

Module de Détection de Fraude Avancé - Notation

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

Table des matières

1	Qu'est-ce que le module de détection des fraudes ?	5
1.1	Avantages	5
1.2	Accès	5
1.3	Contenu	5
2	Activation et configuration de la détection des fraudes	7
2.1	Groupes de pays de carte	7
2.2	Groupes de pays d'adresse IP	7
2.3	Combinaisons risquées de pays IP et pays émetteurs de cartes	8
2.4	Limite de montant	8
2.5	Limites d'utilisation	8
2.5.1	Utilisation de la carte	8
2.5.2	Utilisation de l'adresse IP	9
2.5.3	Utilisation de l'adresse électronique	9
2.6	Données risquées	10
2.6.1	Codes postaux et adresses risqués	10
2.6.2	Périodes risquées (dates et heures de commande)	11
2.6.3	Modes d'expédition risqués	12
2.6.4	Détails des modes d'expédition risqués	12
2.6.5	Catégories de produits risquées	13
2.6.6	Délais de livraison risqués	14
2.6.7	Sous-marques risquées	14
2.6.8	Numéros d'émetteur risqués	14
2.7	Dupliquer paramètres	15
3	3-D Secure	17
3.1	Généralités	17
3.1.1	Demande d'affiliation	17
3.1.2	Traitement des transactions 3-D Secure standard	17
3.2	Options de configuration	18
3.2.1	Problème technique	18
3.2.2	Service d'identification temporairement indisponible	18
3.2.3	Échec de l'authentification (MasterCard seulement)	18
3.2.4	Activation et désactivation de 3-D Secure	18

4	Configuration des listes noires, grises et blanches	19
4.1	Liste générale des fonctionnalités.....	19
4.1.1	Entrées	19
4.1.2	Commentaires	19
4.1.3	Raison	19
4.1.4	Filtre	19
4.1.5	Téléchargement des listes	19
4.1.6	Avertissement en cas d'entrée sur liste noire	20
4.2	Listes blanches.....	20
4.2.1	Liste blanche des adresses IP	20
4.2.2	Liste blanche des identifiants de client uniques	20
4.2.3	Liste blanche des adresse e-mails	20
4.3	Listes noires et grises.....	20
4.3.1	Numéro de carte	21
4.3.2	Code BIN	21
4.3.3	Adresse IP	21
4.3.4	Adresse électronique	21
4.3.5	Nom	21
4.3.6	Numéro de téléphone	21
4.3.7	Données génériques	22
5	Notation	23
6	Dispute	25
6.1	Ajouter des données de transaction à une liste noire et blanche.....	25
7	Retour d'information	28
7.1	Vue des transactions dans le Back Office	28
7.1.1	Critères de sélection avancés	28
7.1.2	Informations de la transaction	28
7.1.2.1	Litige	28
7.1.2.2	Affichage des transactions issues de la même adresse IP.....	29
7.1.2.3	Affichage des détails de la notation.....	29
7.1.3	Codes d'erreur	29
7.2	Paramètres de transaction supplémentaires.....	30
8	Annexe : Paramètres et contrôles/règles	33

9	Annexe : Informations supplémentaires via e-Terminal (MOTO)	36
10	Annexe : CVC2 et AAV	37
10.1	CVC2	37
10.2	AAV/AVS	37
10.3	Adaptation de la notation sur la base du résultat AAV/AVS	37
11	Annexe : Conseils relatifs au signalement des fraudes	39
12	Annexe : Configuration des groupes et partage de listes noires	40
13	Annexe : Fonction Ignorer	41

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

Contrairement au module de détection des fraudes standard, le module de détection des fraudes avancé (FDMA) vous permet de configurer le comportement effectif des listes noires, grises et blanches, ainsi que les règles et les limites dans la liste de notation.

