

LCLF - Présentation du module anti-fraude



- 1 Principe de fonctionnement
- 2 Listes
 - 2.1 Passage automatique en liste Clients connus (liste Standard)
 - 2.2 Fonctionnement des listes
- 3 Règles
 - 3.1 Actions possibles
 - 3.2 Périmètre d'une règle
 - 3.3 Règles
 - 3.4 Créer une règle
 - 3.5
 - 3.6
 - 3.7
 - 3.8 Règles génériques
- 4 Listes libres
 - 4.1 Créer une liste
 - 4.2 Utiliser une liste
- 5 Mises en liste automatiques
 - 5.1 Mise en liste sur code retour de la banque
 - 5.2 Mise en liste sur carte en opposition
- 6 Motifs
- 7 Alertes
 - 7.1 Configurer les destinataires
 - 7.2 Activer les alertes pour les règles
 - 7.3 Alerte par email
 - 7.4 Alertes par notifications serveur « getAlertDetails »
- 8 Détail d'une transaction

Principe de fonctionnement

Le module LCLF fonctionne sur le principe suivant :

- Chaque transaction se trouve affectée à une **liste**.
- Chaque liste, à l'exception de la noire, contient des **règles** que vous aurez déterminées et qui s'appliqueront à la transaction.

Listes

Il existe cinq listes dans le module LCLF :

- La liste Nouveaux clients
- La liste Standard (= clients connus)
- La liste Blanche
- La liste Grise
- La liste Noire

Toutes les listes permettent d'y enregistrer des identifiants client.

Les listes grise et noire permettent en plus d'enregistrer des éléments à risque tels que des domaines d'adresses email, des plages d'adresses IP ou encore des cartes bancaires. Voir la [liste complète](#).

Les éléments peuvent être mis en liste définitivement ou temporairement.

Les listes standard, blanche, grise et noire peuvent être alimentées par fichier à l'aide d'un traitement [batch](#). Vous pouvez donc nous communiquer des listes de clients ou éléments à risque que vous souhaitez inclure dans ces listes. Notez que ces travaux peuvent être facturés.

Passage automatique en liste Clients connus (liste Standard)

Le module de lutte contre la fraude vous permet de distinguer vos nouveaux clients des clients connus selon des critères d'historique que vous définissez : nombre de transactions acceptées et/ou ancienneté du compte. Cela permet alors d'appliquer des règles moins contraignantes sur les comptes établis.

Par défaut, un identifiant client est placé dans la liste des Nouveaux clients. Si vous avez défini des critères de passage en liste Standard (clients connus), celui-ci se fait alors automatiquement lorsque les seuils sont atteints, par traitement batch la nuit suivante.

Cette fonction est disponible dans le menu *Configuration*.

Configurer le passage automatique des clients en liste clients connus

Activé

Nombre de transactions acceptées

Nombre de transactions 3DSecure

Ancienneté mois

Fonctionnement des listes

Lorsqu'une transaction est initiée, le module va déterminer dans un premier temps l'appartenance éventuelle d'un ou plusieurs éléments de cette transaction à la liste blanche, noire ou grise et appliquer les règles d'une de ces listes le cas échéant. La liste blanche prime sur la liste noire qui prime sur la liste grise. Par exemple, si une carte bancaire est en liste noire mais qu'elle est utilisée par un identifiant acheteur en liste blanche, nous appliquerons les règles de la liste blanche.

Si aucune appartenance à ces trois listes n'est détectée, le module va alors déterminer s'il s'agit d'une transaction effectuée par un nouveau client ou par un client connu (identifiant acheteur en liste Nouveaux clients ou Standard). Le module contrôle alors la transaction avec l'ensemble des règles paramétrées pour la liste identifiée.

Exemple : un client sans historique sera soumis aux règles de la liste des nouveaux clients. Toutefois, s'il se connecte d'une adresse IP que vous avez mise en liste grise, la transaction sera alors soumise aux règles de la liste grise.



L'**identifiant acheteur** (customerId) est un élément indispensable à faire passer dans les web services pour pouvoir utiliser le module LCLF efficacement. Dans ce document nous considérerons que cette information est passée à Monext.

Si vous ne passez pas d'identifiant acheteur, la transaction sera évaluée par les règles de la liste Standard (clients connus).

La liste des Nouveaux clients

Tout nouveau client sera soumis aux règles de cette liste si aucun élément de la transaction (IP, carte, domaine email, etc.) n'appartient à la liste blanche, grise ou noire. Vos règles doivent être relativement strictes pour cette liste puisque les fraudeurs sont le plus souvent des clients sans historique. Attention toutefois à ceux qui font "mûrir" des comptes à coups de petits paiements légitimes avant de commettre des fraudes.

La liste Standard

Dans cette liste se trouveront vos clients connus, donc présentant un risque de fraude moindre. Le module LCLF vous laisse définir les critères d'ancienneté et de nombre de transactions qui feront qu'un client passera de la liste nouveaux clients à la liste standard. Cette fonction est disponible dans le menu *Configuration* et expliquée ici.

La liste Blanche

La liste blanche est la liste pour laquelle vos règles fraude sont les plus souples. Vous y mettez vos clients de confiance afin de leur faciliter l'achat. Certains marchands n'appliquent aucun filtre à cette liste. Cela nécessite alors de n'y mettre que des clients en lesquels vous avez totalement confiance. Il conviendra toutefois de s'assurer que leur compte n'a pas été piraté.

La liste Grise

La liste grise permet de recenser plusieurs types d'éléments à risque auxquels vous souhaitez toujours appliquer des contrôles fraude. Idéalement, vous devez paramétrer votre liste grise pour demander une authentification 3D-Secure pour les transactions en carte bancaires (par opposition aux demandes d'authentification passive dite "frictionless").



