » pour « Belgique »), son itinéraire de vol doit comprendre l'aéroport Brussels Airport, l'aéroport Schiphol d'Amsterdam ou l'aéroport de Paris - Roissy Charles de Gaulle.

## 9.3 American Express : Enhanced Authorization (Autorisation améliorée)

L'outil « Enhanced Authorization (Autorisation améliorée) » d'American Express aide les marchands spécialisés dans les voyages à réduire la fraude et les réimputations frauduleuses en soumettant différents paramètres de transaction et informations de livraison dont dispose American Express en référence à des données positives et négatives. AmEx est ainsi en mesure de fournir une réponse d'autorisation améliorée.

Lorsqu'un marchand soumet des informations de voyage, tous les champs requis ne sont pas nécessairement soumis à l'hôte d'autorisation d'AmEx. Le marchand doit donc fournir les paramètres suivants :

| Paramètre | Explication |
|---|---|
| CN | Nom du titulaire de la carte |
| OWNERTELNO | Numéro de téléphone |
| EMAIL | Adresse électronique |
| IP | Adresse IP |

*Vous trouverez de plus amples informations sur ces champs dans votre compte Ingenico ePayments. Il vous suffit de vous connecter et d'accéder à la page : Support > Manuels d'intégration & d'utilisation > Guides Techniques > Parameter Cookbook.*

Enhanced Authorization est un service gratuit pour tous les marchands American Express. Il est activé par défaut si l'UID du marchand (son numéro d'affiliation) est configuré avec les spécifications GCAG d'AmEx. Le marchand doit vérifier auprès d'AmEx si oui ou non c'est le cas.

Pour pouvoir utiliser l'outil Enhanced Authorization via Ingenico ePayments, il faut qu'un indicateur soit activé dans le compte Ingenico ePayments du marchand. Par conséquent, le marchand doit contacter notre Customer Care.

## 9.4 Heure de départ

Un billet acheté pour un départ deux jours plus tard est beaucoup plus risqué qu'un billet acheté pour un départ un mois plus tard. Vous pouvez configurer le critère de l'heure de départ dans la page d'évaluation du risque pour ajouter un degré de risque supplémentaire pour trois heures de départ différentes.

Commencez toujours par l'heure de départ la plus rapprochée (en lui attribuant un degré de risque supérieur).

# 10 Annexe : Paramètres et contrôles/règles

| Ingenico ePayments Paramètre | Description | Règles et contrôles dans FDMA |
|---|---|---|
| CN | Le nom du titulaire de la carte peut contenir un maximum de 35 caractères. Ce paramètre peut être envoyé via Ingenico ePayments e-Commerce, DirectLink et Batch. Il est à noter que pour Ingenico ePayments e-Commerce, le nom du titulaire de la carte est aussi collecté via la page de paiement Ingenico ePayments, où il correspond à un champ obligatoire. | • Nom sur liste noire<br>• Nom sur liste grise<br>• Nom de passager différent du nom du titulaire de la carte |
| OWNERADDRESS | L'adresse du client peut contenir un maximum de 35 caractères. | • L'adresse de facturation est une boîte postale |
| ADDRMATCH | Le fait que l'adresse de facturation soit considérée ou non comme différente de l'adresse de livraison se fonde sur la valeur du champ supplémentaire « ADDRMATCH » que le marchand nous envoie dans les informations de la commande. Si la valeur est « 1 », les adresses de facturation et de livraison sont considérées comme identiques. Si la valeur est « 0 », ces adresses sont considérées comme différentes. | • Adresse de facturation différente de l'adresse de livraison |
| OWNERZIP | Le code postal du client peut contenir un maximum de 10 caractères. | • Code postal risqué<br>• Vérification poussée de l'adresse pour certaines marques de carte uniquement |
| OWNERTELNO | Le numéro de téléphone du client peut contenir un maximum de 30 caractères pour tous les modules Ingenico ePayments, à l'exception d'Ingenico ePayments Batch, dont le champ peut contenir au maximum 20 caractères. Les caractères spéciaux (p. ex. « + » ou « / ») sont autorisés dans ce champ. Il est préférable d'être cohérent dans le mode d'envoi des numéros de téléphone. | • N° de téléphone sur liste grise<br>• N° de téléphone sur liste noire |
| OWNERCTY | Le pays de facturation du client peut contenir un maximum de 2 caractères. Les codes des pays selon la norme ISO 3166-1-alpha-2 se trouvent à l'adresse http://www.iso.org/iso/en/prodsservices/iso3166ma/02iso-3166-code-lists/list-en1.html. | • Nombre de pays différents |
| EMAIL | L'adresse électronique du client peut contenir un maximum de 50 caractères. | • Liste blanche des adresse e-mails<br>• Adresse électronique sur liste noire<br>• Adresse électronique sur liste grise<br>• Compte de messagerie gratuit<br>• Limites d'utilisation |
| Generic_BL | La liste noire générique peut contenir un maximum de 50 caractères. | • Liste noire générique<br>• Liste grise générique |
| REMOTE_ADDR | Adresse IP du client.<br>Cette adresse IP ne doit être envoyée que s'il est fait usage d'Ingenico ePayments DirectLink. Pour Ingenico ePayments e-Commerce, l'adresse IP est détectée et enregistrée automatiquement. | • Liste blanche des adresses IP<br>• Liste grise des adresses IP<br>• Liste noire des adresses IP<br>• Limites d'utilisation |