Le module de détection des fraudes de base et le module de détection des fraudes avancé sont tous deux compatibles selon le principe de la compatibilité ascendante, ce qui veut dire qu'une mise à niveau vers le module avancé n'affecte pas le comportement de blocage que vous avez configuré dans le module de base. Concrètement :

- Toutes les entrées des listes noires restent présentes et les critères correspondants dans la page de notation sont configurés de façon à conduire à un blocage.
- Les pays émetteurs de cartes et IP dont les paiements ne doivent pas être acceptés, selon la configuration que vous avez définie, sont considérés comme des pays à « risque élevé » et sont configurés de façon à conduire à un blocage dans la page de notation.
- Les entrées de la liste blanche des adresses IP restent présentes, et le comportement correspondant est défini dans la page de notation.

Bien entendu, dès lors vous avez choisi la mise à niveau vers le module de détection des fraudes avancé, vous pouvez bénéficier des fonctionnalités évoluées et des critères affinés qu'offre ce module pour évaluer le risque des transactions.

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
- Affecter une note en fonction de risques spécifiques identifiés
- 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 au 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 multicritère dépend du moyen de paiement. Pour certains de ces moyens de paiement, 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 Activation et configuration de la détection des fraudes

La table « Fraud detection activation and configuration (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 de notation 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 « Scoring (Notation) ».

2.1 Groupes de pays de carte

Par défaut, tous les pays émetteurs de 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 la carte sur la base de son code BIN, c.-à-d. les 6 premiers chiffres du numéro de la carte de crédit. Le code BIN 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 la notation. Les pays émetteurs de cartes à risque moyen peuvent augmenter la notation. Les pays émetteurs de cartes à risque faible ne sont pas pris en considération dans la notation.

Remarque

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

2.2 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 toutefois être exclu car cette vérification de l'adresse IP 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'élévation de la notation. Les pays IP à risque moyen peuvent augmenter la notation. Les pays IP à risque faible ne sont pas pris en considération dans la notation.

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 « Scoring (Notation) ».

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.

2.3 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 la notation. Les combinaisons à risque moyen peuvent augmenter la notation. Les combinaisons à risque faible ne sont pas prises en considération dans la notation.

Remarque

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

2.4 Limite de montant

Vous pouvez limiter le montant par transaction en saisissant des montants minimum et maximum. 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.

2.5 Limites d'utilisation

2.5.1 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 générer deux notes différentes. Avec un seuil bas, vous pouvez uniquement augmenter la note du risque. Avec un seuil haut, vous pouvez augmenter la note du risque ou procéder directement à un blocage.

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.

2.5.2 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 à partir de 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 générer deux notes différentes. Avec un seuil bas, vous pouvez uniquement augmenter la note du risque. Avec un seuil haut, vous pouvez augmenter la note du risque ou procéder directement à un blocage.

« 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

2.5.3 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 définir un seuil bas et un seuil haut afin d'obtenir deux notes différentes. Avec un seuil bas, vous pouvez uniquement augmenter la note du risque. Avec un seuil haut, vous pouvez augmenter la note du risque ou procéder directement à un blocage.

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.

2.6 Données risquées

2.6.1 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 lié	d'entrée	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 lié	d'entrée	Format	Explication	Exemple
ECOM_BILLTO_POSTAL_COUNTRYCODE		AN (2)	Pays de facturation	UK
ECOM_BILLTO_POSTAL_POSTALCODE		AN (10)	Code postal - adresse de facturation	75420
ECOM_BILLTO_POSTAL_		AN (35)	Adresse de	Rue Baker 221B

Paramètre lié	d'entrée	Format	Explication	Exemple
STREET_LINE1			facturation, première ligne	
ECOM_BILLTO_POSTAL_STREET_LINE2		AN (35)	Adresse de facturation, deuxième ligne	2ème étage

Adresse de livraison

Paramètre lié	d'entrée	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.

2.6.2 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 niveaux de risque possibles :

- Risque élevé
- Risque moyen
- Risque faible

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

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 « Appliquer ».

