LCLF - Guide pratique des règles LCLF

Contenu

Guide pratique des règles LCLF

PRÉCISION UTILE : le module LCLF ne fait pas de distinction dans les champs texte entre les minuscules et les majuscules.

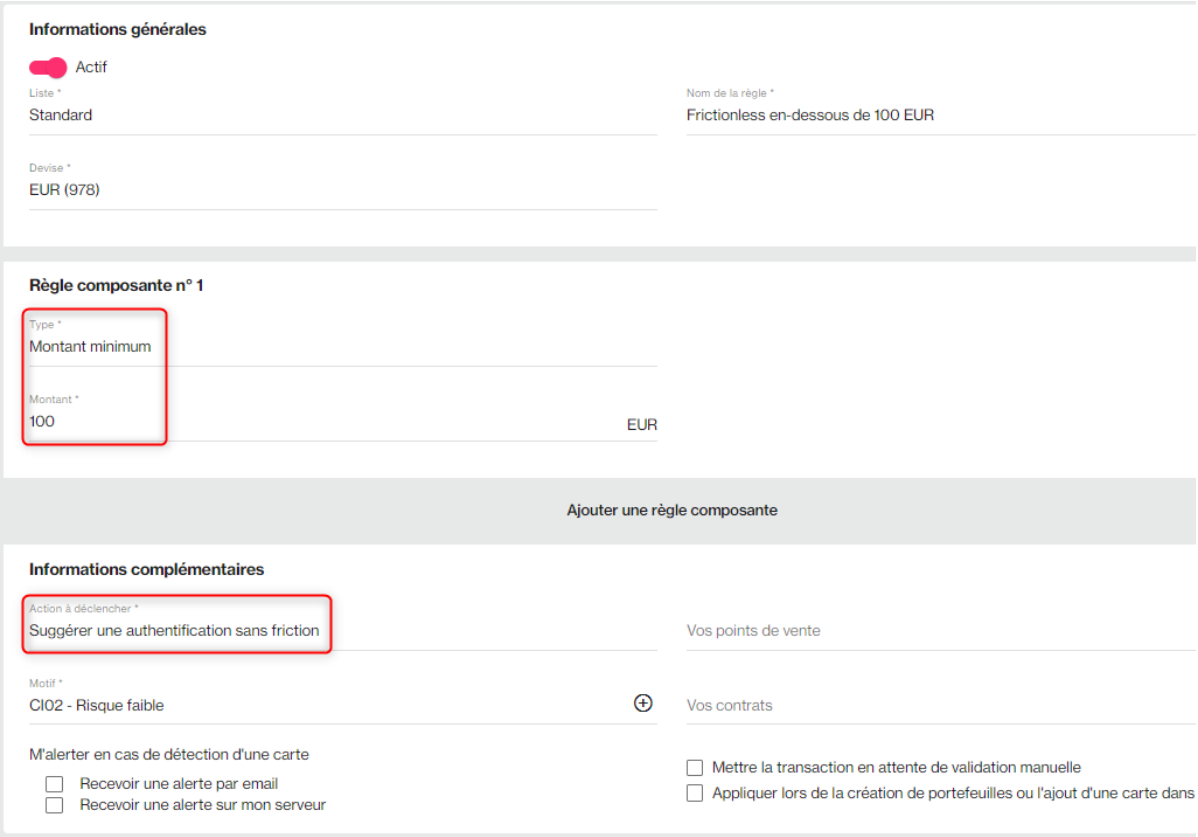
RAPPEL : plusieurs règles ne fonctionnent que si vous transmettez à Payline un identifiant client. A défaut d'une référence propre, celui-ci peut être l'adresse email du client, que vous ferez alors passer dans le champ prévu pour l'identifiant client en plus du champ email. Attention toutefois aux changements d'adresse email : notre système ne reconnaitrait alors plus le compte client et le traiterait comme un nouveau client.

Montant maximum

Cette règle permet de déclencher une action si le montant de la transaction est supérieur au montant configuré.

Montant minimum

Cette règle permet de déclencher une action si le montant de la transaction est inférieur au montant configuré. Vous pouvez vous en servir pour demander des exemptions d'authentification forte 3DSv2 pour vos transaction en dessous de X EUR.