| Ingenico ePayments Paramètre | Description | Règles et contrôles dans FDMA |
|---|---|---|
| | | • Groupes de pays IP<br>• Serveur proxy anonyme<br>• Combinaison non autorisée de pays émetteurs de cartes et de pays IP<br>• Pays IP différent du pays émetteur de cartes |
| CUID | Identifiant unique du client. Cet identifiant peut contenir un maximum de 50 caractères. | • Liste blanche des identifiants de client uniques |
| CARDNO | Le numéro de carte ou le numéro de compte peut contenir au maximum 21 caractères. Cette adresse IP ne doit être envoyée que s'il est fait usage d'Ingenico ePayments DirectLink.<br>Pour Ingenico ePayments e-Commerce, le numéro de la carte est détecté et enregistré automatiquement. | • Liste grise des cartes<br>• Liste noire des cartes<br>• Liste noire des codes BIN<br>• Liste grise des codes BIN<br>• Pays émetteur de cartes à risque élevé<br>• Pays émetteur de cartes à risque moyen<br>• Limites d'utilisation |
| ECOM_SHIPTO_POSTAL_POSTALCODE | Code postal de l'adresse de livraison. Ce champ peut contenir un maximum de 10 caractères alphanumériques. | • Code postal risqué |
| ECOM_BILLTO_POSTAL_POSTALCODE | Code postal de l'adresse de facturation. | • Code postal risqué<br>• Vérification poussée de l'adresse pour certaines marques de carte uniquement |
| | AIRLINE / TRAVEL DATA | |
| AIPASNAME | Nom du passager principal. La valeur par défaut est le nom du titulaire de la carte de crédit. | • Nom sur liste noire<br>• Nom sur liste grise<br>• Nom de passager différent du nom du titulaire de la carte |
| AIEXTRAPASNAME1 | Nom de passager supplémentaire pour les dossiers passagers (PNR) comptant plus d'un passager. Ce champ peut être répété jusqu'à 5 fois (p. ex. pour 5 passagers supplémentaires), en changeant le chiffre à la fin du nom du champ. | • Nom sur liste noire<br>• Nom sur liste grise<br>• Nom de passager différent du nom du titulaire de la carte |
| AIORCITY1 | L'aéroport de départ (désignation courte) constitue un champ obligatoire qui peut contenir un maximum de 5 caractères. | • Aéroport de départ ne figurant pas dans la liste des aéroports de confiance<br>• Itinéraire risqué (groupes d'aéroports)<br>• Pays IP non autorisé pour l'itinéraire |
| AIORCITYL1 | L'aéroport de départ (désignation longue) constitue un champ obligatoire qui peut contenir un maximum de 20 | • Aéroport de départ ne figurant pas |

