Geavanceerde Fraudedetectie: Scoring

Configuratiegids voor de geavanceerde fraudedetectiemodule: Scoring v.4.4.7

Inhoud

1 Wat is de fraudedetectiemodule?

In distance selling, the fight against fraud requires maximum levels of know-how, speed and flexibility. To help you implement effective risk management, the Fraud Detection Module offers a real-time service that provides all the necessary analysis information, and offers fully customised safeguards for handling dubious transactions.

Use of the Fraud Detection Module does not, however, guarantee protection against all fraud, it only helps you to thwart it. The Fraud Detection Module can be configured based on the risks or past fraud issues that have been encountered by your business.

In tegenstelling tot de fraudedetectiebasismodule, configureert de handelaar in de geavanceerde module het werkelijke gedrag van de zwarte witte en grijze lijsten, samen met de regels en limieten in de scorelijst.

De basis en geavanceerde fraudedetectiemodule zijn allebei opwaarts compatibel, wat betekent dat een upgrade naar de geavanceerde module geen invloed heeft op het blokkerende gedrag dat u hebt geconfigureerd in de fraudedetectiebasismodule. Bijvoorbeeld:

- alle vermeldingen op de zwarte lijst zijn nog steeds aanwezig en de corresponderende criteria op de scorepagina worden geconfigureerd om te blokkeren.
- de creditcard- en IP-adreslanden die u hebt geconfigureerd om geen betalingen van te accepteren, worden beschouwd als landen met een hoog risico en worden op de scorepagina geconfigureerd om te blokkeren.
- de vermeldingen op de witte lijst voor IP-adressen zijn nog steeds aanwezig en het corresponderende gedrag (vertrouwen) wordt op de scorepagina ingesteld.

Uiteraard kunt u na een upgrade naar de geavanceerde fraudedetectiemodule profiteren van nog meer functies en nuances in de criteria die worden gebruikt voor het beoordelen van het risico van de transacties.

1.1 Voordelen

Met de fraudedetectiemodule kunt u:

- Afwijkingen tijdens transacties detecteren
- Pogingen van erkende oplichters onmiddellijk blokkeren
- Een score aan specifieke risico's toewijzen
- Beschermen tegen landspecifieke risico's
- Volledig aangepast beveiligingsbeleid definiëren en toepassen
- Profiteren van een voorwaardelijke betalingsgarantie (zie hier) in overeenstemming met het beleid van uw individuele acquirer (3-D Secure)

1.2 Toegang

U kunt de fraudedetectiemodule raadplegen via de "Fraud detection"-link in het menu van uw <% COMPANY > account.

1.3 Inhoud

De fraudedetectiemodule bestaat uit aparte functionele gedeelten:

- Activering en configuratie van fraudedetectie
- 3-D Secure
- Zwarte lijsten / grijze lijsten / witte lijsten

BELANGRIJK

- De VISA/MasterCard-criteria die in deze documentatie worden beschreven, zijn niet per se beschikbaar voor alle betaalmethoden.
- De beschikbaarheid van de configuratie met meerdere criteria is afhankelijk van de betaalmethode. Voor sommige betaalmethoden is de configuratie beperkt.
- We raden u aan de specifieke configuratie voor uw individuele betaalmethoden te controleren door op de knop 'Edit' (Bewerken) te klikken naast de betaalmethode in de tabel 'Fraud detection activation and configuration' (Fraudedetectie activeren en configureren) in het configuratiescherm van de fraudedetectie.

2 Activering en configuratie van fraudedetectie

In de tabel 'Fraud detection activation and configuration' (Fraudedetectie activeren en configureren) ziet u het onderscheid tussen creditcards en andere betaalmethoden. We bespreken nu de configuratie van de opties voor fraudedetectie voor creditcards.

Als u opties voor fraudedetectie wilt configureren voor een specifieke creditcard, klikt u op de knop 'Edit' (Bewerken) naast de betaalmethode. U kunt de scorepagina openen voor deze betaalmethode met koppelingen naar de configuratiepagina's voor de diverse regels, limieten en lijsten.

Het werkelijke gedrag van deze regels (of ze al dan niet transacties blokkeren) is afhankelijk van uw instellingen op de pagina 'Scoring' (Scores).

2.1 Landengroepen van kaartuitgevers

Alle landen van kaartuitgevers worden standaard geaccepteerd. Hier betekent de term 'land kaartuitgever' het land waar de kaart is uitgegeven. Ons systeem kan het land van de kaartuitgever identificeren op basis van de BIN-code van de kaart, oftewel de eerste 6 cijfers van een creditcardnummer. Een BIN-code is gekoppeld aan een specifieke bank in een specifiek land.

U kunt een bepaald risico per land van kaartuitgever instellen. Er zijn drie mogelijke categorieën om een land van kaartuitgever te classificeren:

- Hoog risico
- Gemiddeld risico
- Laag risico

Uitgiftelanden met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Uitgiftelanden met gemiddeld risico kunnen leiden tot een hogere score. Uitgiftelanden met een laag risico worden niet in aanmerking genomen voor de score.

Opmerking

- Alleen beschikbaar voor VISA, MasterCard, American Express en Diners Club

2.2 IP-landengroepen

Alle IP-adreslanden worden standaard geaccepteerd. Ons systeem kan het IP-adresland identificeren op basis van het IP-adres van uw klant. (Hoewel deze controle positieve resultaten oplevert in 94 % van alle gevallen, wordt deze IP-controle gebaseerd op extern ingevoerde IP-lijsten. Er bestaat dan ook een kleine kans op fouten, omdat we vertrouwen op de nauwkeurigheid van die lijst).

Net zoals bij het land van kaartuitgever, kunt u een bepaald risico per IP-adresland instellen. Er zijn drie mogelijke categorieën om een IP-adresland te classificeren:

- Hoog risico
- Gemiddeld risico
- Laag risico

IP-adreslanden met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. IP-adreslanden met gemiddeld risico kunnen leiden tot een hogere score. IP-adreslanden met een laag risico worden niet in aanmerking genomen voor de score.

Behalve deze IP-adreslanden, bestaan er ook anonieme proxy's. Anonieme proxy's zijn internetproviders die toestaan dat internetgebruikers hun IP-adres verbergen. We raden ten zeerste aan dat u transactie van anonieme proxy's blokkeertop de pagina 'Scoring' (Scores).

BELANGRIJK

'Asia Pacific Network', 'European Network' en 'Satellite Provider' verwijzen naar IP-adressen waarvan het land van oorsprong niet zeker is.

'European Network' betekent bijvoorbeeld dat het exacte IP-adresland niet zeker is, maar dat het wel in Europa ligt. 'European Network' als het IP-adresland accepteren betekent niet dat u betalingen uit alle landen van Europa accepteert, het betekent dat u betalingen van IP-adressen accepteert die door Europese instellingen worden beheerd (bijvoorbeeld een internetprovider die in meerdere Europese landen, de Europese Commissie enz. actief is).

Meestal is het IP-adresland gelijk aan het land van levering. De volgende bezorgingsregio's/-landen worden als riskant beschouwd door acquirers: Oost-Europa, Azië, Indonesië, Afrika en Groot-Brittannië. Als u echter veel zaken doet in die regio's/landen, of als u een specifieke lever- of bestelprocedure hanteert om de identiteit van de klant te controleren, hoeft u geen hoog risico voor deze regio's/landen in te stellen.

2.3 Riskante combinaties van IP-land / land kaartuitgever

Alle combinaties van IP-adreslanden/land kaartuitgever worden standaard geaccepteerd.

Als u een combinatie van IP-adresland/land kaartuitgever wilt configureren, selecteert u in de vervolgkeuzelijsten een IP-adresland en een land van kaartuitgever die u wilt combineren.

Op dezelfde wijze als voor landen kaartuitgever en IP-adreslanden kunt u een bepaald risico per combinatie van IP-adresland/land kaartuitgever instellen. Er zijn drie mogelijke categorieën om een IP-adresland/land kaartuitgever te classificeren:

- Hoog risico
- Gemiddeld risico
- Laag risico

Combinaties met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Combinaties met gemiddeld risico kunnen leiden tot een hogere score. Combinaties met een laag risico worden niet in aanmerking genomen voor de score.