Ancienneté du compte client

Cette règle permet de déclencher une action si l'âge du compte est inférieur au seuil choisi. Elle se combine de préférence avec d'autres règles comme montant maximum et/ou cumul client.
Exemple de règle:

- Si ancienneté < 30 jours et cumul client sur 30 jours > 200 EUR, alors déclencher 3DS

Nouvelle carte

Cette règle permet de déclencher une action lorsque le client tente d'utiliser une nouvelle carte. Elle peut s'avérer utile pour contrer la fraude par piratage de compte client; en effet, un fraudeur qui accéderait aux données de connexion d'un de vos clients n'utilisera pas nécessairement la carte de votre client pour passer commande. Il est d'ailleurs plus probable qu'il utilise une autre carte, qu'il aura testée au préalable.

De même, elle est utile pour contrer la fraude aux petits montants, qui impacte particulièrement les commerçants du secteur du jeu (paris sportifs, crédit de jeu pour consoles).

Gestion des cartes virtuelles

Cette règle permet de déclencher une action lorsque le client utilise une carte virtuelle ou, à l'inverse, une carte qui n'est pas virtuelle. Vous pouvez par exemple refuser un paiement par carte virtuelle pour un paiement en trois fois.

Bon à savoir : si vous demandez une authentification 3D-Secure pour une transaction en carte virtuelle, il n'y aura pas nécessairement d' authentification forte du porteur, certaines banques considérant que le fait de générer une carte virtuelle équivaut déjà à une authentification forte. En 3DSv2, l'authentification pourra indiquer A (=attempt) au lieu de Y (=yes) pour certaines cartes. Le transfert de responsabilité reste assuré dans un tel cas pour les cartes européennes.

Plage horaire risquée

Cette règle permet de déclencher une action si une transaction est faite à une heure jugée à risque. Les marchands l'utilisant définissent en général la plage 1h00 - 6h00 comme à risque élevé pour des secteurs d'activité comme l'habillement ou l'électronique.
Idéalement cette règle devrait être combinée à un montant maximum et une ancienneté de compte de façon à ne pas impacter tous les clients noctambules sans distinction.

Exemple de règle:

- Si transaction entre 1h00 et 6h00 et montant > 50 EUR et ancienneté < 30 jours, alors 3DS

Cumul client

Cette règle permet de déclencher une action si un client dépasse un montant cumulé de transactions acceptées sur une période donnée. Elle peut être combinée à la règle d'ancienneté du compte pour plus de finesse.
Note: dans tous les cas, il faut y ajouter une règle de vélocité client "nombre de transactions acceptées 1" sinon la règle se déclenche au premier achat si celui-ci est supérieur au montant défini.

Exemples de règles:

- Si montant cumulé sur compte client sur 3 jours > 200 EUR et nombre de transactions acceptées sur 3 jours 1 et ancienneté < 30 jours, alors déclencher 3DS
- Si montant cumulé sur compte client sur 2 heures > 500 EUR et nombre de transactions acceptées sur 2 heures 1 et ancienneté < 1 jour, alors refuser la transaction

Attention, cette règle nécessite l'utilisation d'un identifiant unique du client. Sans cette information, toutes les transactions seront systématiquement refusées !

Vélocité client

Cette règle permet de déclencher une action si un client dépasse un nombre de transactions sur une période donnée. Vous pouvez choisir de comptabiliser uniquement les transactions acceptées ou uniquement les refusées ou de toutes les comptabiliser. La règle peut être combinée à la règle d'ancienneté du compte pour plus de finesse.

Exemples de règles:

- Si nombre de transactions acceptées sur 3 jours 2 et ancienneté < 30 jours, alors déclencher 3DS
- Si nombre de transactions (toutes transactions) sur 1 heure 5 et ancienneté < 7 jours, alors refuser la transaction

Attention, cette règle nécessite l'utilisation d'un identifiant unique du client. Sans cette information, toutes les transactions seront systématiquement refusées !

Cumul device fingerprint - indisponible

Cette règle permet de déclencher une action si un même appareil - identifié par son "fingerprint" - dépasse un montant cumulé de transactions acceptées sur une période donnée.
Note: dans tous les cas, il faut y ajouter une règle de vélocité device fingerprint "nombre de transactions acceptées 1" sinon la règle se déclenche au premier achat si celui-ci est supérieur au montant défini.