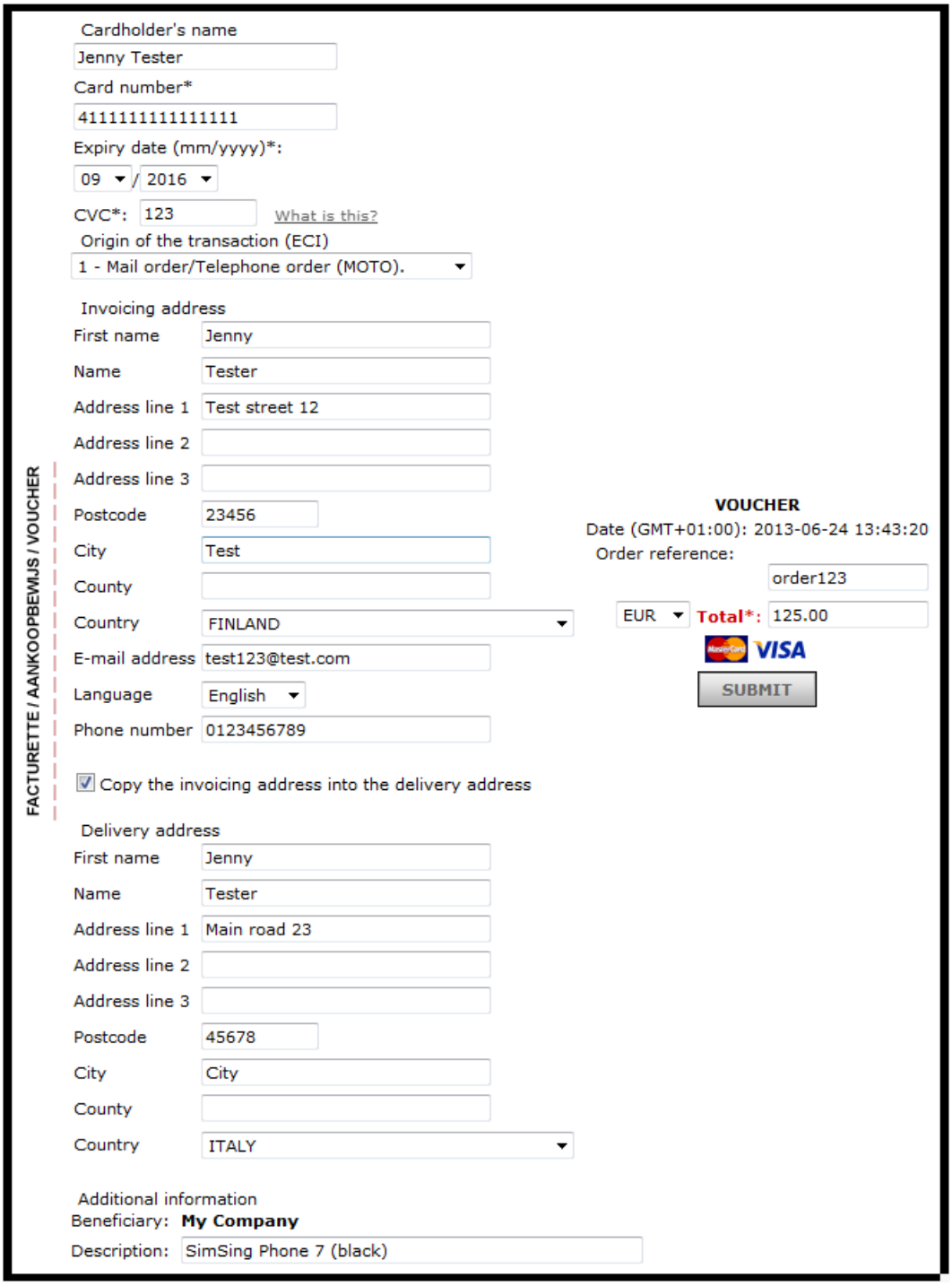
| Ingenico ePayments Paramètre | Description | Règles et contrôles dans FDMA |
|---|---|---|
| | caractères. | dans la liste des aéroports de confiance<br>• Itinéraire risqué (groupes d'aéroports)<br>• Pays IP non autorisé pour l'itinéraire |
| AIDESTCITY1 | L'aéroport d'arrivée (désignation courte) constitue un champ obligatoire qui peut contenir un maximum de 5 caractères. | • Itinéraire risqué (groupes d'aéroports)<br>• Pays IP non autorisé pour l'itinéraire |
| AIDESTCITYL1 | L'aéroport d'arrivée (désignation longue) constitue un champ obligatoire qui peut contenir un maximum de 20 caractères. | • Itinéraire risqué (groupes d'aéroports)<br>• Pays IP non autorisé pour l'itinéraire |
| AISTOPOV1 | Escale autorisée pour l'aéroport.<br>Valeurs possibles : O et X (lettres).<br>O : Le passager est autorisé à s'arrêter et à y séjourner.<br>X : Le passager n'est pas autorisé à y séjourner. | • Itinéraire risqué (groupes d'aéroports) |
| AIFLDATE1 | Date du vol. | • Heure de départ 1<br>• Heure de départ 2<br>• Heure de départ 3 |