Opmerking

- Alleen beschikbaar voor VISA, MasterCard, American Express en Diners Club

2.4 Bedraglimiet

U kunt het bedrag per transactie beperken door een minimum- en maximumbedrag in te voeren. De valuta van de limiet is gelijk aan die van uw hoofdaccount. Als u meerdere valuta's gebruikt en een transactie is uitgevoerd in een valuta die niet uw standaardvaluta is, converteert ons systeem het limiet naar een andere valuta.

2.5 Gebruikslimieten

2.5.1 Kaartgebruik

U kunt het 'maximum utilisation per card, per period' (maximumgebruik per kaart, per periode) instellen op basis van het totaal aantal transacties per kaart en het aantal transacties per kaart.

U moet deze limiet configureren op basis van uw bedrijf/producten. Als u bijvoorbeeld een product verkoopt dat iemand niet vaker dan eenmaal per week koopt, kunt u het kaartgebruik beperken tot eenmaal per week.

Voorbeeld

Als u niet meer dan twee transacties voor een bepaalde creditcard op dezelfde dag wilt accepteren en u niet meer dan 250 EUR op die creditcard op die dag wilt accepteren, moet u het volgende configureren:

- *Maximumgebruik per kaart, per periode 1 dag(en)*

- *Totaalbedrag van transacties per kaart, hoge drempel: 250 EUR*
- *Aantal transacties per kaart, hoge drempel: 2*

Als geavanceerd gebruik van deze regel, kunt u ook een lage en een hoge drempel instellen, zodat u twee verschillende scores krijgt. Met een lage drempel kunt u alleen de risicoscore verhogen. Met een hoge drempel kunt u ook de risicoscore verhogen of direct blokkeren.

De limiet 'maximum utilisation per card, per period' (maximumgebruik per kaart, per periode) is alleen van toepassing op kaarten die zijn gebruikt in transacties die een van de volgende statussen hebben gekregen: 9, 91, 92, 5, 51, 52.

2.5.2 IP-gebruik

U kunt het 'maximum utilisation per IP address, per period' (maximumgebruik per IP-adres, per periode) instellen op basis van het aantal geslaagde transacties per IP-adres en het totaalaantal transacties (geaccepteerd en geweigerd) per IP-adres.

Oplichters werken vaak met een lijst met gestolen creditcards, die ze een voor een uitproberen. Het resultaat is dat transacties met verschillende kaarten vanaf hetzelfde IP-adres worden gestuurd. U kunt het aantal transacties (geaccepteerd en geweigerd) per IP-adres beperken om fraude gemakkelijker te kunnen detecteren. Wanneer overmatig gebruik aan u wordt gemeld, is het ook belangrijk de geschiedenis van het IP-adres te bekijken. Op deze manier kunt u de levering van uw goederen stoppen wanneer u ziet dat veel transacties afkomstig zijn van een IP-adres dat verschillende kaarten binnen een bepaalde periode gebruikt.

Voorbeeld

als u niet meer dan één geslaagde transactie afkomstig van hetzelfde IP-adres binnen 3 dagen wilt accepteren en niet meer dan 3 pogingen vanaf dit IP-adres in deze periode wilt accepteren, kunt u dit als volgt instellen:

- *Maximumgebruik per IP-adres, per periode 3 dag(en)*
- *Aantal geslaagde transacties per IP-adres, hoge drempel: 1.*
- *Aantal transacties (geaccepteerd of geweigerd) per IP-adres, hoge drempel: 3.*

Als geavanceerd gebruik van deze regel, kunt u ook een lage en een hoge drempel instellen, zodat u twee verschillende scores krijgt. Met een lage drempel kunt u alleen de risicoscore verhogen. Met een hoge drempel kunt u ook de risicoscore verhogen of direct blokkeren.

Het maximale gebruik per IP-adres per periodelimiet is alleen van toepassing op IP's die werden gebruikt in transacties die resulteren in de volgende twee statussen:

- Succesvolle transacties: 9, 91, 92, 5, 50, 51, 52
- Alle andere transacties: 9, 91, 92, 5, 50, 51, 52, 2

2.5.3 E-mailgebruik

U kunt het maximumgebruik per e-mailadres, per periode instellen. U kunt aangeven hoe vaak een specifiek e-mailadres in een bepaalde periode kan worden gebruikt.

U kunt ook een lage en een hoge drempel instellen voor het e-mailgebruik, zodat u twee verschillende scores krijgt. Met een lage drempel kunt u alleen de risicoscore verhogen. Met een hoge drempel kunt u ook de risicoscore verhogen of direct blokkeren.

Het maximumgebruik per e-mailadres, per periode is van toepassing op transacties met alle statussen.

Het maximale gebruik per e-mailadres per periodelimiet is alleen van toepassing op e-mailadressen die werden gebruikt in transacties die resulteren in een van de volgende statussen: 9, 91, 92, 5, 50, 51, 52, 2.

2.6 Riskante gegevens

2.6.1 Riskante postcodes

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante postcodes geldt voor alle betaalmethoden. NB: de adressen zijn factuur- en verzendadressen.

U kunt een bepaald risico per postcode instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Postcodes met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Postcodes met gemiddeld risico kunnen leiden tot een hogere score. Postcodes met een laag risico worden niet in aanmerking genomen voor de score. Voor het beoordelen van de regel moet ook de landcode worden opgenomen.

Als u deze functionaliteit wilt gebruiken, verzendt u de volgende parameters voor factuur- en verzendadressen met de bijbehorende waarden in het bestellingsverzoek van uw website:

Factuuradres

Bijbehorende inputparameter	Formaat	Verklaring	Voorbeeld
OWNERCTY	AN (2)	Land van de klant	UK
OWNERZIP	AN (10)	Postcode van de klant	75420
OWNERADDRESS	AN (35)	Adres van de klant, eerste regel	Baker Street 221B
OWNERADDRESS2	AN (35)	Adres van de klant, tweede regel	tweede verdieping

of

Bijbehorende inputparameter	Formaat	Verklaring	Voorbeeld
ECOM_BILLTO_POSTAL_COUNTRYCODE	AN (2)	Land factuuradres	UK
ECOM_BILLTO_POSTAL_POSTALCODE	AN (10)	Postcode factuuradres	75420
ECOM_BILLTO_POSTAL_STREET_LINE1	AN (35)	Factuuradres, eerste regel	Baker Street 221B
ECOM_BILLTO_POSTAL_STREET_LINE2	AN (35)	Factuuradres, tweede regel	tweede verdieping

Verzendadres

Bijbehorende inputparameter	Formaat	Verklaring	Voorbeeld
ECOM_SHIPTO_POSTAL_COUNTRYCODE	AN (2)	Landcode verzendadres	UK
ECOM_SHIPTO_POSTAL	AN (10)	Postcode	75420

_POSTALCODE		verzendadres	
ECOM_SHIPTO_POSTAL_STREET_LINE1	AN (35)	Verzendadres, eerste regel	Baker Street 221B
ECOM_SHIPTO_POSTAL_STREET_LINE2	AN (35)	Verzendadres, tweede regel	tweede verdieping

Meer informatie over deze velden vindt u in uw KBC/CBC-Paypage account. Log in en ga naar: Ondersteuning > Integratie- en gebruikershandleidingen > Technische Handleidingen > Parameter Cookbook.

2.6.2 Riskante perioden (tijd van bestelling)

BELANGRIJK

- U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante perioden geldt voor alle betaalmethoden.
- De gebruikte tijdzone is CET!

U kunt een bepaald risico per bestelperiode instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Perioden met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Perioden met gemiddeld risico kunnen leiden tot een hogere score. Perioden met een laag risico worden niet in aanmerking genomen voor de score.

Als u de tabel wilt configureren, selecteert u het risico onder aan de tabel, vinkt hokjes aan die u aan dit risico wilt toewijzen en klikt u op de knop 'Apply' (Toepassen).

2.6.3 Riskante verzendingsmethode

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante verzendingsmethoden geldt voor alle betaalmethoden.

U kunt een bepaald risico per verzendingsmethode instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Verzendingsmethoden met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Verzendingsmethoden met gemiddeld risico kunnen leiden tot een hogere score. Verzendingsmethoden met een laag risico worden niet in aanmerking genomen voor de score.

U kunt uw lijst configureren door de verzendingsmethode in te voeren, selecteer bij Gegevens verzendingsmethode de waarde in de vervolgkeuzelijst, het risico in te stellen en op de knop 'Add' (Toevoegen) te klikken. Klik op de knop 'Submit' (Doorvoeren) om te voltooien.