Exemples de règles:

- Si montant cumulé sur un même appareil sur 3 jours > 200 EUR et nombre de transactions acceptées sur 3 jours 1, alors déclencher 3DS
- Si montant cumulé sur un même appareil sur 2 heures > 500 EUR et nombre de transactions acceptées sur 2 heures 1 et ancienneté du compte < 1 jour, alors refuser la transaction

Astuce : si vous utilisez aussi la règle de cumul client avec les mêmes seuils, alors nous vous recommandons d'ajouter la règle de Nombre de cartes par device fingerprint que vous paramétrez à 1 carte acceptée. Cela évitera les doubles déclenchements cumul client et cumul device fingerprint. De plus, le déclenchement de la règle ainsi paramétrée vous signalera qu'au moins deux cartes sont utilisées sur un même appareil, donc un risque potentiel plus élevé.

Attention, dans ce cas, il faut aussi vous protéger avec une règle de nombre de clients par carte.

Vélocité device fingerprint - indisponible

Cette règle permet de déclencher une action si un appareil dépasse un nombre de transactions sur une période donnée. Vous pouvez choisir de comptabiliser uniquement les transactions acceptées ou uniquement les refusées ou de toutes les comptabiliser.

Cumul moyen de paiement

Cette règle permet de déclencher une action si un moyen de paiement (une même carte par exemple) dépasse un montant donné de transactions acceptées sur une période donnée. Elle est particulièrement utile pour bloquer un fraudeur qui ouvrirait plusieurs comptes avec la même carte.

Note: dans tous les cas, il faut y ajouter une règle de vélocité moyen de paiement "nombre de transactions acceptées 1" sinon la règle se déclenche au premier achat si celui-ci est supérieur au montant défini.

Exemple de règle:

- Si montant cumulé sur 7 jours > 500 EUR et nombre de transactions acceptées 1, alors 3DS

Astuce : si vous utilisez aussi la règle de cumul client avec les mêmes seuils, alors nous vous recommandons d'ajouter la règle de Nombre de clients par carte que vous paramétrez à 1 client accepté. Cela évitera les doubles déclenchements cumul client et cumul carte. De plus, le déclenchement de la règle ainsi paramétrée vous signalera une carte utilisée par deux clients au moins, donc un risque potentiel plus élevé.

Vélocité moyen de paiement

Cette règle permet de déclencher une action si un moyen de paiement dépasse un nombre de transactions sur une période donnée. Vous pouvez choisir de comptabiliser uniquement les transactions acceptées ou uniquement les refusées ou de toutes les comptabiliser. Elle est particulièrement utile dans ces cas de figure :

- bloquer un fraudeur qui ouvrirait plusieurs comptes avec la même carte ;
  bloquer un fraudeur qui testerait différents montants pour trouver le seuil en dessous duquel 3DS ne serait pas appliqué.

Exemple de règle:

- Si nombre de transactions (toutes trans.) sur 1 heure 2, alors déclencher 3DS

Dans l'exemple ci-dessus, si le client est un fraudeur et passe sous votre montant maximum à la troisième tentative, il sera quand même soumis à 3DS.

Cumul IP

Cette règle permet de déclencher une action si un montant donné de transactions acceptées est dépassé sur une même adresse IP. Elle est particulièrement utile pour bloquer un fraudeur débutant ou peu habile qui ouvrirait plusieurs comptes sans changer son adresse IP.
Note: dans tous les cas, il faut y ajouter une règle de vélocité IP "nombre de transactions acceptées 1" sinon la règle se déclenche au premier achat si celui-ci est supérieur au montant défini.

Exemple de règle:

- Si montant cumulé sur 24 heures > 200 EUR et vélocité IP 1, alors déclencher 3DS

Vélocité IP

Cette règle permet de déclencher une action si un nombre de transactions sur une période donnée est dépassé sur une même IP. Vous pouvez choisir de comptabiliser uniquement les transactions acceptées ou uniquement les refusées ou de toutes les comptabiliser. Elle est particulièrement utile pour ces raisons :

- bloquer un fraudeur qui ouvrirait plusieurs comptes sans changer son IP ;
- bloquer un fraudeur qui testerait différents montants pour trouver le seuil en dessous duquel 3DS ne serait pas appliqué.