2.6.3 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 d'expédition. 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 la notation. Les modes de livraison à risque moyen peuvent augmenter la notation. Les modes de livraison à risque faible ne sont pas pris en considération dans la notation.

Pour configurer votre liste, saisissez le mode d'expédition, définissez le risque et cliquez sur le bouton « Ajouter ». Pour terminer, cliquez sur le bouton « Envoyer ».

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

2.6.4 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 caractères)	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.

2.6.5 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 Aliments 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.

2.6.6 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 « Ajouter ». Pour terminer, cliquez sur le bouton « Envoyer ».

Paramètre lié	d'entrée	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.

2.6.7 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 « Ajouter ». Pour terminer, cliquez sur le bouton « Envoyer ».

2.6.8 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 des numéros . 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'élévation de la notation. Les numéros d'émetteur à risque moyen peuvent augmenter la notation. Les numéros d'émetteur à risque faible ne sont pas pris en considération dans la notation.

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) ».

2.7 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

Whenever you copy settings from one payment method to another, the other payment method existing configuration will be erased and replaced. No undo possible.

Features		American Express	Bancontact/Mister Cash	Direct Debits DE	Direct Debits NL	MasterCard	JCB	PAYPAL
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FDMA criteria weights	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Usage limits settings	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP country groups list	n.c.							
Card country groups list	<input type="checkbox"/>	<input type="checkbox"/>	-	-	-	<input checked="" type="checkbox"/>	-	-
Min max amount settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time to departure settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Time to delivery settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Number of different countries	n.c.							
Fraud Expert settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

SUBMIT

CLOSE WINDOW

3 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.

3.1 Généralités



3.1.1 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.

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

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.

3D-Secure				
About Verified By Visa and SecureCode (3D-Secure)				
Credit card	Acquirer	Card status	3DS activation date	3DS status
 MasterCard	Test MasterCard acquirer	Active	-	REQUEST 3DS
 VISA	Test VISA acquirer	Active	-	REQUEST 3DS

3.1.2 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/AmEx 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.

3.2 Options de configuration

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

3.2.1 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/AmEx 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/AmEx (étape 1), VISA/MasterCard/JCB/AmEx 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](#)).

3.2.2 Service d'identification temporairement indisponible

Au cas où le service d'identification du titulaire de la carte serait temporairement indisponible, le marchand peut choisir de *poursuivre* ou d' *interrompre* la transaction.

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/AmEx recommande de continuer l'opération (option *poursuivre*). En pareil cas, toutefois, le marchand ne bénéficie plus de la garantie de paiement conditionnelle (voir [ici](#)).

3.2.3 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](#)).

3.2.4 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/AmEx.

ATTENTION

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

4 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 « Scoring (Notation) ».

« 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) ».

4.1 Liste générale des fonctionnalités

4.1.1 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 « Envoyer ».

4.1.2 Commentaires

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

Vous pouvez l'enregistrer au moment de la soumission en le saisissant dans le champ « Comment (Commentaire) ». 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.

4.1.3 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.

4.1.4 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) ».

4.1.5 Téléchargement des listes

Vous pouvez télécharger le contenu d'une liste dans une feuille de calcul (p. ex. 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.

4.1.6 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. Le courriel d'avertissement est envoyé aux adresses électroniques configurées dans la zone « E-mail address(es) for transaction-related e-mails (Adresses électroniques des courriels liés aux transactions) » dans la page Technical information (Informations techniques) de votre compte.

IMPORTANT

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

4.2 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 de notation du marchand).

4.2.1 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 sont ignorées (selon les paramètres de notation du marchand).

Pour que notre système puisse vérifier l'adresse IP du client, les marchands utilisant DirectLink doivent également envoyer l'adresse IP dans le champ « REMOTE_ADDR ».

Vous pouvez saisir des plages d'adresses IP au format « a.b.c-d.0-255 », « a.b.c-d.* » ou « a.b.c.d-e ».