Gerelateerde invoerparameter	Indeling	Verklaring	Voorbeeld
ECOM_SHIPMETHODTYPE	Geheel getal: 1-9	Bezorgingsmethode 1: Ophalen bij handelaar 2: Ophaalpunt (postkantoor, Kiala-punt...) 3: Ophalen op luchthavenn , treinstation of reisbureau 4: Koerier (DHL, UPS ...) 5: Downloaden 6: Carrier Laag kosten 7: Verzamel bij Parcel Lockers 8: Militair 9: elektronisch 91: Door merchant gedefinieerd 1 92: Door merchant gedefinieerd 2 93: Door merchant gedefinieerd 3 94: Door merchant gedefinieerd 4 95: Door merchant gedefinieerd 5 96: Door merchant gedefinieerd 6 97: Door merchant gedefinieerd 7 98: Door merchant gedefinieerd 8 99: Door merchant gedefinieerd 9	4

Meer informatie over deze velden vindt u in uw KBC/CBC-Paypage account. Log in en ga naar: Ondersteuning > Integratie- en gebruikershandleidingen > Technische Handleidingen > Parameter Cookbook.

2.6.4 Details van riskante verzendingsmethoden

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante verzendingsmethoden geldt voor alle betaalmethoden.

U kunt een bepaald risico per vermelding instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Verzendingsmethodedetails met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Verzendingsmethodedetails met gemiddeld risico kunnen leiden tot een hogere score. Verzendingsmethodedetails met een laag risico worden niet in aanmerking genomen voor de score.

U kunt uw lijst selecteer bij Gegevens verzendingsmethode de waarde in de vervolgkeuzelijst, het risico in te stellen en op de knop 'Add' (Toevoegen) te klikken. Klik op de knop 'Submit' (Doorvoeren) om te

voltooien.

Gerelateerde invoerparameter	Indeling	Verklaring	Voorbeeld
ECOM_SHIPMETHODDETAILS	Vrij in te voeren tekst (max. 50 tekens)	Bepaling van ophaalpunt	Postkantoor KR124

Meer informatie over deze velden vindt u in uw KBC/CBC-Paypage account. Log in en ga naar: Ondersteuning > Integratie- en gebruikershandleidingen > Technische Handleidingen > Parameter Cookbook.

2.6.5 Riskante productcategorieën

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante productcategorieën geldt voor alle betaalmethoden. Riskante productcategorieën hebben alleen betrekking op e-Commerce en DirectLink.

U kunt een bepaald risico per productcategorie instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Productcategorieën met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Productcategorieën met gemiddeld risico kunnen leiden tot een hogere score. Productcategorieën met een laag risico worden niet in aanmerking genomen voor de score.

Als u deze functionaliteit wilt gebruiken, verzendt u uitsluitend de parameter ITEMFDMPRODUCTCATEGx met de bijbehorende waarden.

Gerelateerde invoerparameter	Indeling	Verklaring	Voorbeeld
ITEMFDMPRODUCTCATEGx	Gratis tekst (maximaal 50)	Productcategorie	Reizen Eten Sport

Opmerking:

Vervang "x" met: ITEMFDMPRODUCTCATEG1, ITEMFDMPRODUCTCATEG2, etc.

Meer informatie over deze velden vindt u in uw KBC/CBC-Paypage account. Log in en ga naar: Ondersteuning > Integratie- en gebruikershandleidingen > Technische Handleidingen > Parameter Cookbook.

2.6.6 Riskante tijd tot levering

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante tijd tot levering geldt voor alle betaalmethoden.

U kunt een bepaald risico per tijd instellen (aantal uren). Er zijn drie mogelijke niveaus:

- Hoog risico

- Gemiddeld risico
- Laag risico

Tijd tot levering met een hoog risico kan leiden tot geblokkeerde transacties of een hogere score. Tijd tot levering met gemiddeld risico kan leiden tot een hogere score. Tijd tot levering met een laag risico wordt niet in aanmerking genomen voor de score.

U kunt uw lijst configureren door de productcategorie in te voeren, het risico in te stellen en op de knop 'Add' (Toevoegen) te klikken. Klik op de knop 'Submit' (Doorvoeren) om te voltooien.

Gerelateerde invoerparameter	Indeling	Verklaring	Voorbeeld
ECOM_SHIPMETHODSPEED	Geheel getal	Het aantal uren dat nodig is voor de levering	24

Meer informatie over deze velden vindt u in uw KBC/CBC-Paypage account. Log in en ga naar: Ondersteuning > Integratie- en gebruikershandleidingen > Technische Handleidingen > Parameter Cookbook.

2.6.7 Riskante submerken

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante submerken geldt voor alle betaalmethoden.

U kunt een bepaald risico per submerk instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Submerken met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Submerken met gemiddeld risico kunnen leiden tot een hogere score. Submerken met een laag risico worden niet in aanmerking genomen voor de score.

U kunt uw lijst configureren door het submerk in te voeren, het risico in te stellen en op de knop 'Add' (Toevoegen) te klikken. Klik op de knop 'Submit' (Doorvoeren) om te voltooien.

2.6.8 Riskante uitgeversnummers

BELANGRIJK

U hoeft deze pagina maar eenmaal te configureren. De configuratie van de riskante uitgeversnummers geldt voor alle betaalmethoden.

U kunt een bepaald risico per nummer instellen. Er zijn drie mogelijke niveaus:

- Hoog risico
- Gemiddeld risico
- Laag risico

Uitgeversnummers met een hoog risico kunnen leiden tot geblokkeerde transacties of een hogere score. Uitgeversnummers met gemiddeld risico kunnen leiden tot een hogere score. Uitgeversnummers met een laag risico worden niet in aanmerking genomen voor de score.

U kunt uw lijst configureren door het uitgeversnummer in te voeren, het risico in te stellen en op de knop 'Add' (Toevoegen) te klikken. Klik op de knop 'Submit' (Doorvoeren) om te voltooien.

2.7 Instellingen dupliceren

Naast elke betaalmethode in het overzicht "Fraudedetectie activatie en configuratie" ziet u een knop "Dupliceren". Met deze knop kunt u de geconfigureerde instellingen van een betaalmethode naar een of meer andere betaalmethoden in de lijst kopiëren. Bij een account met meerdere betaalmethoden hoeft u dus dezelfde configuratie niet meerdere keren uit te voeren.