Exemple de règle:

- Si nombre de transactions (toutes transactions) sur 1 heure 2, alors déclencher 3DS

Dans l'exemple ci-dessus, si le client est un fraudeur et passe sous votre montant max à la troisième tentative, il sera quand même soumis à 3DS.

Cumul numéro de téléphone portable

Cette nouvelle règle (juillet 2018) permet de déclencher une action si le montant cumulé de transactions acceptées sur un même numéro de téléphone portable sur une période donnée dépasse un montant donné. Elle est particulièrement utile pour bloquer un fraudeur qui ouvrirait plusieurs comptes mais renseignerait toujours le même numéro.

Pour que cette règle fonctionne, le numéro de téléphone portable doit impérativement nous être envoyé via le champ dédié mobilePhone. Notez n'y a pas de contrôle de surface sur ce champ, donc 06 01 02 03 04 et +33 6 01 02 03 04 sont deux numéros distincts.

Note: dans tous les cas, il faut y ajouter une règle de vélocité numéro de téléphone portable "nombre de transactions acceptées = 1" sinon la règle se déclenche au premier achat si celui-ci est supérieur au montant défini.

Exemple de règle:

Si montant cumulé sur 7 jours > 500 EUR et nombre de transactions acceptées = 1, alors 3DS

> Si vous utilisez aussi la règle de cumul client avec les mêmes seuils, alors nous vous recommandons d'ajouter la règle de Nombre de clients par numéro de téléphone portable que vous paramétrez à 1 client accepté. Cela évitera les doubles déclenchements cumul client et cumul numéro de téléphone portable. De plus, le déclenchement de la règle ainsi paramétrée vous signalera un numéro de téléphone utilisé par deux clients au moins, donc un risque potentiel plus élevé.

Vélocité numéro de téléphone portable

Cette règle permet de déclencher une action si le nombre de transactions sur un numéro de téléphone portable sur une période donnée dépasse un seuil que vous aurez fixé. Vous pouvez choisir de comptabiliser uniquement les transactions acceptées ou uniquement les refusées ou de toutes les comptabiliser.

Pour que cette règle fonctionne, le numéro de téléphone portable doit impérativement nous être envoyé via le champ dédié mobilePhone. Notez n'y a pas de contrôle de surface sur ce champ, donc 06 01 02 03 04 et +33 6 01 02 03 04 sont deux numéros distincts.

Contrôle pays transaction/émetteur du moyen de paiement

Cette règle permet de déclencher une action si le pays de la carte et le pays de l'IP sont différents. Vous pouvez la compléter par les règles de pays de la carte et de l'adresse IP (voir plus bas) de façon à exclure les transactions avec une carte ou IP du pays de vente.
Exemple de règle pour un site expédiant seulement en Espagne :

- Si pays de l'adresse IP pays de la carte et pays de l'adresse IP Espagne et pays de la carte Espagne, alors déclencher 3DS

Nombre de cartes par client

Cette règle permet de déclencher une action si un nombre de cartes utilisées par un client est dépassé sur une période.

Le module LCLF maintient deux compteurs de cartes pour chaque client : un compteur de cartes ayant donné lieu à une transaction acceptée et un compteur de cartes ayant donné lieu à une transaction refusée.
Le compteur de cartes refusées permet de s'attaquer au problème des testeurs de cartes, ceux-ci testant souvent des cartes déjà déclarées volées, cartes qui auparavant ne donnaient pas lieu à une association entre le client et la carte et donc passaient au travers des règles. Vous pouvez maintenant gêner les testeurs avec cette règle, à combiner avec une règle de vélocité client.
Note: une carte ayant initialement donné lieu à une transaction refusée mais qui donne ensuite lieu à une transaction acceptée passera du compteur "refusées" au compteur "acceptées". L'inverse n'est pas vrai.

Exemples de règles:

- Si nombre de cartes acceptées sur le dernier mois 2, alors déclencher 3DS si tentative d'utiliser une nouvelle carte.
- Si nombre de cartes refusées sur le dernier mois 2 et vélocité client 2 transactions refusées sur 24 heures, alors déclencher 3DS si tentative d'utiliser une nouvelle carte.