Fraude 3DSecure

Notez que si demander une authentification 3DSecure vous garantit contre les impayés, cela ne vous prémunit pas des fraudes. En effet, les techniques de manipulation des porteurs de cartes qui leur permettent d'obtenir des authentifications fortes avec la carte de leur victime, pour des sommes souvent très élevées, se sont répandues dans la "communauté" des escrocs. L'authentification forte à deux facteurs n'est donc en rien une garantie d'absence de fraude.

La liste Noire

La liste noire est la plus stricte : toute transaction faite avec un élément de la liste noire sera refusée.

Éléments que vous pouvez ajouter dans les listes

Le tableau ci-dessous liste les critères qui sont analysés pour déterminer l'appartenance à une liste.

| Critère | Liste Blanche | Liste Grise | Liste Noire |
|----------------------------------|---------------|-------------|-------------|
| Identifiant client | ✓ | ✓ | ✓ |
| Numéro de carte bancaire | | ✓ | ✓ |
| Compte acheteur (Paypal, Skrill) | | ✓ | ✓ |
| Adresse IP | ✓ | ✓ | ✓ |
| Plage de BIN | | ✓ | ✓ |
| Type de carte | | ✓ | ✓ |
| Plage d'adresses IP | ✓ | ✓ | ✓ |
| Adresse email | | ✓ | ✓ |
| Numéro de téléphone | | ✓ | ✓ |
| Pays du client (= pays de l'IP) | | ✓ | ✓ |
| Pays émetteur de la carte | | ✓ | ✓ |
| Domaine de l'adresse email | | ✓ | ✓ |
| Nom du client | | ✓ | ✓ |

Rappel de l'ordre des priorités : **liste blanche > liste noire > liste grise**. La logique est donc la suivante :

- si une transaction contient des éléments en liste blanche, ce sont les règles de la liste blanche qui seront appliquées, même si cette transaction contient aussi des éléments des listes noire ou grise.
- si une transaction contient des éléments en liste noire mais pas d'éléments en liste blanche, c'est la règle de la liste noire qui est appliquée (refus de la transaction), même si cette transaction contient aussi des éléments de la liste grise.

Ajouter un élément en liste

L'ajout en liste blanche, grise ou noire d'un élément se fait soit via le menu **Listes > Actions > Créer** (menu complet), soit via la page **Détail d'une transaction > Actions**. Les deux méthodes sont détaillées ci-dessous.



Notez que le module LCLF ne tient pas compte des majuscules et accents, cela afin de contrecarrer les fraudeurs qui reviennent avec des variantes simples de leur nom ou adresse email. Donc mettre bob@yopmail.com en liste noire permet aussi de bloquer BOB@yopmail.com. De même, Dupont et Dupoñt ne font plus qu'un. Ce principe s'applique aussi aux [règles génériques](#).

Via le menu Listes

Exemple : vous souhaitez ajouter le domaine d'adresse email yopmail.com en liste noire :

- sélectionnez la liste dans laquelle vous souhaitez ajouter l'élément
- sélectionnez le type d'élément *Domaine d'adresse email*
- renseignez l'élément *yopmail.com*
- affectez un motif à l'élément
- sélectionnez une date de sortie de liste. Si aucune date n'est renseignée, l'élément restera en liste indéfiniment (mais peut être supprimé manuellement si besoin)

- facultatif : laissez un commentaire
- Sauvegardez

Informations générales

Liste *
Noire

Type d'élément *
Domaine de l'adresse email

Domaine de l'adresse email

Domaine de l'adresse email *
yopmail.com

Informations complémentaires

Motif *
DOM - Domaine d'adresse em... ⊕

Expire le 
Laisser vide si définitif

Commentaire

Un client se présentant alors avec une adresse email @yopmail.com verra sa transaction refusée (sauf si son identifiant ou adresse IP est en liste Blanche).

Via Détails d'une transaction

Depuis la page de détails d'une transaction, vous avez aussi la possibilité via le menu Actions en haut à droite de rapidement passer en liste grise ou noire les éléments suivants :

- Numéro de carte
- Identifiant acheteur (customerid)
- Adresse IP
- Numéro de téléphone portable
- Compte PayPal, Skrill, etc (= compte acheteur)

| Acheteur | Actions |
|-------------------------------|---------------------------|
| Bob Dit L'ane | |
| Actions de fraude | |
| Mettre la carte en liste | <u>Grise</u> <u>Noire</u> |
| Mettre l'ID acheteur en liste | <u>Grise</u> <u>Noire</u> |
| Mettre l'IP en liste | <u>Grise</u> <u>Noire</u> |
| Mettre le téléphone en liste | <u>Grise</u> <u>Noire</u> |

La liste proposée est dynamique : si vous ne passez pas de numéro de téléphone dans le champ mobile.phone, l'option "Mettre le téléphone en liste" sera absente.

Règles

! IMPORTANT

Avec la nouvelle mouture du module de lutte contre la fraude (LCLF) la manière de gérer vos règles change : **la notion de règle par défaut n'existe plus**. Ce fonctionnement était un héritage des évolutions successives de l'outil et posait plus de problèmes qu'il n'en évitait.

Dorénavant, lors de la création d'une règle, vous affectez celle-ci aux listes que vous souhaitez, comme ici :

Informations générales

● Actif

1 liste *

Standard

Grise

Nouveaux clients

Blanche

Règle composante n° 1

Type *

Vous pouvez aussi visualiser l'ensemble de vos règles sur un même écran. Et si vous avez construit une règle complexe que vous souhaitez dupliquer sans avoir à tout refaire, c'est possible!