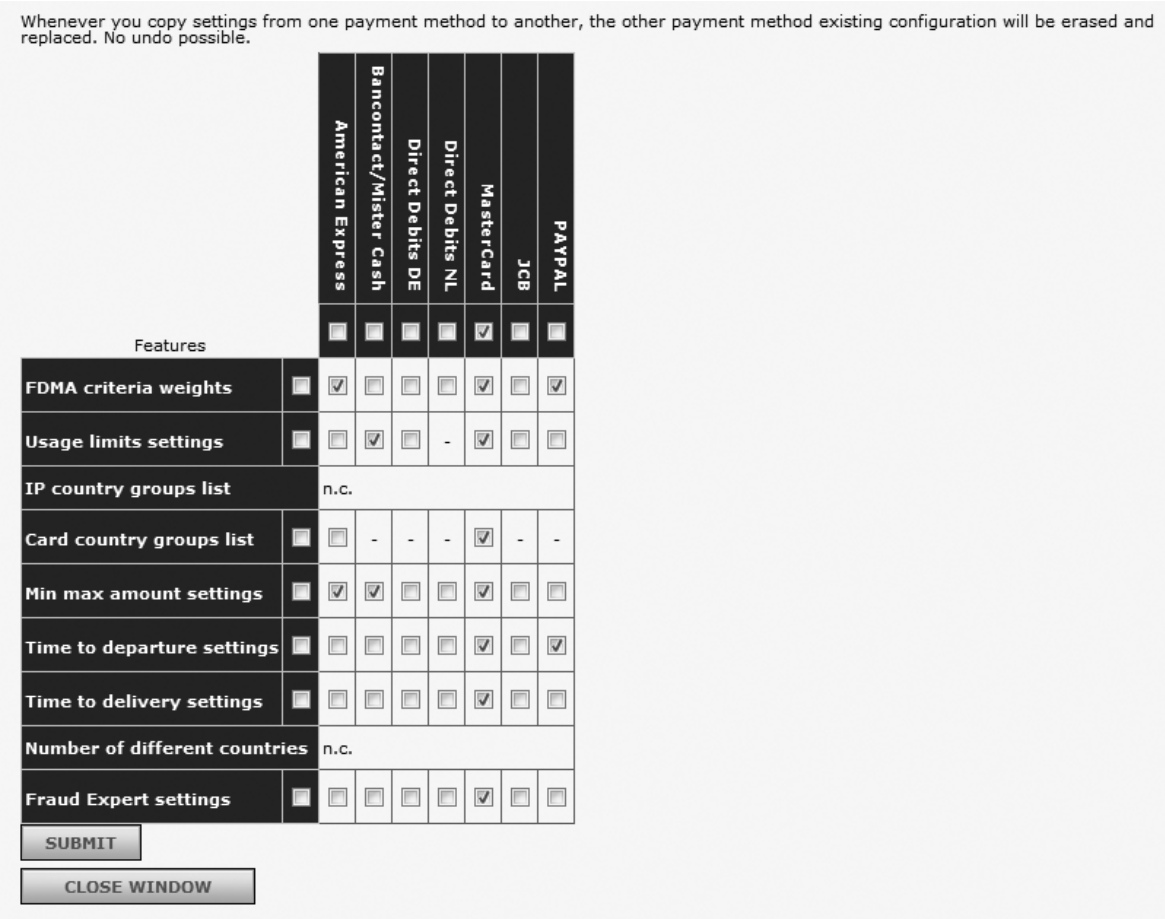
Belangrijk

Als u fraudedetectie al hebt ingesteld voor een betaalmethode waarnaar u instellingen van een andere betaalmethode wilt kopiëren, worden de oorspronkelijke instellingen overschreven door de gekopieerde instellingen.

De volgende instellingen kunnen worden gekopieerd, ongeacht of deze door de beoogde betaalmethode worden ondersteund:

- 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

Voorbeeld



3 3-D Secure

3-D Secure biedt een hoog beveiligingsniveau, omdat klanten ondubbelzinnig kunnen worden geïdentificeerd door middel van technologie, bijvoorbeeld html-wachtwoorden, Digipass, kaartlezers, biometrie enz., die door banken worden toegepast.

Met 3-D Secure kan een handelaar profiteren van een voorwaardelijke betalingsgarantie (zie hier) die wordt beschreven in het 3-D Secure-contract met zijn acquirer. Onder deze omstandigheden wordt de rekening van een handelaar niet meer gedebiteerd voor geschillen over "niet-identificatie van de kaarthouder". (Dit is niet van toepassing op geschillen over andere kwesties!)

De volgende merken hebben het 3-D Secure-protocol geïmplementeerd:

- Visa onder de naam Verified by Visa
- MasterCard onder de naam SecureCode
- JCB onder de naam J-Secure
- American Express onder de naam SafeKey

Als het unieke IP-adres van een klant op deze witte lijst staat, worden alle IP-gerelateerde blokkerings- en controleregels gedeactiveerd (afhankelijk van de score-instellingen van de merchant). Zie voor meer informatie over het deactiveringsmechanisme Bijlage: Deactiveringsmechanisme.

3.1 Algemeen

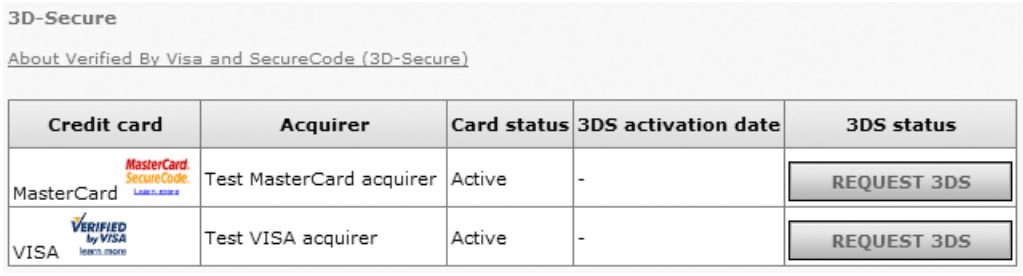
3.1.1 Aanvraag affiliatie

Indien 3-D Secure niet voor uw account is geactiveerd, ziet u de knop '3DS aanvragen' in de tabel '3-D Secure'.

Als u op de knop '3DS aanvragen' klikt, wordt een e-mail aan uw acquirer gestuurd. Als uw contract met uw acquirer geen ruimte biedt voor 3-D Secure, kunt u contact opnemen met uw acquirer voor meer informatie over de registratie voor 3-D Secure, als u wilt dat uw acquirer de 3-D Secure-betaalmethode toevoegt.

Opmerking: Om u aan te melden voor SafeKey, gelieve contact op te nemen met American Express of ga naar het SafeKey-portaal.

Zodra 3-D Secure is ingeschakeld in uw account, ziet u de activeringsdatum in de tabel. U kunt de configuratie voor 3-D Secure wijzigen door op de knop 'Edit' (Bewerken) naast de betaalmethoden te klikken.



3.1.2 Standaard 3-D Secure-transactie wordt verwerkt

1. Wanneer we de creditcardgegevens van uw klant ontvangen, stuurt ons systeem een verzoek aan de VISA/MasterCard/JCB/AmEx-lijst om te controleren of de kaart is geregistreerd, dat wil zeggen dat de kaarthouder een identificatiebewijs aan zijn/haar kaart heeft gekoppeld en, indien van toepassing, haalt de servergegevens voor de uitgeversauthenticatie op.

2. Als de kaart is geregistreerd, verbindt ons systeem de koper door naar de authenticatieserver van de

uitgever om de authenticatie uit te voeren.

3. Ons systeem ontvangt het resultaat van de authenticatie en verwerkt de betaling op de gebruikelijke wijze.

Als de authenticatie is geslaagd, kan de handelaar gebruikmaken van de voorwaardelijke betalingsgarantie van zijn acquirer.

Als de kaart niet is geregistreerd, ontvangt de handelaar voorwaardelijke betalingsgarantie van zijn acquirer.

In beide gevallen heeft de handelaar onder bepaalde omstandigheden (gedefinieerd door VISA, MasterCard en financiële organisaties, en zoals beschreven in het 3-D Secure-contract met zijn acquirer) een betalingsgarantie, zelfs zonder ID-informatie over de klant te ontvangen. Deze voorwaardelijke betalingsgarantieregels worden exclusief geregeld tussen de handelaar en zijn acquirer. KBC/CBC-Paypage treedt alleen op als technische tussenpersoon.

3.2 Configuratieopties

Dit zijn configuratieopties voor Verified by Visa, MasterCard SecureCode en J-Secure. Afhankelijk van uw acquirer zijn sommige (of alle) van deze opties mogelijk niet toegankelijk.

3.2.1 Technisch probleem

De handelaar kan kiezen om *door te gaan* of *de transactie te onderbreken* indien een technisch probleem verbinding met de VISA/MasterCard/JCB/AmEx-lijst verhindert tijdens de registratiecontrole door 3-D Secure.

Indien een technisch probleem verhindert dat ons systeem verbinding maakt met de VISA/MasterCard/JCB/AmEx-lijst (stap 1), raadt VISA/MasterCard/JCB/AmEx aan dat het proces wordt voortgezet zonder authenticatie (optie *doorgaan*). In dit geval kan de handelaar echter niet gebruikmaken van de voorwaardelijke betalingsgarantie (zie hier).

3.2.2 Identificatieservice tijdelijk niet beschikbaar

Indien de identificatiedienst voor de kaarthouder tijdelijk niet beschikbaar is, kan de handelaar ervoor kiezen om *door te gaan* of *de transactie te onderbreken* .

Als de authenticatieserver van de uitgever tijdelijk niet beschikbaar is (stap 2), kan de kaarthouder niet worden geïdentificeerd. In dit geval raadt VISA/MasterCard/JCB/AmEx aan door te gaan met het proces (optie *doorgaan*). In dit geval kan de handelaar echter niet gebruikmaken van de voorwaardelijke betalingsgarantie (zie hier).

3.2.3 Authenticatie mislukt (alleen MasterCard)

De handelaar kan ervoor kiezen om *door te gaan* of *de transactie te onderbreken* als de authenticatie mislukt.