Dans le cas de cartes refusées, nous vous recommandons une règle de refus au-delà de 3 cartes sur une courte période. Il y a en effet peu de chances que le client soit honnête passé ce seuil :

- Si nombre de cartes refusées sur le dernier mois 3 et vélocité client 3 transactions refusées sur 24 heures, alors refuser la transaction si tentative d'utiliser une nouvelle carte.

> Attention, cette règle nécessite l'utilisation d'un identifiant unique du client. Sans cette information, toutes les transactions seront systématiquement refusées !

Nombre de clients par carte

Cette règle permet de déclencher une action si un nombre de comptes clients utilisant une même carte est dépassé sur une période.

Le module LCLF maintient deux compteurs pour chaque client : un compteur de cartes ayant donné lieu à une transaction acceptée et un compteur de cartes ayant donné lieu à une transaction refusée.
Pour cette règle, le compteur le plus utile est celui de cartes acceptées. En effet, si un fraudeur a obtenu un premier succès avec une carte, il sera tenté de la réutiliser. Pour échapper aux règles de cumul et vélocité client, certains feront leur deuxième tentative avec un nouveau compte acheteur, et ce rapidement avant que la carte ne soit mise en opposition.
Les testeurs de cartes eux vont tenter d'utiliser une même carte avec plusieurs comptes clients.

Exemples de règle:

- Si nombre de clients acceptés par carte 1, alors déclencher 3DS
- Si nombre de clients refusés par carte 3, alors refuser la transaction (testeurs de cartes)

> Attention, cette règle nécessite l'utilisation d'un identifiant unique du client. Sans cette information, toutes les transactions seront systématiquement refusées !

Nombre de clients par numéro de téléphone portable

Cette règle permet de déclencher une action si un nombre de comptes clients utilisant un même numéro de téléphone portable est dépassé sur une période.

Le module LCLF maintient deux compteurs pour chaque numéro de téléphone portable : un compteur de clients ayant eu une transaction acceptée et un compteur de clients ayant donné une transaction refusée.

Exemple de règle :

- Si nombre de clients acceptés par numéro de téléphone portable 1, alors déclencher 3DS

> Attention, cette règle nécessite l'utilisation d'un identifiant unique du client. Sans cette information, toutes les transactions seront systématiquement refusées !

Nombre de cartes par device fingerprint - indisponible

Cette règle permet de déclencher une action si un nombre de cartes utilisées via un même appareil - identifié par son "fingerprint" - est dépassé sur une période.
Le module LCLF maintient deux compteurs de cartes pour chaque (empreinte d') appareil: un compteur de cartes ayant donné lieu à une transaction acceptée (= cartes acceptées) et un compteur de cartes ayant donné lieu à une transaction refusée (= cartes refusées).
Note: une carte ayant initialement donné lieu à une transaction refusée mais qui donne ensuite lieu à une transaction acceptée passera du compteur "refusées" au compteur "acceptées". L'inverse n'est pas vrai.
Exemples de règles:

- Si nombre de cartes acceptées par appareil sur le dernier mois 2, alors déclencher 3DS si tentative d'utiliser une nouvelle carte.
- Si nombre de cartes refusées par appareil sur le dernier mois 2 et vélocité device fingerprint 2 transactions refusées sur 24 heures, alors déclencher 3DS si tentative d'utiliser une nouvelle carte.

Pays de l'adresse IP

Cette règle permet de déclencher une action si le pays de l'adresse IP appartient à une liste que vous aurez définie.
Note: de nombreux marchands sont tentés de refuser les paiements sur IP étrangère. Ce paramétrage ne prend pas en compte le fait que de nombreux clients vivent à l'étranger ou se déplacent souvent. Une authentification 3DS est alors préférable à un refus si vous n'utilisez que ce critère de discrimination, sauf cas particulier.