De même **la notion de règle composée n'existe plus** : lorsque vous construisez une règle vous pouvez utiliser une ou plusieurs règles, sans avoir à indiquer que vous souhaitez faire une "règle composée". Cette notion était aussi le résultat des évolutions de l'outil qui au départ ne proposait pas la possibilité de combiner des règles. Rappel : si vous êtes sur la version gratuite, vous ne pourrez pas combiner plusieurs règles en une seule.

Notez que les règles que vous configurez pour la liste Standard sont celles qui seront appliquées aux clients connus, c'est-à-dire qui ont déjà effectué plus de X transactions et/ou existent depuis X mois, selon les paramètres que vous aurez définis [ici](#).

Actions possibles

Pour la majorité des règles les actions suivantes sont disponibles :

- **Demander une authentification forte** : une authentification forte sera demandée à la banque de l'acheteur via le challenge indicator 03 du protocole 3DSv2 (EMV 3DS). Attention, la banque peut tout de même choisir de faire une authentification passive.
- **Refuser la transaction** : le paiement est refusé catégoriquement
- **Aucune action** : la règle n'a aucun impact sur le paiement mais vous permet de tester une règle avant de lui attribuer une action 3DS ou refus. Elle vous permet aussi de faire de la surveillance via les alertes de déclenchement d'une règle sans impacter le parcours client.
- **Pas de préférence** : le commerçant indique à l'émetteur (la banque de l'acheteur) qu'il ne se positionne pas concernant l'évaluation du risque (challenge indicator 01)
- **Exiger une authentification forte** : le commerçant indique à l'émetteur qu'une authentification forte est requise pour se conformer à la DSP2, par exemple dans le cas d'une première échéance de paiement récurrent (challenge indicator 04)
- **Suggérer une authentification sans friction** : le commerçant indique à l'émetteur qu'il ne considère pas la transaction comme à risque (challenge indicator 02) et souhaiterait une authentification passive (frictionless). Attention, dans le cas où l'émetteur accepte de ne pas faire d'authentification forte, les règles de transfert de responsabilité diffèrent selon que la transaction est passée par le réseau Visa, Mastercard ou CB.



REMARQUE : avant l'entrée en vigueur de la DSP2, l'outil LCLF permettait de router vers 3DS les transactions pour lesquelles vous ne souhaitiez pas prendre la responsabilité en cas de fraude. Vous appeliez un contrat VAD et le module LCLF routait la transaction vers un contrat VADS (S pour Secure) si besoin, en fonction des règles que vous aviez définies. Sinon la transaction poursuivait son chemin en autorisation simple (contrat VAD).

Aujourd'hui, toutes les transactions dans le périmètre DSP2 doivent passer par l'authentification 3DS, mais certaines peuvent bénéficier d'une exemption d'authentification forte. C'est ce que l'on appelle une authentification sans friction (frictionless ou FR), que permet le nouveau standard EMV 3DS, plus communément appelé 3DSv2.

Nous avons donc adapté le module LCLF pour vous permettre de demander une exemption d'authentification forte via l'action **Suggérer une authentification sans friction** : comme auparavant, vous appelez un contrat VAD puis le module LCLF redirige la transaction sur un contrat VADS avec un indicateur de choix commerçant concernant le type d'authentification souhaité, le "challenge indicator" mentionné plus haut.

Il est aussi possible d'appeler directement un contrat VADS tout en gérant les indicateurs de challenge 3DSv2 via vos règles LCLF. Cela vous évite alors de doubler chaque contrat VAD par son pendant VADS.

Périmètre d'une règle

De nombreux commerçants utilisent des configurations multi-points de vente et multi-contrats. Le module de gestion des risques de fraude prend en compte ce besoin en permettant un paramétrage spécifique des règles par point de vente et par contrat. Si vous ne sélectionnez pas de point de vente ou contrat particulier lors de la construction d'une règle, celle-ci s'appliquera à l'ensemble des transactions de votre compte commerçant.



IMPORTANT : une règle LCLF dont l'action serait 3D-Secure ne déclenchera aucune action dans le cas d'un paiement non-compatible avec 3D-Secure, tel que PayPal, 3XCB ou encore Paysafecard. Il est donc inutile de faire une sélection qui exclurait ces moyens de paiement.

Si vous souhaitez par exemple appliquer une règle 3D-Secure à un point de vente auquel seraient rattachés des contrats Carte et des contrats PayPal, il vous suffit de sélectionner le point de vente. A l'opposé, si vous faites une règle de refus que vous ne voulez appliquer qu'à certains moyens de paiement, il vous faut sélectionner les **contrats** associés à ces moyens de paiement.

Règles

Le module LCLF vous propose des règles aux logiques prédéfinies mais dont vous devrez généralement configurer les seuils que vous souhaitez. Par exemple, pour la règle Cumul client, vous devez choisir un montant d'achats cumulés ainsi que la période sur laquelle vous souhaitez que ce cumul soit calculé.