Indien de authenticatie van de kaarthouder mislukt (stap 3), raadt MasterCard aan de betalingsverwerking te onderbreken (optie *onderbreken*). Indien de transactie doorgaat, kan de handelaar niet gebruikmaken van de voorwaardelijke betalingsgarantie (zie hier).

3.2.4 3-D Secure activeren/deactiveren

Hier kan de handelaar 3-D Secure in- of uitschakelen voor alle VISA/MasterCard/JCB/AmEx-kaarten.

WAARSCHUWING

Indien 3-D Secure is uitgeschakeld, kan de handelaar niet gebruikmaken van de voorwaardelijke betalingsgarantie (zie hier).

4 Zwarte lijsten, grijze lijsten en witte lijsten configureren

In de geavanceerde fraudedetectiemodule kunt u uw eigen zwarte en grijze lijsten genereren voor creditcards,gebaseerd op BIN-codes, creditcardnummers, e-mailadressen, telefoonnummers, namen, algemene gegevens en IP-adressen waarvan u geen transacties wilt accepteren. Er zijn ook witte lijsten, die zijn gebaseerd, IP-adressen en een uniek klant-ID, op witte lijst met e-mailadressen.

Het werkelijke gedrag van deze lijsten (of ze al dan niet blokkeren) is afhankelijk van uw instellingen op de pagina 'Scoring' (Scores).

'No' in het hoofdmenu geeft aan dat niets is geconfigureerd in de betreffende zwarte/grijze/witte lijst. Wanneer een zwarte/grijze/witte lijst al is geconfigureerd, is de status 'Yes'.

4.1 Algemene lijstfuncties

4.1.1 Vermeldingen

In de geavanceerde fraudedetectiemodule is geen limiet voor het aantal vermeldingen op de lijsten. U kunt maximaal 1000 items tegelijk invoeren in het veld.

U kunt altijd vermeldingen uit uw lijsten verwijderen door op de selectievakjes te klikken in de kolom 'Delete' (Verwijderen) en op de knop 'Submit' (Doorvoeren) te klikken.

4.1.2 Opmerkingen

U kunt een opmerking toevoegen aan een vermelding in een zwarte, grijze of witte lijst.

U kunt deze bij het indienen invoeren, door de opmerking in het veld 'Comment' in te voeren. Alle items die u hebt ingevoerd voor die indiening, krijgen dezelfde opmerking.

U kunt ook een opmerking toevoegen of verwijderen door te klikken op de koppeling '...' in de opmerkingenkolom.

4.1.3 Reden

Voor elke vermelding in een zwarte of grijze lijst, kunt u een reden selecteren waarom u de gegevens wilt invoeren: werkelijke fraude of een commercieel geschil.

BELANGRIJK

Selecteer alleen "werkelijke fraude" wanneer u een chargeback hebt ontvangen met een fraudeoorzaakcode.

4.1.4 Filter

U kunt de gegevens in de lijsten filteren met de knop 'Filter' boven aan de tabel. U kunt filteren op datum en op lijstinhoud.

U kunt een filter verwijderen door op de knop 'Remove filter' (Filter verwijderen) te klikken.

4.1.5 Lijstdownloads

U kunt de lijstinhoud in een spreadsheet downloaden (bijvoorbeeld Excel-bestand) door op de knop 'Download List' (Lijst downloaden) boven aan de tabel te klikken.

Als u op de knop 'Download List' (Lijst downloaden) klikt wanneer u een filter hebt toegepast, wordt de gefilterde inhoud gedownload.

4.1.6 Waarschuwing zwarte lijst

In de zwarte lijsten kunt u een keuzerondje selecteren om een waarschuwing via e-mail te verzenden wanneer een zwarte lijst wordt geactiveerd. De waarschuwing wordt naar het e-mailadres (of meerdere adressen) gestuurd dat is geconfigureerd in 'E-mail address(es) for transaction-related e-mails' (E-mailadres(sen) voor berichten over transactie) op de pagina 'Technical information' (Technische informatie) van uw account.

BELANGRIJK

U hoeft deze optie slechts eenmaal in- of uit te schakelen. De configuratie van deze optie wordt op alle zwarte lijsten toegepast.

4.2 Witte lijsten

Witte lijsten bevatten gegevens voor bevoorrechte klanten en/of gegevens die worden gebruikt om andere regels te vervangen (afhankelijk van de score-instellingen van de handelaar).

4.2.1 Witte lijst voor IP-adressen

U kunt IP-adressen van klanten waarvan u bestellingen wilt ontvangen op de lijst met vertrouwde IP-adressen zetten. Als een uniek IP-adres van een klant op deze witte lijst staat, worden alle overige IP-blokkeringsregels genegeerd (afhankelijk van de score-instellingen van de handelaar).

Ons systeem kan alleen het IP-adres van de klant controleren, indien de handelaar werkt via DirectLink moet het IP-adres in het veld 'REMOTE_ADDR' worden meegestuurd.

U kunt een reeks IP-adressen invoeren in de indelingen 'a.b.c-d.0-255', 'a.b.c-d.*' of 'a.b.c.d-e'.

4.2.2 Witte lijst voor unieke klant-ID's

De CUI (uniek klant-ID) wordt door de handelaar aan de klant toegekend. Het kan een naam, klantnummer, e-mailadres enz. zijn. Als de handelaar dit ID wil gebruiken, moet hij ons de CUI sturen via het extra veld 'CUID' (alfanumeriek, max. 50 tekens).

Als een uniek CUI op deze witte lijst staat, worden alle overige blokkeringsregels genegeerd (afhankelijk van de score-instellingen van de handelaar), behalve de zwarte lijst voor creditcards.

4.2.3 Witte lijst met e-mailadressen

U kunt het e-mailadres van de klant op de witte lijst plaatsen door het e-mailadres aan deze lijst toe te voegen. Verder moet u het e-mailadres van de klant in de details van de bestelling verzenden zodat het systeem het e-mailadres kan controleren. Als dit al is gebeurd, wordt de controle automatisch uitgevoerd.

Als het e-mailadres van een klant op deze witte lijst staat, worden vrijwel alle andere blokkerings- en controleregels gedeactiveerd (afhankelijk van de score-instellingen van de merchant). Voor meer informatie over het deactiveringsmechanisme raadpleegt u de bijlage: Deactiveringsmechanisme.

4.3 Zwarte lijsten / grijze lijsten

De zwarte lijst maakt het mogelijk om (op basis van de ingestelde regels) transacties te blokkeren, transacties gedwongen te controleren en risicoscores toe te kennen aan transacties. De grijze lijst maakt het mogelijk om (op basis van de ingestelde regels) transacties gedwongen te controleren en risicoscores toe te kennen aan transacties.

Voorbeeld: U hebt problemen gehad met transacties vanaf een specifiek IP-adres, maar weet niet zeker of dit IP-adres aan één persoon toebehoort. Het IP-adres kan ook van een bedrijf/gebouw zijn of kan in de toekomst aan een andere persoon worden toegewezen door de provider.

In dat geval wilt u dit IP-adres niet meteen op de zwarte lijst zetten, omdat u andere potentiële klanten niet wilt benadelen/blokkeren. U kunt het IP-adres op de grijze lijst zetten totdat u zeker weet of dit naar de zwarte lijst wilt verplaatsen of van de grijze lijst wilt verwijderen.

U kunt gegevens van de grijze naar de zwarte lijst verplaatsen door op de selectievakjes in de kolom 'Move to blacklist' (Naar zwarte lijst verplaatsen) in de grijze lijst te klikken en op 'Submit' (Doorvoeren) te klikken.

4.3.1 Kaartnummer

In uw zwarte/grijze lijst voor creditcards moet u het volledige creditcardnummer invoeren.

In de zwarte lijst voor kaarten kunt u een keuzerondje selecteren om het IP-adres van transacties die overeenkomen met een kaart op de zwarte lijst op de grijze lijst te zetten.

Als u de betaalmethoden Direct Debits NL, Direct Debits DE of Direct Debits AT in uw account hebt geactiveerd, fungeert de zwarte of grijze lijst voor kaarten ook als een zwarte of grijze lijst voor rekeningnummers.

4.3.2 BIN

De BIN-code bestaat uit de eerste 6 cijfers van een creditcardnummer. Een BIN-code is gekoppeld aan een specifieke bank in een specifiek land. Als gevolg kunt u alle creditcards invoeren die bank X in land Y op uw lijst heeft uitgegeven, door de BIN-code toe te voegen.