Pays émetteur du moyen de paiement

Cette règle permet de déclencher une action si le pays du moyen de paiement appartient à une liste que vous aurez définie.
Note: de nombreux marchands sont tentés de refuser les paiements en carte étrangère. Ce paramétrage ne prend pas en compte le fait que de nombreux clients vivent à l'étranger et donc possèdent une carte de leur lieu de résidence ou vivent dans le pays du site marchand mais sont étrangers et en possession d'une carte de leur pays d'origine.
Une authentification 3DS est alors préférable à un refus, en prenant soin toutefois de paramétrer la règle de Résultat 3DS de façon à ne pas se faire attaquer par des cartes étrangères hors zone Euro qui souvent passent 3DS sans authentification réelle.

Résultats 3DSecure

Cette règle permet de refuser un paiement 3DS qui n'aurait pas fait l'objet d'une authentification positive mais pourrait tout de même être accepté par la banque. Les cas les plus fréquents sont les suivants :

Vérification d'enrôlement

- Service « indisponible » (U)
- Carte non-enrôlée (N)

Authentification

- Service « indisponible » (U)
- Essai (A)

Dans le cas où la vérification d'enrôlement ou l'authentification seraient « indisponibles » (codes U pour Unavailable), le transfert de responsabilité ne s'applique pas. Nous conseillons la plus grande prudence dans ces cas-là, les fraudeurs ayant semble-t-il trouvé une faille avec certaines cartes qui leur permet de passer en U.Il est donc recommandé de paramétrer une règle de Résultat 3DSecure qui au minimum génèrerait une alerte pour vos équipes fraude et éventuellement refuserait les transactions pour lesquels l'un des éléments du 3DS est indisponible.Les retours "carte non-enrôlée" et "Essai" sont aussi à surveiller car aussi exploités par les fraudeurs. Ils peuvent faire l'objet d'une deuxième règle de Résultat 3DSecure. Le transfert de responsabilité est supposé s'appliquer dans ces cas-là, mais certains marchands nous ont signalé des cas de dossier d'impayé (chargeback).

A noter : il est maintenant possible de combiner la règle de Résultat 3DSecure avec d'autres règles. Cela vous permet de réduire le périmètre de cette règle en y ajoutant par exemple une règle de montant maximum ou de pays de carte.

Exemple d'utilisation : une authentification en Essai (A) indique souvent une fraude lorsque la carte est émise hors-Europe et source d'impayé (pas de transfert de responsabilité). De nombreux marchands refusent alors ces transactions.

Toutefois, Essai (A) est aussi observé avec des cartes européennes, en particulier comme étant le retour d'authentification des cartes prépayées, dont l'utilisation s'intensifie. Dans un tel cas, la fraude est moins probable et le transfert de responsabilité s'applique généralement.

Vous pouvez alors faire de telles règles :

- si le résultat de l'authentification = Essai et le produit de la carte bancaire ne contient pas Prepaid (règle générique), alors refuser la transaction
- si le résultat de l'authentification = Essai et la carte est émise hors-Europe, alors refuser la transaction

Connexions et machines à risque - indisponible

Cette règle permet de déclencher une action si la connexion utilisée par l'acheteur est considérée comme à risque, comme par exemple une connexion d'une IP Tor.
Exemples de règles:

- Si connexion Tor = oui et ancienneté du compte < 30 jours, alors refuser la transaction
- Si Navigation incognito = oui et nombre de commandes à date < 5, alors déclencher 3DS

Notez que ces informations concernant le type de connexion sont fournies par un prestataire et ne sont pas toujours exactes. La prudence est donc recommandée. Évitez par exemple des règles trop strictes.

Mise en quarantaine

Cette nouvelle règle (avril 2018) permet de déclencher une action si la transaction précédente du client, de la carte, du device fingerprint et/ou de l'adresse IP a échoué du fait d'un contrôle anti-fraude.

Elle permet par exemple de contrecarrer un fraudeur qui modifierait son panier pour passer en dessous d'un seuil de déclenchement de règle fraude.

A noter : pour bénéficier de la fonctionnalité de mise en quarantaine suite à un échec d'authentification 3DS, il faut veiller à définir dans le module anti-fraude une règle de contrôle 3DS refusant les transactions lorsque l'authentification 3DS échoue. Pour cela, configurez une règle 'Résultats 3DSecure' dans laquelle vous cochez 'Echec d'authentification (N)' et positionnez l'action à 'Refuser la transaction'.