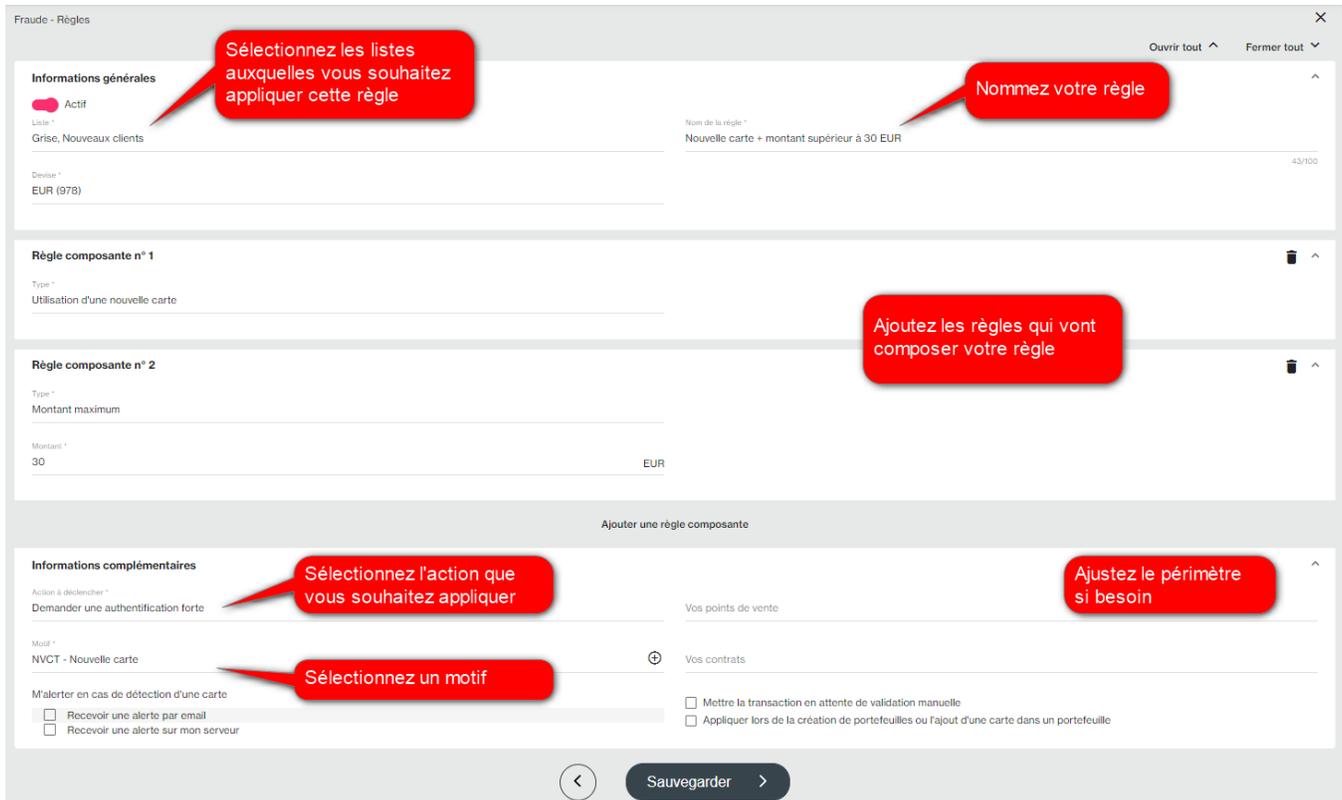
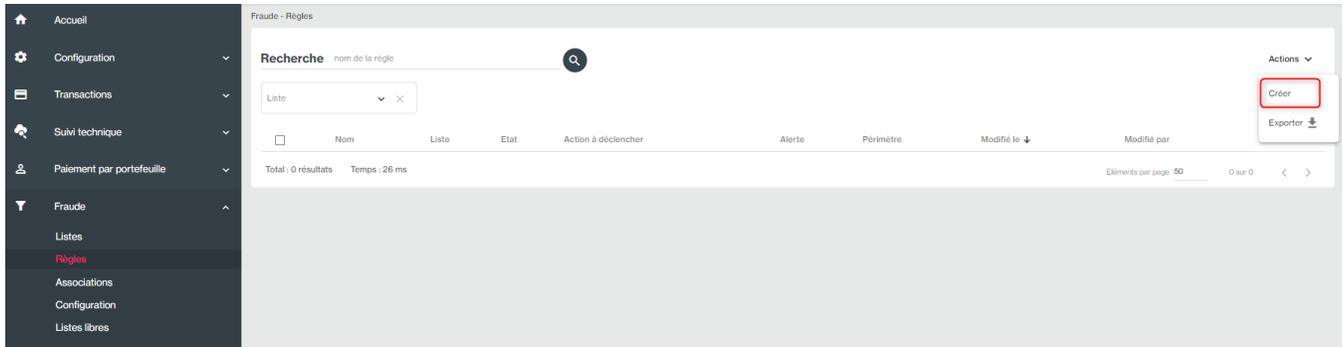
Les règles sont les suivantes :

| Nom de la règle | Description |
|-----------------|--|
| Montant maximum | Se déclenche pour tout montant au-delà du seuil que vous avez fixé |
| Montant minimum | Se déclenche pour tout montant en-deçà du seuil que vous avez fixé |