4.2.2 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](#).

4.2.3 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](#).

4.3 Listes noires et grises

La liste noire permet, en fonction du paramétrage des règles, de bloquer des transactions, de forcer la vérification de transactions et d'ajouter des notations de risque aux transactions. La liste grise permet, en fonction du paramétrage des règles, de forcer la vérification de transactions et d'ajouter des notations de risque 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 dans l'avenir 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) ».

4.3.1 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.

4.3.2 Code BIN

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. 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.

4.3.3 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 ».

4.3.4 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.

4.3.5 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.

4.3.6 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.

4.3.7 Données génériques

La liste noire et la liste grise des données génériques permettent au marchand d'avoir des listes entièrement personnalisées auxquelles il peut ajouter les données qu'il veut voir être prises en considération dans la notation des transactions. Les données doivent être alphanumériques et ne doivent pas dépasser 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).

5 Notation

La liste des critères apparaît dans la page de configuration Scoring (Notation) ; cette page contient tous les critères qui peuvent être définis dans le module de détection des fraudes avancé.

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 de notation.

Vous pouvez configurer une des actions suivantes par critère :

- *Augmentation de la pondération du risque* : Une pondération de 0 à 5 peut être ajoutée lorsque le critère augmente le risque.
- *Diminution de la pondération du risque* : Une pondération de 0 à 5, 10 ou 20 peut être déduite lorsque le critère diminue le risque.
- *Examen forcé* : Il est possible de forcer l'examen d'une transaction pour tous les critères. L'examen forcé induit également l'addition de 3 points à la note, indépendamment des effets des autres règles. La transaction devient orange si la note est verte ou orange, ou reste rouge si la note totale se situe au-dessus du seuil rouge et si d'autres critères de blocage sont remplis.
- *Blocage de la transaction* : Certains critères donnent également la possibilité de bloquer la transaction. Les règles définies par le marchand peuvent donc soit bloquer la transaction, soit influencer la note générale de la transaction. La note finale correspond à la pondération totale des différents critères. Plus la note est élevée, plus le risque est grand.
- *Ignorer les règles de blocage et de vérification*

Le marchand peut définir une valeur de note déterminée comme limite supérieure de la notation intermédiaire, c.-à-d. avant que la transaction soit autorisée. Cette configuration indique que toutes les transactions présentant cette note ou une note supérieure doivent être bloquées avant toute procédure d'autorisation. Le contrôle AAV et CVC a lieu après l'envoi de la transaction à l'acquéreur (c.-à-d. après l'autorisation), de telle sorte que ces valeurs de notation ne sont pas prises en considération en ce qui concerne cette limite de notation intermédiaire.

La somme des valeurs avant autorisation et des valeurs des notes AAV et CVC donne la notation finale. Le marchand peut déterminer les catégories de notation sur la base de cette valeur de notation finale, associée à des couleurs : vert (risque faible), orange (risque moyen) et rouge (risque élevé). Ces couleurs s'affichent dans le retour d'information au marchand.

Si une transaction est bloquée sur la base de vos paramètres, nous définissons le statut « Autorisation declined (Autorisation refusée) ».

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

La liste qui suit présente une sélection (non exhaustive) de critères de notation :

- *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 une notation du 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)
 - 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 de définir les critères de notation suivants à « Block transaction (Bloquer la transaction) » dans la page Scoring (Notation) :

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

6 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.

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
			DISPUTE

6.1 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	EURO British Pound US Dollar
<input type="checkbox"/> EURO	
<input type="checkbox"/> US Dollar	
<input type="button" value="REMOVE SELECTED ITEMS"/>	
<input type="button" value="ADD SELECTED ITEMS"/>	
<input type="button" value="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	AFGHANISTAN (AF) Åland Islands (AX) ALBANIA (AL) ALGERIA (DZ)
<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	
<input type="button" value="REMOVE SELECTED ITEMS"/>	
<input type="button" value="ADD SELECTED ITEMS"/>	
<input type="button" value="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.