4.3.3 IP-adres

In uw zwarte of grijze lijst voor IP-adressen kunt niet alleen een specifiek IP-adres invoeren, maar ook een reeks IP-adressen met de volgende indelingen: a.b.c-d.0-255 of a.b.c-d.* of a.b.c.d-e.

Ons systeem kan alleen het IP-adres van de klant controleren indien de handelaar het IP-adres via DirectLink stuurt in het veld 'REMOTE_ADDR'.

4.3.4 E-mailadres

Het e-mailadres kan een vast adres zijn, of een reeks adressen (domein) met een asterisk (*) voor het teken @. Het e-mailadres dat door de handelaar is ingevoerd wordt in de kolom 'e-mail' weergegeven. Op basis van dit e-mailadres genereert ons systeem de gedeeltelijke overeenkomst.

Ons systeem kan alleen het e-mailadres van de klant controleren als de handelaar dat aan de bestelgegevens toevoegt.

4.3.5 Naam

De handelaar kan namen van klanten in de zwarte of grijze lijst opnemen. De naam die door de handelaar is ingevoerd wordt in de kolom 'Name' weergegeven. Op basis van die naam genereert ons systeem twee andere versies van de naam: de opgeschoonde naam en de gedeeltelijke overeenkomst.

Ons systeem kan alleen de naam van de klant controleren als de naam van de kaarthouder, vervoersnaam en naam op de factuur.

4.3.6 Telefoonnummer

De handelaar kan het telefoonnummer van een klant in de zwarte of grijze lijst opnemen. Het telefoonnummer dat door de handelaar is ingevoerd wordt in de kolom 'Phone number' weergegeven. Op basis van dit telefoonnummer genereert ons systeem twee andere versies: het opgeschoonde nummer en de gedeeltelijke overeenkomst.

Ons systeem kan alleen het telefoonnummer van de klant controleren als de handelaar dat aan de bestelgegevens toevoegt.

4.3.7 Algemene gegevens

De zwarte en grijze lijst voor algemene gegevens bieden de handelaar de optie een volledig gepersonaliseerde lijst te hanteren waaraan hij de gegevens kan toevoegen die hij wil laten meewegen voor de fraudescore van transacties. De gegevens moeten alfanumeriek zijn en mogen niet meer dan 50

tekens bevatten.

Ons systeem kan alleen de algemene gegevens controleren als de handelaar de gegevens in het veld 'GENERIC_BL' van de bestelling invoert (alfanumeriek, max. 50 tekens).

5 Scoring (Scores)

U kunt een lijst met criteria vinden op de configuratiepagina 'Scoring' (Scores), die alle criteria bevat die in de geavanceerde fraudedetectiemodule kunnen worden ingesteld.

BELANGRIJK

In tegenstelling tot de fraudedetectiebasismodule, waar het blokkeringsgedrag wordt ingesteld in de zwarte en witte lijsten, blokkeringsregels enz., configureert de handelaar het werkelijke gedrag van de zwarte/ grijze/witte lijsten samen met de limieten en regels in de scorelijst.

Per criterium kan een van de volgende acties worden geconfigureerd:

- *Risicoweging verhogen*: een weging van 0 tot 5 kan worden toegevoegd wanneer de criteria het risico verhogen.
- *Risicoweging verlagen*: een weging van 0 tot 5, 10 of 20 kan worden afgetrokken wanneer de criteria het risico verlagen.
- *Controle opleggen*: voor alle criteria is het mogelijk een controle van de transactie op te leggen. Met een opgelegde controle wordt ook een +3 aan de score toegevoegd naast de andere regels. De transactie wordt oranje indien de score groen of oranje is, of blijft rood als de totaalscore boven de rode drempel is en aan andere blokkeringscriteria is voldaan.
- *Transactie blokkeren*: voor bepaalde criteria hebt u de optie de transactie te blokkeren. De regels die door de handelaar zijn ingesteld blokkeren dan ook een transactie of beïnvloeden de algemene score van de transactie. De eindscore is de totale weging van de diverse criteria. Hoe hoger de score, hoe hoger het risico.
- *Blokkerings:* en controleregels deactiveren

De handelaar kan een bepaalde scorewaarde instellen als bovenlimiet voor een tussenstand voordat de transactie wordt geautoriseerd. Dit geeft aan dat alle transactie met deze score of hoger moeten worden geblokkeerd vóór de autorisatieprocedure. De AAV- en CVC-controle vinden plaats nadat we de transactie aan de acquirer hebben gestuurd (na de autorisatie), zodat deze scorewaarden niet worden meegerekend in deze tussenstand.

De som van de waarden vóór autorisatie en de waarden van de AAV- en CVC-scores leveren de definitieve en algemene score op. De handelaar kan scorecategorieën kiezen op basis van zijn definitieve scorewaarde, gekoppeld aan kleuren: groen (laag risico), oranje (gemiddeld risico) en rood (geblokkeerde transactie). Deze kleuren worden weergegeven in de feedback aan de handelaar.

Indien een transactie wordt geblokkeerd op basis van uw instellingen, krijgt die de status 'Authorisation declined' (Autorisatie geweigerd).

Voorwaarden: aangezien sommige informatie afkomstig is van extern aangeleverde lijsten, vertrouwen we op hun nauwkeurigheid en kunnen we geen resultaat garanderen dat 100 % correct is.

Hier volgt een (oneindige) selectie van scorecriteria:

- *3-D Secure*: wanneer de kaarthouder volledig door 3-D Secure is geauthenticeerd (identificatie OK) en de kaarthouder niet is geregistreerd. Wanneer een creditcard 3-D Secure is en u een 3-D Secure-contract hebt met uw acquirer, hebt u een voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) voor de transactie. Zelfs als u geen betalingen wilt ontvangen van een bepaalde creditcard of IP-adreslanden vanwege een verhoogd risico op fraude, kunt u nog steeds transacties met 3-D Secure-creditcards toestaan die afkomstig zijn uit deze landen, aangezien het risico veel lager is.
- *Anonieme proxy's*: Anonieme proxy's zijn internetproviders die toestaan dat internetgebruikers hun IP-adres verbergen. We raden u aan geen betalingen te accepteren die van anonieme proxy's afkomstig zijn!
- *Gratis e-mail*oplichters gebruiken meestal valse e-mailaccounts die via gratis e-mailservices zijn aangemaakt. Ons systeem controleert (op basis van extern aangeleverde lijsten) of het e-mailadres van de klant een gratis adres is. De handelaar kan besluiten een risicoscore toe te voegen aan transacties waar het e-mailadres van de klant een gratis e-mailadres is. Ons systeem kan alleen het e-mailadres van de klant controleren als de handelaar dat aan de bestelgegevens toevoegt.
- *Aantal landen: de handelaar kan het toegestane aantal landen opgeven en de toe te passen score instellen indien het aantal die limiet overschrijdt op basis van*:
    - Land van de creditcard (voor VISA, MasterCard, American Express en Diners Club)
    - Land van het IP-adres (indien beschikbaar)
    - Factuur- en verzendadres indien meegestuurd
    - Luchthaven van vertrek indien van toepassing en meegestuurd

- *IP-adresland wijkt af van het cc-land* (alleen voor VISA, MasterCard, American Express en Diners Club): als u deze parameter instelt op 'Block transaction' (Transactie blokkeren), staat u alleen transacties toe indien het IP-adres van de klant in hetzelfde land als zijn creditcarduitgever is. Met andere woorden: alleen als het land van de kaartuitgever en het IP-adres identiek zijn. Deze controle wordt niet uitgevoerd indien het IP-adres van een anonieme proxy, het Aziatisch Pacifisch netwerk, het Europese netwerk of een satellietprovider afkomstig is.
- *Factuuradres wijkt af van het afleveradres*: dit geeft aan of het factuuradres wordt gezien als afwijkend van het afleveradres, gebaseerd op de waarde van het extra veld 'addMatch' dat de handelaar ons in de bestelgegevens stuurt. Als de waarde '1' is, worden het factuur- en afleveradres als identiek beschouwd. Als de waarde '0' is, worden ze als afwijkend beschouwd.
- *Bedraglimiet, gebruikslimieten*
- *Identificatie van CUI op witte lijst*
- *Witte lijst met e-mailadressen*
- *Vertrouwd IP-adres*
- *Kaart/BIN/IP-adres/e-mail/telefoonnummer/naam kaarthouder/algemene gegevens op zwarte en grijze lijst*
- *Uitgiftelanden met hoog en gemiddeld risico, IP-adreslanden met hoog en gemiddeld risico, postcodes met hoog en gemiddeld risico, besteltijden met hoog en gemiddeld risico*

BELANGRIJK

We raden het ten zeerste aan de volgende scorecriteria in te stellen op 'Block transaction' (Transactie blokkeren) op de pagina 'Scoring' (Scores):

- Kaart op zwarte lijst
- Anonieme proxy (onder IP-adresland)

6 Dispute

Het accepteren van transacties in om het even welke omgeving houdt inherente risico's in, zoals het risico op chargebacks. Vooral bij verwerking in een omgeving waar de kaart niet aanwezig is (Card-Not-Present, CNP) is het risico op chargebacks altijd aanwezig.