| | |
|---|---|
| Cumul client | Contrôle le montant cumulé des transactions que vous autorisez par client sur une période* Se déclenche si la transaction en cours ferait que le seuil que vous avez fixé sera atteint ou dépassé |
| Vélocité client | Contrôle le nombre maximum de transactions que vous autorisez par client sur une période* |
| Cumul moyen de paiement | Contrôle le montant cumulé des transactions que vous autorisez par moyen de paiement sur une période Se déclenche si la transaction en cours ferait que le seuil que vous avez fixé sera atteint ou dépassé |
| Vélocité moyen de paiement | Contrôle le nombre maximum de transactions que vous autorisez par moyen de paiement sur une période |
| Cumul IP | Contrôle le montant cumulé des transactions que vous autorisez par adresse IP sur une période Se déclenche si la transaction en cours ferait que le seuil que vous avez fixé sera atteint ou dépassé |
| Vélocité IP | Contrôle le nombre maximum de transactions que vous autorisez par adresse IP sur une période |
| Cumul numéro de téléphone portable | Contrôle le montant cumulé des transactions que vous autorisez par numéro de téléphone portable sur une période Se déclenche si la transaction en cours ferait que le seuil que vous avez fixé sera atteint ou dépassé |
| Vélocité numéro de téléphone portable | Contrôle le nombre maximum de transactions que vous autorisez par numéro de téléphone portable sur une période |
| Résultat 3DSecure | Contrôle le résultat de l'authentification 3DSecure afin de refuser certains cas de figure |
| Gestion des cartes virtuelles | Déclenche une action sur les transactions par cartes identifiées comme virtuelles ou non-virtuelles |
| Pays de l'adresse IP | Déclenche une action en fonction du pays de l'adresse IP |
| Pays émetteur du moyen de paiement | Déclenche une action en fonction du pays du moyen de paiement |
| Nombre de cartes acceptées par client | Contrôle le nombre de cartes de paiement que vous autorisez par client sur une période |
| Nombre de comptes ewallet ou bancaire acceptés par client | Contrôle le nombre de comptes de type PayPal ou bancaire que vous autorisez par client sur une période |
| Nombre de clients acceptés par carte | Contrôle le nombre de clients que vous autorisez à utiliser une même carte de paiement sur une période* |
| Nombre de clients acceptés par compte ewallet ou bancaire | Contrôle le nombre de clients que vous autorisez à utiliser un même compte de type PayPal ou bancaire* |
| Nombre de client par numéro de téléphone portable | Contrôle le nombre de clients que vous autorisez à utiliser un même numéro de téléphone portable sur une période* |
| Plage horaire risquée | Déclenche une action si la transaction a lieu dans une plage horaire définie |
| Contrôle pays transaction/émetteur du moyen de paiement | Déclenche une action si le pays de la carte est différent du pays de l'adresse IP |
| Ancienneté du compte client | Déclenche une action en fonction de l'âge du compte du client |
| Nouvelle carte | Déclenche une action à chaque fois qu'un client (=identifiant client) tente d'utiliser une nouvelle carte |
| Média de paiement | Déclenche une action en fonction du type d'appareil (mobile, ordinateur) utilisé par le client |
| Mise en quarantaine | En cas d'échec du fait d'une règle LCLF, les éléments de la transaction sont mis en quarantaine |
| AVS | Contrôle l'adresse de facturation (cartes UK, CA et US seulement) |
| Listes libres | Utiliser une liste libre |

* Le module LCLF fait abstraction de la casse lorsque vous passez une adresse email dans le champ identifiant acheteur (customerId), ce qui permet de stopper les fraudeurs qui utiliseraient des variantes de leur adresse email pour contourner les seuils de déclenchement. Donc, si un client fait une première transaction avec l'adresse email bob@email.com puis une deuxième avec BoB@email.com et que vous passez ces adresses dans le champ identifiant client, le module LCLF enregistrera deux transactions pour l'identifiant client normalisé bob@email.com. Il en va de même pour les différentes cartes bancaires ou comptes e-wallet (PayPal) qui seront associés à l'identifiant client.

Créer une règle



Règles génériques

Les règles dites génériques permettent de contrôler des champs des web services tels que les adresses email, le code postal de livraison, le nombre de commandes à date (order count) ou encore des données privées à l'aide d'un champ comparateur.

Exemple tiré d'un cas réel : un fraudeur ouvre de multiples comptes avec des adresses email toutes différentes mais qui contiennent toutes le mot 'zira'. Une règle générique peut alors être créée comme suit :

Si `buyer.email` contient `zira` alors demander une authentification 3D-Secure

D'une manière générale, les règles génériques vous permettent aussi un contrôle plus fin que via la mise en liste grise ou noire. Par exemple, plutôt que de mettre le domaine email `clipmail.eu` en liste noire, ce qui déclencherait un refus systématique de la transaction, vous pouvez créer une règle qui ne se déclencherait que si d'autres conditions sont remplies (montant, ancienneté, etc.).

Remarque : si vous avez besoin de faire de tels contrôles sur plusieurs éléments, il est préférable d'utiliser la fonctionnalité **Listes libres** détaillée plus bas si le type d'élément à contrôler est pris en charge par cette fonctionnalité.

Notez que les contrôles font dorénavant abstraction de la casse et des accents (Bob = BOB = bôb)

Listes libres

Les listes libres sont une fonctionnalité qui vous permet de **constituer des listes d'éléments** (adresse IP, domaines d'adresses email, codes postaux...) que vous pouvez ensuite utiliser comme condition dans des règles fraude.

Cette fonctionnalité offre **plus de souplesse et de possibilités** que les listes grise et noire. Par exemple, plutôt que mettre des adresses IP en liste grise et ainsi affecter tous les clients qui utiliseraient ces adresses IP, vous pouvez constituer une liste de ces IPs puis la combiner à d'autres conditions telles qu'un seuil de montant ou l'ancienneté du compte.

De même, elle peuvent remplacer avantageusement les règles génériques, qui ne permettent d'agir que sur un élément à la fois. Ainsi, au lieu de faire 10 règles pour 10 domaines d'adresses email, par exemple, une seule liste libre suffira.

Vous pouvez aussi mettre en liste des éléments partiels grâce au système « wildcard ». Par exemple :

- 13* pour le département des Bouches du Rhône
- *123@gmx.fr pour toutes les adresses email se terminant par 123@gmx.fr
- *yopmail* pour les adresses email utilisant les domaines yopmail.com et yopmail.fr

La fonctionnalité Listes libres ne tient pas compte des accents ni des majuscules. Il n'est donc pas nécessaire d'enregistrer les variantes d'un même élément.