*La liste des paramètres de voyage ci-dessus contient uniquement les paramètres liés aux règles et contrôles du module FDMA. Pour la liste complète des paramètres de voyage obligatoires, consultez l'annexe relative au format spécial voyage de nos manuels DirectLink ou e-Commerce avancé .*

# 11 Annexe : Informations supplémentaires via e-Terminal

Si vous utilisez notre solution MOTO e-Terminal, vous pouvez saisir des informations de contact et d'adresse en plus des informations par défaut de la commande. Ces données sont prises en compte dans votre outil de détection des fraudes et améliorent ainsi vos possibilités de prévention.

Dans votre Back Office, sous « Operations (Opérations) », sélectionnez « New transaction (Nouvelle transaction) ». La quittance où vous pouvez saisir les informations par défaut (nom, numéro de carte, code CVC, etc.) s'affiche.



# 12 Annexe : CVC2 et AAV

## 12.1 CVC2

CVC2 est une procédure d'authentification mise en œuvre par les sociétés de carte de crédit pour prévenir l'utilisation frauduleuse des cartes de crédit dans le cadre de transactions internet. Selon la marque, ce code peut porter un nom différent (CVC2 ou Card Validation Code (Code de validation de la carte) pour MasterCard, CVV2 ou Card Verification Value (Valeur de vérification de la carte) pour VISA, CID ou Card Identification Number (Numéro d'identification de la carte) pour American Express). Il est toutefois généralement fait référence à ce code sous le nom de « CVC ». La fonctionnalité du code CVC2 est identique pour toutes les marques.

Ce code de vérification est lié de manière unique au numéro de la carte, mais ne fait pas partie du numéro de la carte proprement dit. Selon la marque de la carte, le code de vérification est constitué de 3 ou 4 chiffres inscrits au recto ou au verso de la carte, d'un numéro d'émission, d'une date de début ou d'une date de naissance. Pour MasterCard et VISA, par exemple, le verso de la carte comporte un code de 3 chiffres dans la bande de signature qui fait suite au numéro de compte complet du client ou aux quatre derniers chiffres du numéro de compte du client.