Bij KBC/CBC-Paypage beschikken klanten over een geschillenpagina, wat handelaars in staat stelt transactiegegevens toe te voegen aan de zwarte en witte lijst met de juiste oorzaak van het geschil. Dit beschermt handelaars tegen verdere fraude en herhaaldelijk misbruik. Het verbetert ook de Fraud Expert-database van KBC/CBC-Paypage en de werking ervan.

IMPORTANT

Selecteer alleen "werkelijke fraude" wanneer u een chargeback hebt ontvangen met een fraudeoorzaakcode.

6.1 Transactiegegevens toevoegen aan een zwarte en witte lijst

1. Klik op de "PAYID" onder de transactieweergave om te zoeken naar de transacties die u wilt melden als commercieel geschil, werkelijke fraude of vermoeden van fraude.
2. Klik op de knop "DISPUTE" (geschil) om de ontvangen transactiegegevens weer te geven die kunnen worden toegevoegd aan de zwarte en witte lijst.
3. Ga naar de geschillenpagina en kies de lijst waaraan u de transactiegegevens wilt toevoegen (zwarte lijst of witte lijst). Kies vervolgens de oorzaak van het geschil.

   U kunt de transactie als volgt markeren:

   - Commercieel geschil, dit zijn alle door de handelaar ontvangen chargebacks die geen verband houden met fraude.
   - Werkelijke fraude, wanneer u een chargeback ontvangt als gevolg van fraude.
   - Vermoeden van fraude, wanneer u een frauduleuze transactie vermoedt en wilt voorkomen.

   Afhankelijk van welke knop u selecteert, verschillen de gevolgen voor de fraudedatabase.

   Opmerking: Werkelijke fraude geldt alleen voor chargebacks als gevolg van fraude.
4. Sla op en bevestig om de gegevens aan de juiste lijst toe te voegen. De fraudecontrole vindt onmiddellijk plaats.

Vanaf de geschillenpagina kunt u ook de gegevens selecteren (bv. van uw callcenter, VIP-client enz.) die u aan de witte lijst wilt toevoegen. Als u gegevens selecteert die voordien tot de zwarte lijst behoorden, worden deze automatisch toegevoegd aan de witte lijst. De fraudecontrole vindt onmiddellijk plaats.

7 Feedback

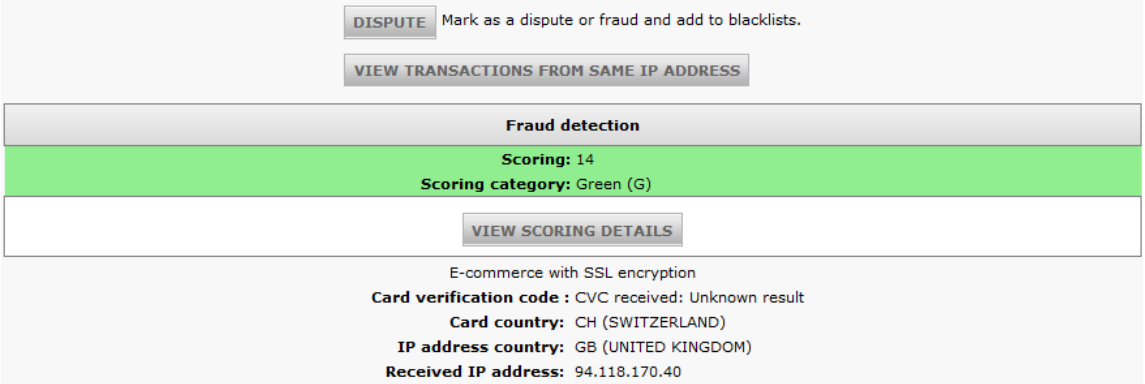
7.1 Transactieweergaven in de backoffice

7.1.1 Geavanceerde selectiecriteria

Wanneer u een transactie opzoekt via de koppeling 'Transacties weergeven' of 'Financiële historiek' in uw accountmenu, hebt u twee extra criteria onder 'Geavanceerde selectiecriteria': Risicocategorie en IP-adres. Onder Scoring (Scores) kunt u uit drie categorieën kiezen: Rood, Oranje, Groen. U kunt het veld IP-adres gebruiken om alle transacties op te zoeken van hetzelfde IP-adres of IP-adressen die met dezelfde cijfers beginnen.

7.1.2 Transactiedetails

In de transactiedetails (financiële pagina) ziet u extra informatie, zoals het resultaat van de CVC-controle (indien de CVC door de klant is ingevoerd), het land van de kaartuitgever, het IP-adresland en het ontvangen IP-adres. U ziet ook de eindscore en de scorecategorie, samen met de knop om scoredetails weer te geven, als u meer informatie wilt over de score.



Boven de tabel ziet u twee knoppen met de extra informatie: 'Dispute' (Geschil) en 'View transactions from same IP address' (Transacties van hetzelfde IP-adres weergeven)

7.1.2.1 Geschil

Met de knop 'Dispute' (Geschil) opent u een pagina waar u bepaalde transactiegegevens aan uw zwarte lijsten kunt toevoegen. Met deze optie kunt u bijvoorbeeld het kaartnummer voor de transactie aan uw zwarte lijst toevoegen zonder het volledige kaartnummer te weten.

U kunt ook de transactie markeren als commercieel geschil of fraude.

BELANGRIJK

Selecteer alleen 'actual fraud' (werkelijke fraude) als de klant daadwerkelijk fraude met deze kaart heeft gepleegd, bijvoorbeeld wanneer een kaarthouder een kaart gebruikt die hem niet toebehoort.

7.1.2.2 Transacties van hetzelfde IP-adres weergeven

Wanneer u op de knop Transacties van hetzelfde IP-adres weergeven klikt, wordt een lijst weergegeven met alle transacties die van hetzelfde IP-adres afkomstig zijn binnen een bepaalde periode.

7.1.2.3 Scoredetails weergeven

Wanneer u op de knop 'View scoring details' (Scoredetails weergeven) klikt, kunt u extra informatie raadplegen over de scoreberekening. U ziet een lijst met scorecriteria die in de berekening werden opgenomen, samen met het scoreresultaat. Criteria waaraan werd voldaan, worden vet weergegeven in de criterialijst.

Analyse van fraudespoor

Op de pagina met scoredetails kunt u de transactie vergelijken met transacties die zijn geregistreerd met hetzelfde kaartnummer, BIN, IP-adres, e-mailadres, naam van kaarthouder, creditcardland en IP-adresland binnen een bepaalde periode die u hebt ingesteld.

U kunt één of meerdere zoekcriteria aanvinken en de logische operator selecteren die u wilt toepassen op de geselecteerde zoekcriteria (AND of OR). Wanneer u op de knop 'Start lookup' (Zoeken starten) klikt, worden alle transacties die aan de geselecteerde criteria voldoen opgehaald. Alle transacties worden doorzocht vanaf het moment dat u met de zoekopdracht begint (niet vanaf de oorspronkelijke transactiedatum!).

De eerste zoekopdracht is gebaseerd op de waarden van de oorspronkelijke transactie, dus voor elk criterium wordt één waarde gecontroleerd. Wanneer u de volgende zoekopdracht uitvoert ('Start look-up 2' (Zoekopdracht 2 starten), 'Start look-up 3' (Zoekopdracht 3 starten) enz.), zoeken we in de resultaten van de vorige zoekopdracht. In achtereenvolgende zoekopdrachten kunnen de criteria meerdere waarden hebben, wat de resultaten vermenigvuldigt en mogelijke fraudesporen onthult.