Créer une liste

Fraude > Listes libres > Créer une nouvelle liste libre



Cliquez sur **Créer une nouvelle liste libre** :

Veillez choisir le type de la liste libre

- Créer une nouvelle liste libre
- Créer une nouvelle liste composée



Un menu apparait contenant des sous-menus :

| | |
|--------------------------|---|
| Client | ▼ |
| Moyen de paiement | ▼ |
| Email | ▼ |
| Livraison | ▼ |
| Connexion | ▼ |
| Commande | ▼ |

Le menu Client, par exemple, permet de constituer des listes d'identifiants client, d'identifiants de comptes PayPal (= compte acheteur), de noms de famille ou de numéros de portables :

| | |
|----------------------------|---|
| Client | ▲ |
| Compte acheteur | |
| Identifiant client | |
| Nom de famille du client | |
| Numéro de téléphone mobile | |

Créons une liste de domaines d'adresses email. Pour cela, sélectionnez le menu Email puis entrez vos domaines sous la forme *@domaine :

Type : **Liste libre** Critère : **Adresse email**

Nom de la liste *

Domaines email - niveau 1

Description de la liste

Domaines d'adresse email à risque élevé

Contenu de la liste

- *@besttempmail.com
- *@jourrapide.com
- *@mailo.com
- *@newmail.top
- *@yopmail*

Votre liste est créée et apparait comme suit :

| Nom de la liste ↓ | Description de la liste | Type | Nombre d'éléments | |
|------------------------------|---|-------------|-------------------|---|
| Domaines email - niveau 1 | Domaines d'adresse email à risque élevé | Liste libre | 5 |   |
| Codes postaux - départements | Départements présentant un risque élevé | Liste libre | 3 |   |

Éléments par page 5 ▾ 1 - 2 sur 2 |< < > >|

Utiliser une liste

Une fois créées, vous trouverez vos listes libres dans la liste des règles disponibles. Dans l'exemple ci-dessous nous construisons une règle avec une liste libre de codes postaux et une règle de cumul sur le moyen de paiement. Cette règle déclenchera une demande d'authentification forte si la livraison se fait dans un des codes postaux de la liste et que le montant cumulé dépensé sur le moyen de paiement dépassera 90 EUR sur 3 jours si la transaction est acceptée.

Informations générales

Actif

Liste *
Nouveaux clients

Devise *
EUR (978)

Nom de la règle *
Codes postaux à surveiller

26/100

Règle composante n° 1

Type *
Liste libre

Liste libre *
Codes postaux

Règle composante n° 2

Type *
Cumul moyen de paiement

Montant maximum cumulé des transactions *
90 EUR

Durée *
3

Unité *
Jour(s)

Ajouter une règle composante

Informations complémentaires

Action à déclencher *
Demander une authentification forte

Vos points de vente

Mises en liste automatiques

Le module de lutte contre la fraude Payline offre une fonction permettant de faire passer automatiquement en liste grise ou noire certains éléments d'une transaction en fonction du code retour de la banque ainsi que sur réception d'un avis de mise en opposition d'une carte. Cette fonction non-seulement soulage vos équipes fraude mais permet aussi une action instantanée : lors de sa tentative suivante, le client sera soumis aux règles de la liste choisie (grise ou noire).

Mise en liste sur code retour de la banque

 Menu : Fraude > Configuration > Mettre en liste automatique à partir du code retour banque

Dans l'exemple ci-dessous, si une transaction retourne un code Carte volée (code 1209) ou Carte perdue (1208), l'identifiant client ainsi que l'adresse IP seront passés en liste grise pour une période de 90 jours sauf si cet identifiant est en liste blanche. Toutes les transactions suivantes avec le même identifiant client ou la même adresse IP sur une période de 90 jours seront alors soumises aux règles de la liste grise.

Mettre en liste automatique à partir du code retour banque

Activé Mettre la transaction en attente de validation manuelle ?

Lorsqu'une transaction est refusée pour les raisons suivantes

- Carte inactive (01125)
- Carte contrefaite (01129)
- Fraude suspectée (01202)
- Carte perdue (01208)
- Carte volée (01209)

Exclure les cas suivants

- La carte utilisée pour le paiement est déjà enregistrée dans un portefeuille
- Le consommateur est en liste blanche

Ou lorsqu'une transaction

- Génère un impayé

Mettre les éléments suivants

- Identifiant client
- Nom du client
- Adresse mail du client
- Adresse IP du client
- Numéro de mobile du client

En liste

- Grise
- Noire

Pour une durée

- Définitivement
- De 90 jour(s)

Mise en liste sur carte en opposition

Le module LCLF vous permet d'être alerté lorsqu'une carte du réseau CB utilisée récemment sur votre site est mise en opposition. Vous pouvez aussi paramétrer cette fonction pour que l'identifiant client soit automatiquement mis en liste grise.

 Menu: Fraude > Configuration > Configurer les alertes de mise en opposition

Dans l'exemple ci-dessous, si nous recevons un avis de mise en opposition d'une carte utilisée dans les trois derniers jours sur votre site, vous recevrez une alerte par email et l'identifiant client sera mis en liste grise pour 90 jours si cet identifiant appartient à la liste Nouveaux clients. Le motif attribué est "Carte en opposition".

Notez que la fonctionnalité de Device Fingerprinting n'est plus disponible sur Monext Online.

Configurer les alertes de mise en opposition ?

Rechercher dans les transactions des derniers jour(s)

Mettre en liste grise

L'identifiant client
 Le Device Fingerprint

M'alerter en cas de détection d'une carte

Recevoir une alerte par email
 Recevoir une alerte sur mon serveur

Pour les clients appartenant aux listes

Clients connus
 Nouveaux clients
 Blanche

Pour une durée

Définitivement
 De jour(s)

! IMPORTANT : ces alertes n'indiquent pas une opposition sur la transaction. L'information que nous recevons des banques est uniquement que la carte vient d'être mise en opposition.
Notez que ces alertes ne fonctionnent que pour les cartes du réseau Cartes Bancaires, donc des cartes de banques françaises affiliées au réseau CB.