Il est strictement interdit aux marchands et aux PSP de stocker les codes CVC2 des clients dans une base de données. Lorsque le titulaire de la carte n'est pas présent en personne, c.-à-d. dans les transactions réalisées en l'absence physique de la carte, et qu'il est invité à saisir le code CVC2 en plus du numéro de sa carte, ce code de vérification contribue à établir que le client qui place la commande a bien cette carte en main et que le compte de la carte est légitime.

## 12.2 AAV/AVS

AAV est une procédure d'authentification disponible sur certains marchés qui vise à prévenir l'utilisation frauduleuse des cartes de crédit dans le cadre de transactions internet. Cette procédure d'authentification porte un nom différent selon la marque (AVS ou Address Verification Service/System pour VISA/ MasterCard, AAV ou Automated Address Verification pour American Express). Toutefois, la fonctionnalité AAV est identique pour toutes les marques.

Elle consiste en une vérification de l'adresse qui a lieu lorsque l'acquéreur demande à l'émetteur de la carte de comparer les éléments numériques (numéro de maison et code postal) de l'adresse (de facturation ou de livraison) du client envoyée par le marchand avec ceux de l'adresse de facturation fournie par le client à l'émetteur lorsqu'il a fait sa demande de carte.

American Express effectue ce contrôle automatiquement au moment de la réception des informations d'adresse, avec la transaction. Pour les autres marques, l'exécution de ce contrôle dépend du fait que l'acquéreur effectue ce contrôle d'adresse ou non. Dans tous les cas, nous recommandons que les informations d'adresse du client soient envoyées conjointement avec les informations de la commande que vous transmettez à notre système.

Bien qu'une transaction ne soit pas rejetée suite au résultat de la vérification de l'adresse, le marchand peut utiliser ce résultat pour décider de livrer les marchandises ou de demander de plus amples renseignements au client avant de les expédier.

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

## 12.3 Adaptation de la notation sur la base du résultat AAV/AVS

Vous pouvez influencer le classement FDMA sur la base du résultat de la vérification AAV/AVS. Vous pouvez sélectionner l'action qui doit être appliquée par notre système en fonction de la réponse reçue :

| Réponse | Action |
|---|---|
| Résultat OK | *Aucune (seule option)* |
| Résultat KO | Bloquer (examiner si le mode activé est « Direct Sale (Vente directe) ») / examiner / aucune |
| Code postal KO, adresse OK | Bloquer (examiner si le mode activé est « Direct Sale (Vente directe) ») / examiner / aucune |
| Code postal OK, adresse KO | Bloquer (examiner si le mode activé est « Direct Sale (Vente directe) ») / examiner / aucune |
| Résultat non reçu ou inconnu | Bloquer (examiner si le mode activé est « Direct Sale (Vente directe) ») / examiner / aucune |

**Remarque**

La réponse « Résultat non reçu ou inconnu » peut être générée si la banque émettrice du client ne prend pas en charge le contrôle AAV/AVS, contrairement à votre acquéreur. Il convient d'en tenir compte lors de la configuration de FDMA.

# 13 Annexe : Conseils relatifs au signalement des fraudes

L'utilisation frauduleuse d'une carte de crédit doit être signalée par le titulaire de la carte lui-même à sa banque émettrice, c.-à-d. la banque à laquelle il a demandé sa carte de crédit.

Si un marchand croit que l'un de ses clients commet un acte frauduleux, il doit le signaler à son acquéreur.

Si un marchand souhaite signaler un fraudeur à la police, il n'a pas besoin du numéro de la carte de crédit. Les informations utiles à la police sont l'adresse IP que le client a utilisée au moment de la transaction ainsi que la date, l'heure et le fuseau horaire. Si le marchand peut joindre à ces informations la ou les adresses de livraison, la police aura plus de chance de retrouver le fraudeur. Il est à noter toutefois que l'adresse IP peut être usurpée et que l'adresse de livraison peut constituer seulement l'adresse d'un intermédiaire qui est chargé de réacheminer les marchandises dans un pays étranger, ce qui compliquerait la tâche de la police et le pistage du fraudeur.