Exemple 1

Vous avez configuré la règle comme suit :

et vous avez une règle de Montant maximum qui déclenche 3DS au delà de 100 EUR

Un client tente de faire un achat de deux paires de chaussures à 90 EUR chacune

Le module LCLF déclenche une demande d'authentification 3DS puisque le montant total est supérieur à 100 EUR

Le client ne s'authentifie pas (abandon ou 3 codes erronés), revient sur son panier et supprime une paire de chaussures, ramenant son panier à 90 EUR, soit en dessous du seuil de 100 EUR

La seconde tentative de paiement, si elle est faite dans les 12 heures qui suivent la première, va alors déclencher 3DS.

Exemple 2

Un client tente de faire une transaction à 90 EUR mais son identifiant a été mis en liste grise, ce qui déclenche une demande d'authentification 3DS

Le client ne s'authentifie pas, ouvre un nouveau compte acheteur et tente de refaire le même achat avec la même carte dans les 12 heures suivant la première transaction

La carte ayant été mise en quarantaine, la transaction déclenche elle aussi 3DS.

AVS - Address Verification Service

Cette fonction contrôle la correspondance entre les champs numériques de l'adresse de facturation renseignée par le client lors de sa commande et l'adresse du porteur de la carte telle qu'enregistrée auprès de la banque.

Le service est disponible uniquement pour les cartes émises aux Etats-Unis (US), au Canada (CA) et au Royaume Uni (UK).

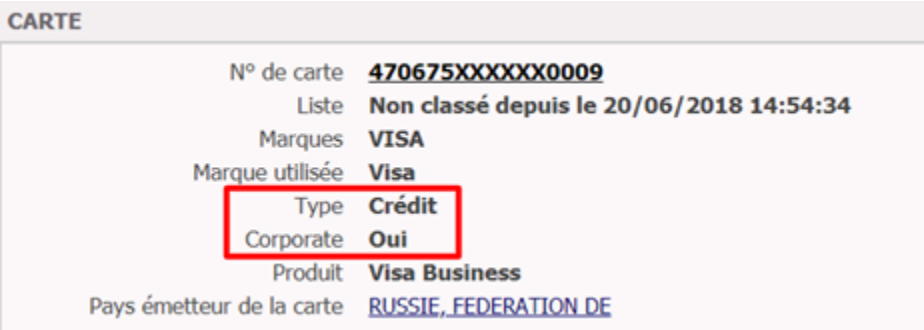
Type de carte

La règle Type de carte vous permet d'agir sur le type de la carte bancaire utilisée par un client. Quatre caractéristiques des cartes peuvent être exploitées :

- Crédit
- Débit
- Prépayée
- Corporate

La règle peut se déclencher si la carte est du type sélectionné ou n'est pas du type sélectionné.

L'information relative au type d'une carte est extraite du fichier SICB fourni par le GIE CB. Vous la retrouverez dans le détail d'une transaction :



CARTE

N° de carte	470675XXXXXX0009
Liste	Non classé depuis le 20/06/2018 14:54:34
Marques	VISA
Marque utilisée	Visa
Type	Crédit
Corporate	Oui
Produit	Visa Business
Pays émetteur de la carte	RUSSIE, FEDERATION DE

Notez que nous avons séparé l'information Corporate des trois autres, une carte pouvant être à la fois Corporate ET crédit/débit/prépayée.

Exemples d'utilisation

Ne pas appliquer le contrôle Résultat 3DS = A (Essai) aux cartes prépayées

Vous pouvez exclure les cartes prépayées de la règle sur le résultat 3DS si vous l'aviez configurée pour refuser les transactions qui ne sont pas pleinement authentifiées. En effet, les cartes prépayées sont souvent de type anonyme et donc leurs porteurs ne peuvent pas faire une authentification 3DS. Nous avons alors un retour A (Essai), couvert par le transfert de responsabilité en zone Euro mais rarement en dehors, sauf pour les prépayées. Dans ce cas, plutôt que de systématiquement refuser de telles transactions, faites une règle composée Résultat 3DS + Type de carte afin d'exclure les prépayées.

Garder l'œil sur les transactions en cartes Corporate

En fonction de votre activité vous pourriez vouloir surveiller les commandes passées avec des cartes de société. Par exemple, une commande d'une console de jeux avec telle carte présente un risque de fraude plus élevé.