7 Retour d'information

7.1 Vue des transactions dans le Back Office

7.1.1 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 Scoring (Notation), vous pouvez choisir entre trois catégories : rouge, orange et vert.

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.

7.1.2 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 reçue. Apparaissent aussi la notation finale et la catégorie de notation, ainsi que le bouton permettant d'accéder à l'affichage des détails de la notation, pour le cas où vous voudriez en savoir plus sur la notation.

DISPUTE Mark as a dispute or fraud and add to blacklists.

VIEW TRANSACTIONS FROM SAME IP ADDRESS

Fraud detection

Scoring: 14
Scoring category: Green (G)

VIEW SCORING DETAILS

E-commerce with SSL encryption
Card verification code : CVC received: Unknown result
Card country: CH (SWITZERLAND)
IP address country: GB (UNITED KINGDOM)
Received IP address: 94.118.170.40

Deux boutons sont situés au-dessus de la table pour accéder à d'autres informations encore : « Dispute (Litige) » et « View transactions from same IP address (Affichage des transactions issues de la même adresse IP) ».

7.1.2.1 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.

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
			DISPUTE

7.1.2.2 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.

7.1.2.3 Affichage des détails de la notation

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

Pistage des fraudes

La page des détails de la notation 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 recherche porte sur toutes les transactions à partir du moment où vous la lancez (et non à partir de la date de la transaction d'origine).

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.

7.1.3 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 des cartes 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
- 3 / 30001180 Note maximale atteinte

7.2 Paramètres de transaction supplémentaires

Différents paramètres de transaction supplémentaires liés à la notation 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	<p>Pays d'origine de l'adresse IP.</p> <p>Format : code ISO à 2 caractères alphabétiques. Si ce paramètre n'est pas disponible, « 99 » est renvoyé dans la réponse.</p> <p>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.</p>
CCCTY	<p>Pays d'origine de la carte de crédit.</p> <p>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 disponible, « 99 » est renvoyé dans la réponse.</p> <p>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.</p>
ECI	<p>Indicateur de commerce électronique (Electronic Commerce Indicator). Les valeurs ECI possibles et leur signification sont présentées ci-dessous :</p> <ul style="list-style-type: none"> 1 Saisie manuelle 2 Paiements périodiques 3 Paiements échelonnés 5 Identification du titulaire de la carte réussie

Paramètre	Valeur
	<p>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)</p> <p>7 Commerce électronique avec cryptage SSL</p> <p>9 Paiements périodiques après la première transaction de commerce électronique</p> <p>12 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) (idem 6)</p> <p>91 ÉCHEC de l'identification du titulaire de la carte !!! (Application possible de la garantie de paiement conditionnelle (voir ici). Vérifier avec votre acquéreur)</p> <p>92 Site d'authentification de la banque émettrice temporairement indisponible, mais poursuite de la transaction</p>
CVCHECK	<p>Résultat du contrôle du code de vérification de la carte. Valeurs possibles :</p> <p>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.</p> <p>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 2. L'acquéreur a envoyé un code d'autorisation, mais n'a pas renvoyé de résultat spécifique pour la vérification du CVC.</p> <p>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.</p>
AAVCHECK	<p>Résultat de la vérification automatique de l'adresse. Cette vérification est actuellement disponible uniquement pour American Express. Valeurs possibles :</p> <p>KO L'adresse a été envoyée mais l'acquéreur a donné une réponse négative à la vérification de l'adresse ; l'adresse est erronée.</p> <p>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 2. L'acquéreur a envoyé un code d'autorisation, mais n'a pas renvoyé de résultat spécifique pour la vérification de l'adresse.</p> <p>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.</p>
VC	<p>Carte virtuelle. Valeurs possibles :</p> <p>ECB : E Carte Bleue.</p> <p>ICN : Internet City Number.</p> <p>NO : Tous les autres cas. Par exemple, la carte n'est pas une carte virtuelle, la carte correspond à un type de carte virtuelle qui ne nous est pas connu, etc.</p>
IP	<p>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.</p>