# 14 Annexe : Configuration des groupes et partage de listes noires

Les marchands disposant d'un compte de type groupe qui gère plusieurs comptes individuels (plusieurs PSPID) sous un seul compte maître peuvent bénéficier de possibilités de gestion de la fraude inter-PSPID.

Ces possibilités permettent au marchand :

- de partager des listes noires, des listes grises et des listes blanches entre les différents PSPID appartenant au compte groupe du marchand ;
- de partager la configuration du module FDMA (critères, règles, limites, etc.) et des listes (groupes de pays, codes postaux risqués, etc.).

Activation

- Si vous utilisez la fonctionnalité Group Manager (Gestionnaire des groupes) et que vous souhaitez que soient activés la configuration et le partage des informations de fraude pour les groupes, contactez notre Customer Care.
- Si vous n'utilisez pas encore Group Manager, mais que vous avez plusieurs PSPID que vous voudriez joindre dans un compte de type groupe pour utiliser les possibilités de configuration et de partage des informations de fraude pour les groupes, contactez notre équipe de vente ou votre gestionnaire de compte pour de plus amples informations.

# 15 Annexe : Fonction Ignorer

Le tableau ci-après contient tous les critères pouvant être ignorés:

| Critère | Ignoré par 3-D Secure / liste blanche des CUI / Liste blanche des adresse e-mails | Ignoré par liste blanche des adresses IP |
|---|---|---|
| L'adresse est une boîte postale | ✓ | |
| Montant supérieur à la plage | ✓ | |
| Montant inférieur à la plage | ✓ | |
| BIN sur liste noire | ✓ | |
| BIN sur liste grise | ✓ | |
| Pays émetteur de cartes à risque élevé | ✓ | |
| Pays émetteur de cartes à risque moyen | ✓ | |
| Carte sur liste grise | ✓ | |
| Sous-marque de cartes à risque élevé | ✓ | |
| Sous-marque de cartes à risque moyen | ✓ | |
| Nom du titulaire de la carte sur liste noire - Correspondance partielle | ✓ | |
| Nom du titulaire de la carte sur liste noire - Correspondance parfaite | ✓ | |
| Nom du titulaire de la carte sur liste grise - Correspondance partielle | ✓ | |
| Nom du titulaire de la carte sur liste grise - Correspondance parfaite | ✓ | |
| Données sur liste noire générique | ✓ | |
| Données sur liste grise générique | ✓ | |
| Empreinte numérique de l'appareil non reçue | ✓ | |
| Empreinte numérique de l'appareil non demandée - par défaut | ✓ | |
| Empreinte numérique de l'appareil non demandée - niveau de transaction | ✓ | |
| Catégorie de profil Empreinte numérique d'appareil - Risque élevé | ✓ | |

| Critère | Ignoré par 3-D Secure / liste blanche des CUI / Liste blanche des adresse e-mails | Ignoré par liste blanche des adresses IP |
|---|---|---|
| Catégorie de profil Empreinte numérique d'appareil - Suspect | ✓ | |
| Catégorie de profil Empreinte numérique d'appareil - Suspect | ✓ | |
| E-mail sur liste noire - Correspondance partielle | ✓ | |
| E-mail sur liste noire - Correspondance parfaite | ✓ | |
| E-mail sur liste grise - Correspondance partielle | ✓ | |
| E-mail sur liste grise - Correspondance parfaite | ✓ | |
| Notation d'Expert indisponible | ✓ | |
| Premier aéroport de départ absent de la liste des aéroports de confiance | ✓ | |
| E-mail gratuite | ✓ | |
| Adresse de facturation différente de l'adresse de livraison | ✓ | |
| Adresse IP sur liste noire | ✓ | ✓ |
| Adresse IP sur liste grise | ✓ | ✓ |
| Pays IP - Serveur proxy anonyme | ✓ | ✓ |
| Pays IP à risque élevé | ✓ | ✓ |
| Pays IP à risque moyen | ✓ | ✓ |
| Pays IP différent du pays émetteur de cartes | ✓ | ✓ |
| Numéro de l'émetteur à risque élevé | ✓ | |
| Numéro de l'émetteur à risque moyen | ✓ | |
| Montant max/carte - Seuil élevé | ✓ | |
| Montant max/carte - Seuil moyen | ✓ | |
| Utilisation max. e-mail - Seuil élevé | ✓ | |
| Utilisation max. e-mail - Seuil moyen | ✓ | |
| Utilisation max. IP tous statuts - Seuil élevé | ✓ | ✓ |
| Utilisation max. IP tous statuts - Seuil moyen | ✓ | ✓ |
| Utilisation max./carte - Seuil élevé | ✓ | |