Les alertes de mise en opposition vous seront très utiles pour détecter d'éventuelles fraudes, en particulier avec des transactions authentifiées 3DS. En effet, l'absence d'impayé ne signifie pas que vous n'avez pas de fraude et ces alertes peuvent vous permettre de vous en apercevoir. Exemple ici avec une transaction de 350 EUR, montant élevé pour le site concerné : la carte a été mise en opposition moins de 30 minutes après la transaction, ce qui laisse penser que cette transaction n'était pas autorisée (c'est le cas).

| | |
|-----------------------------------|---------------------------------|
| N° de l'alerte | 52XXX |
| Raison de l'alerte | Carte mise en opposition |
| Date de mise en opposition | 26/08/2021 11:12:00 |
| ID Transaction | 122XXX |
| Montant | 350,00 EUR |
| Date | 26/08/21 10:44 |
| État de la transaction | ACCEPTÉ |
| Niveau de sécurité | Avec CVV, Avec 3DSecure |

Motifs

Les motifs permettent d'identifier facilement la raison d'un déclenchement d'une règle LCLF, en particulier dans les emails d'alerte. Ils peuvent être attribués aux règles ainsi qu'aux éléments mis en liste. C'est vous qui les nommez.

Un motif est composé d'un Nom, d'un message et d'une description. Cette dernière n'apparaît que sur l'écran de configuration des motifs et ne sert qu'à éventuellement fournir plus d'information sur le motif.

i Menu : Fraude > Configuration > Configurer les motifs

Exemple de motif:

The screenshot shows a web interface for configuring patterns. On the left, a 'Recherche' (Search) sidebar contains several filter options, each with a checkbox: 'Nom ↑', '3DS', '@DOM', 'ART', 'CLT', and 'IP'. The 'CLT' option is selected. The main area is titled 'Créer un motif' (Create a pattern) and contains three input fields:

- Nom *** (Name): CLTMOB | 6/ (character count)
- Message *** (Message): Nombre de clients par numéro de portable | 40/11 (character count)
- Description *** (Description): Nombre de clients par numéro de portable | 40/2 (character count)

Notez qu'il existe un motif par défaut, appliqué si vous n'avez pas défini de motif personnalisé :

- Code : PAY001
- Message court : **Fraude suspectée**
- Message long : La transaction a été détectée comme frauduleuse

Les autres motifs prédéfinis sont **les suivants** :

- **Mise en liste automatique**, affecté aux éléments mis en liste automatiquement suite à un code retour bancaire de type carte perdue, carte volée, etc.
- **Carte en opposition**, affecté aux éléments mis en liste automatiquement suite à une alerte de mise en opposition d'une carte

[LCLF - Présentation du module anti-fraude#Sommaire](#)

Alertes

Le module LCLF vous permet de recevoir des alertes par email ou notification serveur dans les cas suivants :

- déclenchement d'une règle.
- transaction passée par la liste noire
- avis de mise en opposition d'une carte du réseau CB

Les alertes sont particulièrement utiles dans les cas suivants :

- vous souhaitez surveiller un comportement en particulier sans nécessairement appliquer d'action automatique sur la transaction > créez une règle sans action mais avec alerte et vous serez alors notifié lorsqu'une transaction correspond à vos critères d'alerte. Par exemple, nouveau compte avec adresse email @gmx.fr et montant supérieur à 500 EUR
- vous souhaitez tester une règle et en mesurer son impact
- vous souhaitez être alerté en cas de mise en opposition d'une carte utilisée récemment sur votre site

Configurer les destinataires

Pour utiliser les alertes, vous devrez commencer par sélectionner le type d'alerte que vous souhaitez puis ajouter soit une url pour des notifications serveur, soit une ou plusieurs adresses email. Le séparateur des emails est le point-virgule. Pas d'espaces. Maximum 150 caractères.

Dans l'exemple ci-dessous, nous avons choisi de recevoir les alertes par email à l'adresse david.ledru[at]monext.net.

Configurer les alertes

Recevoir les alertes sur mon serveur

URL de notification

Recevoir les alertes par email

Destinataire(s) des emails

david.ledru@monext.net

Si plusieurs, séparés par des point-virgules.

Activer les alertes pour les règles

Ensuite vous choisissez d'activer une alerte pour chaque règle et fonctionnalité. L'écran d'édition de chaque règle vous propose l'option :

Informations complémentaires

Action à déclencher *

Demander une authentification forte

Motif *

POST - Codes postaux à surveiller

Générer une alerte

Pour les alertes sur les transactions passant par la liste noire, c'est un paramétrage via le menu Fraude > Configuration > Configurer les actions globales des listes

Configurer les actions globales des listes

Liste *

Noire

Action à déclencher

Refuser la transaction



Générer une alerte

Et pour les mises en opposition, c'est ici :

Configurer les alertes de mise en opposition ?