Champs avancés

NBRUSAGE	<p>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).</p>
NBRIPUSAGE	<p>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).</p>
SCORING	<p>Note finale de la transaction, c.-à-d. total des notes attribuées à chaque élément décrit</p>

	dans la liste de notation.
SCO_CATEGORY	Couleur de la catégorie à laquelle la note finale appartient en fonction des paramètres de la page de notation (Multi-criteria selection of payment methods > Scoring (Sélection multicritère des moyens de paiement > Notation)). 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.

8 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.	<ul style="list-style-type: none"> Nom sur liste noire Nom sur liste grise Nom de passager différent du nom du titulaire de la carte
OWNERADDRESS	L'adresse du client peut contenir un maximum de 35 caractères.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Adresse de facturation différente de l'adresse de livraison
OWNERZIP	Le code postal du client peut contenir un maximum de 10 caractères.	<ul style="list-style-type: none"> Code postal risqué 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.	<ul style="list-style-type: none"> N° de téléphone sur liste grise 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 .	<ul style="list-style-type: none"> Nombre de pays différents
EMAIL	L'adresse électronique du client peut contenir un maximum de 50 caractères.	<ul style="list-style-type: none"> Liste blanche des adresse e-mails Adresse électronique sur liste noire Adresse électronique sur liste grise Compte de messagerie gratuit Limites d'utilisation
Generic_BL	La liste noire générique peut contenir un maximum de 50 caractères.	<ul style="list-style-type: none"> Liste noire générique Liste grise générique
REMOTE_ADDR	Adresse IP du client. 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.	<ul style="list-style-type: none"> Liste blanche des adresses IP Liste grise des adresses IP Liste noire des adresses IP Limites d'utilisation

		<ul style="list-style-type: none"> • Groupes de pays IP • Serveur proxy anonyme • Combinaison non autorisée de pays émetteurs de cartes et de pays IP • Pays IP différent du pays émetteur de cartes
CUID	Identifiant unique du client. Cet identifiant peut contenir un maximum de 50 caractères.	<ul style="list-style-type: none"> • Liste blanche des identifiants de client uniques
CARDNO	Le numéro de carte ou le numéro de compte peut contenir au maximum 21 caractères. Cette information ne doit être envoyée que s'il est fait usage d'Ingenico ePayments DirectLink. Pour Ingenico ePayments e-Commerce, le numéro de la carte est détecté et enregistré automatiquement.	<ul style="list-style-type: none"> • Liste grise des cartes • Liste noire des cartes • Liste noire des codes BIN • Liste grise des codes BIN • Pays émetteur de cartes à risque élevé • Pays émetteur de cartes à risque moyen • Limites d'utilisation
ECOM_SHIPTO_POSTALCODE	Code postal de l'adresse de livraison. Ce champ peut contenir un maximum de 10 caractères alphanumériques.	<ul style="list-style-type: none"> • Code postal risqué
ECOM_BILLTO_POSTALCODE	Code postal de l'adresse de facturation.	<ul style="list-style-type: none"> • Code postal risqué • 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.	<ul style="list-style-type: none"> • Nom sur liste noire • Nom sur liste grise • 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.	<ul style="list-style-type: none"> • Nom sur liste noire • Nom sur liste grise • 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.	<ul style="list-style-type: none"> • Aéroport de départ ne figurant pas dans la liste des aéroports de confiance • Itinéraire risqué (groupes d'aéroports) • 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 caractères.	<ul style="list-style-type: none"> • Aéroport de départ ne figurant pas dans la liste des aéroports de confiance • Itinéraire risqué