| Critère | Ignoré par 3-D Secure / liste blanche des CUI / Liste blanche des adresse e-mails | Ignoré par liste blanche des adresses IP |
|---|---|---|
| Utilisation max./carte - Seuil moyen | ✓ | |
| Utilisation max./IP - Seuil élevé | ✓ | ✓ |
| Utilisation max./IP - Seuil moyen | ✓ | ✓ |
| Nombre de pays différents | ✓ | |
| Aller simple | ✓ | |
| Nom de passager différent du nom du titulaire de la carte | ✓ | |
| Nom du passager sur liste noire - Correspondance partielle | ✓ | |
| Nom du passager sur liste noire - Correspondance parfaite | ✓ | |
| Nom du passager sur liste grise - Correspondance partielle | ✓ | |
| Nom du passager sur liste grise - Correspondance parfaite | ✓ | |
| Téléphone sur liste noire - Correspondance partielle | ✓ | |
| Téléphone sur liste grise - Correspondance partielle | ✓ | |
| Code postal et adresse à risque élevé | ✓ | |
| Code postal et adresse à risque moyen | ✓ | |
| Catégorie de produits à risque élevé | ✓ | |
| Catégorie de produits à risque moyen | ✓ | |
| Itinéraire à risque (groupes d'aéroports) - Aéroport à risque élevé | ✓ | |
| Itinéraire à risque (groupes d'aéroports) - Aéroport à risque moyen | ✓ | |
| Mode de livraison à risque élevé | ✓ | |
| Mode de livraison à risque moyen | ✓ | |
| Détails du mode de livraison à risque élevé | ✓ | |
| Détails du mode de livraison à risque moyen | ✓ | |
| Moment de la commande - Période à risque élevé | ✓ | |
| Moment de la commande - Période à risque moyen | ✓ | |
| Délai de livraison - Strictement inférieur à X heures | ✓ | |
| Délai de livraison - Strictement inférieur à Y | ✓ | |

| Critère | Ignoré par 3-D Secure / liste blanche des CUI / Liste blanche des adresse e-mails | Ignoré par liste blanche des adresses IP |
|---|---|---|
| heures | | |
| Délai de livraison - Strictement inférieur à Y heures | ✓ | |
| Délai de départ - Strictement inférieur à X jours | ✓ | |
| Délai de départ - Strictement inférieur à Y jours | ✓ | |
| Délai de départ - Strictement inférieur à Z jours | ✓ | |
| Combinaison pays émetteur de cartes/pays IP non autorisée - Risque élevé | ✓ | ✓ |
| Combinaison pays émetteur de cartes/pays IP non autorisée - Risque moyen | ✓ | ✓ |
| Pays IP non autorisé pour l'itinéraire | ✓ | ✓ |

Remarques:

- Le critère « Carte sur liste noire » ne peut et ne sera jamais ignoré.
- Les règles d'après-vente (AVS/CVC) ne seront pas ignorées.
- La catégorie (Blocage ou Vérification) peut être ignorée par le critère 3-D Secure/liste des CUI/liste blanche des adresse e-mails.
- Trois points sont ajoutés à la note, même si une règle de vérification est ignorée.