Rechercher dans les transactions des derniers 3 jour(s)

Mettre en liste grise

L'identifiant client

Le Device Fingerprint

Pour les clients appartenant aux listes

Clients connus

Nouveaux clients

Blanche

Pour une durée

Définitivement

De jour(s)



Générer une alerte

Alerte par email

L'email que vous recevez contient les tableaux suivants :

- Un résumé de la transaction avec un lien sur le numéro de transaction vers la page Détail d'une transaction
- Les règles déclenchées
- L'historique sur 7 jours, limité à 20 lignes, du client, du moyen de paiement et de l'adresse IP

| | |
|---------------------------|--|
| N° de l'alerte | 53602603 |
| Raison de l'alerte | Nombre de clients par numéro de portable (CLPH) |

| | |
|---------------------------|----------------|
| Commerçant | YELLO INC. |
| Point de vente | Titi.fr |
| Référence commande | 80904069 |

| | |
|-------------------------------|----------------------------------|
| ID Transaction | LF00008960327053 |
| Montant | 551,95 EUR |
| Date | 03/01/20 10:23 |
| Niveau de sécurité | Avec CVV, Sans 3DSecure |
| État de la transaction | REFUSE |

| | |
|--------------------------|--------------------------------|
| Moyen de paiement | CB |
| Données porteur | FRA 4974XXXXXXXXX0288 |
| Nom du porteur | Non renseigné |
| Adresse IP | FRA 213.123.213.123 |

| | |
|----------------------|--|
| Nom du client | Bobby McScam |
| ID client | TIFR2531 |
| Adresse email | bobby123@disposamail.fr |

ALERTES DÉCLENCHÉES

| Alerte | Raison de l'alerte | Règle | Code | Action |
|----------|--|---|------|------------------------|
| 53602593 | Testeurs de cartes | Testeurs de cartes - REFUS | TCT | Refuser la transaction |
| 53602603 | Nombre de clients par numéro de portable | Nombre de clients refusés par numéro de portable = 1 sur 30 jours | CLPH | Refuser la transaction |

HISTORIQUE DES 7 DERNIERS JOURS

Historique du **consommateur** :

| Id transaction | Réf. Commande | Moyen de paiement | Date transaction | Montant | Etat | Point de vente |
|------------------|---------------|------------------------|------------------|------------|--------|----------------|
| LF00008960327053 | 80904069 | CB - 4974XXXXXXXXX0288 | 03/01/20 10:23 | 551.95 EUR | REFUSE | Titi.fr |
| 10003102117417 | 80902686 | CB - 4200XXXXXXXXX8268 | 03/01/20 10:21 | 551.95 EUR | REFUSE | Titi.fr |
| 10003101849556 | 80902484 | CB - 5272XXXXXXXXX5871 | 03/01/20 10:18 | 551.95 EUR | REFUSE | Titi.fr |

Historique du **moyen de paiement** :

| Id transaction | Réf. Commande | Consommateur | Email client | Date transaction | Montant | Etat | Point de vente |
|------------------|---------------|-------------------------|-------------------------|------------------|------------|--------|----------------|
| LF00008960327053 | 80904069 | Bobby McScam - TIFR2531 | bobby123@disposamail.fr | 03/01/20 10:23 | 551.95 EUR | REFUSE | MICR |

Historique de l'**adresse IP** :

| Id transaction | Réf. Commande | Consommateur | Email client | Moyen de paiement | Date transaction | Montant | Etat |
|------------------|---------------|-------------------------|-------------------------|------------------------|------------------|------------|--------|
| LF00008960327053 | 80904069 | Bobby McScam - TIFR2531 | bobby123@disposamail.fr | CB - 4974XXXXXXXXX0288 | 03/01/20 10:23 | 551.95 EUR | REFUSE |
| 10003102117417 | 80902167 | Tiff Tondou - TIFR2530 | bob321@tempmail.com | CB - 4200XXXXXXXXX8212 | 03/01/20 10:01 | 551.95 EUR | REFUSE |
| 10003101849556 | 80902036 | Bobba X - TIFR2528 | bobba@fete.net | CB - 5272XXXXXXXXX5123 | 03/01/20 09:58 | 551.95 EUR | REFUSE |

Alertes par notifications serveur « getAlertDetails »

Lorsque que le module anti-fraude enverra une alerte suite à une fraude détectée lors du contrôle de la règle concernée, Monext Online appellera l'URL de notification configurée par le commerçant et lui communiquera l'identifiant de l'alerte. Cet identifiant permettra de faire appel à ce nouveau web service afin d'aller récupérer toutes les informations relatives à l'alerte. L'utilisation ainsi que le détail des informations remontées par ce web service sont décrits dans la documentation « Descriptif des appels webservices de la solution de paiement Monext Online » et disponibles en annexe de ce document.

[LCLF - Présentation du module anti-fraude#Sommaire](#)

Détail d'une transaction

Sur la page Détail d'une transaction sur le centre d'administration, il est possible de visualiser les différentes informations liées à la lutte contre la fraude. Un code retour **04002** dans le **pavé ÉTAT** vous informe que la transaction a été refusée suite à un déclenchement d'une règle fraude. Ce code apparaîtra si la transaction a déclenché une règle de refus ou si elle a déclenché une règle 3D-Secure et que le client ne s'est pas authentifié.

Etat

| | |
|-------------------|----------------|
| Code retour | 04002 |
| Message | Fraud detected |
| Partenaire | GTM |
| Moyen de paiement | CB |

Le pavé **FRAUDE** permet de voir rapidement si une règle s'est déclenchée. Cette zone affiche :

- l'une des règles déclenchées
- la liste dans laquelle se trouve la transaction
- le motif correspondant à la règle déclenchée

Fraude

| | |
|--------------------|------------------------|
| Fraude possible | Oui |
| Action finale | Refuser la transaction |
| Motif de la fraude | mobile à risque |
| Liste | Liste noire |
| Règle déclenchée | Numéro de téléphone |

[Plus de détails](#)

Le lien **Plus de détails** ouvre un pop-up affichant toutes les informations renvoyées par le module de lutte contre la fraude. Ce pop-up contient les informations suivantes :

- L'appartenance ou non de chaque élément de la transaction à une liste
- Le résultat de toutes les règles exécutées sur la transaction
- Les temps de traitement de chaque règle