		(groupes d'aéroports) <ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Itinéraire risqué (groupes d'aéroports) • 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.	<ul style="list-style-type: none"> • Itinéraire risqué (groupes d'aéroports) • Pays IP non autorisé pour l'itinéraire
AISTOPOV1	Escale autorisée pour l'aéroport. Valeurs possibles : O et X (lettres). O : Le passager est autorisé à s'arrêter et à y séjourner. X : Le passager n'est pas autorisé à y séjourner.	<ul style="list-style-type: none"> • Itinéraire risqué (groupes d'aéroports)
AIFLDATE1	Date du vol.	<ul style="list-style-type: none"> • Heure de départ 1 • Heure de départ 2 • 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 .

9 Annexe : Informations supplémentaires via e-Terminal (MOTO)

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 FDMA et améliorent en tant que telles vos possibilités en matière de prévention des fraudes.

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.

Les informations d'adresse de facturation et de livraison supplémentaires y apparaissent :

Cardholder's name
Jenny Tester

Card number*
4111111111111111

Expiry date (mm/yyyy)*:
09 / 2016

CVC*: 123 [What is this?](#)

Origin of the transaction (ECI)
1 - Mail order/Telephone order (MOTO).

Invoicing address


First name Jenny
Name Tester
Address line 1 Test street 12
Address line 2
Address line 3
Postcode 23456
City Test
County
Country FINLAND
E-mail address test123@test.com
Language English
Phone number 0123456789

Copy the invoicing address into the delivery address

Delivery address

First name Jenny
Name Tester
Address line 1 Main road 23
Address line 2
Address line 3
Postcode 45678
City City
County
Country ITALY

Additional information
Beneficiary: **My Company**
Description: SimSing Phone 7 (black)

VOUCHER
Date (GMT+01:00): 2013-06-24 13:43:20
Order reference: order123
EUR Total*: 125.00

SUBMIT

FACTURETTE / AANKOOPBEWIJS / VOUCHER

10 Annexe : CVC2 et AAV

10.1 CVC2

CVC2 est une procédure d'authentification mise en œuvre par les sociétés de carte de crédit qui vise à prévenir l'utilisation frauduleuse des cartes de crédit dans le cadre de transactions Internet. Selon la marque, ce code porte un nom différent (CVC2 ou Code de validation de carte (Card Validation Code) pour MasterCard, CVV2 ou Valeur de vérification de carte (Card Verification Value) pour VISA, CID ou Numéro d'identification de carte (Card Identification Number) 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 son code CVC2 en plus du numéro de sa carte, ce code de vérification contribue à établir que le client qui passe la commande a bien cette carte en main et que le compte de la carte est légitime.

10.2 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.

10.3 Adaptation de la notation sur la base du résultat AAV/AVS

Vous pouvez influencer la notation 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 / soustraire la « valeur » de la notation du risque
Résultat KO	Aucune / ajouter la « valeur » à la notation du risque / forcer l'examen / bloquer (examiner si le mode activé est « Direct sale (Vente directe) »)
Code postal KO, adresse OK	Aucune / ajouter la « valeur » à la notation du risque / forcer l'examen / bloquer (examiner si le mode activé est « Direct sale (Vente directe) »)
Code postal OK, adresse KO	Aucune / ajouter la « valeur » à la notation du risque / forcer l'examen / bloquer (examiner si le mode activé est « Direct sale (Vente directe) »)
Résultat non reçu ou inconnu	Aucune / ajouter la « valeur » à la notation du risque / forcer l'examen

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.

11 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 estime 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.

12 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 commerciale pour de plus amples informations.

13 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	✓	
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	✓	
Utilisation max./carte - Seuil moyen	✓	
Utilisation max./IP - 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./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 heures	✓	
Délai de livraison - Strictement inférieur à Y heures	✓	

Critère	Ignoré par 3-D Secure/ liste blanche des CUI / liste blanche des adresse e-mails	Ignoré par liste blanche des adresses IP
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 de notation (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.