7.1.3 Foutcodes

Wanneer een transactie door ons systeem wordt vastgehouden, op basis van de regels die u in de fraudedetectiemodule hebt ingesteld, vindt u de reden in het foutbericht voor de transactie. Op een paar uitzonderingen na beginnen alle foutcodes met betrekking tot fraudedetectie met '300011', gevolgd door nog twee cijfers.

More information about statuses and error codes can be found in your KBC/CBC-Paypage account. Just log in and go to: Support > Integration & user manuals > User guides > List of the payment statuses and error codes.

De volgende oneindige lijst bevat voorbeelden van de meest relevante foutcodes:

3 / 30001100 Niet-geautoriseerd land van klant

3 / 30001120 IP-adres staat op de zwarte lijst van de handelaar

3 / 30001130 BIN staat op de zwarte lijst van de handelaar

3 / 30001140 Kaart staat op de zwarte lijst van de handelaar

3 / 30131002 U hebt het toegestane totaalbedrag bereikt

3 / 30001102 Aantal verschillende landen te hoog

3 / 30001141 E-mailadres staat op de zwarte lijst

3 / 30001142 Naam van passagier staat op de zwarte lijst

3 / 30001143 Naam zwarte lijst

3 / 30001144 Naam van passagier wijkt af van naam van eigenaar

3 / 30001145 Tijd tot vertrek te kort

3 / 30001154 U hebt de toegestane gebruikslimiet bereikt

3 / 30001155 U hebt de toegestane gebruikslimiet bereikt

3 / 30001180 U hebt de maximumscore bereikt

7.2 Aanvullende transactieparameters

In uw verzoeken na de verkoop, doorverwijzingen met feedback, gedownloade bestanden en DirectLink XML-reacties, worden aanvullende transactieparameters voor scores geretourneerd.

De lijst met aanvullende parameters staat hieronder. Deze velden zijn leeg als er een indelingsvalidatiefout is opgetreden voor de transactiedetails.

Parameter	Waarde
IPCTY	IP-adresland. Indeling: alfabetische ISO-code van 2 tekens. Als deze parameter niet beschikbaar is, wordt '99' in het antwoord geretourneerd. Deze IP-controle is gebaseerd op extern aangeleverde IP-lijsten, er bestaat dus een bepaald risico aangezien we vertrouwen op de nauwkeurigheid van die lijsten. In 94 % van de gevallen geeft deze controle een positief resultaat.
CCCTY	Land van uitgifte van creditcard. Dit is alleen beschikbaar voor VISA, MasterCard, American Express en Diners Club. Deze waarde is leeg voor alle merken/betaalmethoden. Indeling: alfabetische ISO-code van 2 tekens. Als deze parameter niet beschikbaar is, wordt '99' in het antwoord geretourneerd. Deze controle op land van kaartuitgever is gebaseerd op extern aangeleverde lijsten, er bestaat dus een bepaald risico aangezien we vertrouwen op de nauwkeurigheid van die lijsten. In 94 % van de gevallen geeft deze controle een positief resultaat.
ECI	Electronic Commerce Indicator. De mogelijke ECI-waarden en hun betekenissen worden hieronder beschreven: 1 Handmatig met sleutel 2 Periodieke betalingen 3 Afbetalingen in termijnen 5 Identificatie van kaarthouder geslaagd 6 Handelaar ondersteunt identificatie maar niet de kaarthouder, regels van voorwaardelijke betalingsgarantie zijn van toepassing (zie hier) 7 E-commerce met SSL-codering 9 Periodieke betalingen na eerste e-commercetransactie

Parameter	Waarde
	12 Handelaar ondersteunt identificatie maar niet de kaarthouder, regels van voorwaardelijke betalingsgarantie zijn van toepassing (zie hier) (idem 6) 91 Identificatie van kaarthouder MISLUKT!!!! (Voorwaardelijke betalingsgarantie (zie hier) kan van toepassing zijn. Raadpleeg uw acquirer) 92 Authenticatiewebsite voor uitgevende bank is tijdelijk niet beschikbaar, maar de transactie wordt verwerkt
CVCCHECK	Resultaat van de CVC-controle. Mogelijke waarden: KO De CVC is verzonden, maar de acquirer heeft een negatief antwoord gegeven op de CVC-controle, m.a.w. de CVC is niet correct. OK 1. De CVC is verzonden en de acquirer heeft een positief antwoord gegeven op de CVC-controle, dat wil zeggen dat de CVC correct is OF 2. De acquirer heeft een autorisatiecode gestuurd, maar heeft geen specifiek resultaat voor de CVC-controle geretourneerd. NO Alle overige gevallen. Bijvoorbeeld als er geen CVC is opgegeven, de acquirer heeft geantwoord dat er geen CVC-controle mogelijk was, de acquirer de autorisatie heeft geweigerd, maar geen specifiek resultaat heeft opgegeven voor de CVC-controle enz.
AAVCHECK	Resultaat van de automatische adresverificatie. Deze verificatie is momenteel alleen beschikbaar voor American Express. Mogelijke waarden: KO Het adres is verzonden, maar de acquirer heeft een negatief antwoord gegeven op de adrescontrole, dat wil zeggen dat het adres niet correct is. OK 1. Het adres is verzonden en de acquirer heeft een positief antwoord gegeven op de adrescontrole, dat wil zeggen dat het adres correct is OF 2. De acquirer heeft een autorisatiecode gestuurd, maar heeft geen specifiek resultaat voor de adrescontrole geretourneerd. NO Alle overige gevallen. Bijvoorbeeld als er geen adres is opgegeven, de acquirer heeft geantwoord dat er geen adrescontrole mogelijk was, de acquirer de autorisatie heeft geweigerd, maar geen specifiek resultaat heeft opgegeven voor de adrescontrole enz.
VC	Virtuele kaart. Mogelijke waarden: ECB: voor E Carte Bleue ICN: voor Internet City Number NO: Alle overige gevallen. De kaart is bijvoorbeeld geen virtuele kaart, is onbekend virtueel-kaarttype enz.
IP	Het IP-adres van de klant zoals door ons systeem is gedetecteerd in een 3-laagsintegratie of door de handelaar aan ons gestuurd in een 2-laagsintegratie.

Geavanceerde velden

NBRUSAGE	Aantal keren dat een creditcard werd gebruikt tijdens een bepaalde periode (wanneer de regel “maximumgebruik per kaart, per periode” is geconfigureerd).
NBRIPUSAGE	Aantal keren dat een IP-adres werd gebruikt tijdens een bepaalde periode (wanneer de regel 'maximum utilisation per IP address, per period' (maximumgebruik per IP-adres, per periode) is geconfigureerd).
SCORING (SCORES)	De eindscore voor de transactie, m.a.w. het totaal van de scores die aan alle items in de in scorelijst werden gegeven
SCO_CATEGORY	De kleur van de categorie waartoe de eindscore hoort, gebaseerd op de instellingen op de scorepagina ('Multi-criteria selection of payment methods > Scoring' (Meerdere criteria selecteren voor betaalmethoden > Scores)). De mogelijke waarden zijn G (voor groen), O (voor oranje) en R (voor rood).

More information about these fields can be found in your KBC/CBC-Paypage account. Just log in and go to: Support > Integration & user manuals > Technical guides > Parameter Cookbook.

8 Bijlage: Parameters versus controles/regels

KBC/CBC-Paypage parameter	Omschrijving	Regels/controles in FDMA
CN	De naam van de kaarthouder mag maximaal 35 tekens bevatten. Deze parameter kan via KBC/CBC-Paypage e-Commerce, DirectLink en Batch worden verzonden. Let op: voor KBC/CBC-Paypage e-Commerce wordt de naam van de kaarthouder ook geregistreerd via de KBC/CBC-Paypage-betalingspagina, waar de naam van de kaarthouder een verplicht veld is.	• Naam zwarte lijst • Naam grijze lijst • Naam van passagier verschilt van naam van kaarthouder.
OWNERADDRESS	De naam van de klant mag maximaal 35 tekens bevatten.	• Het factuuradres is een postbus.
ADDRMATCH	Of het factuuradres wordt gezien als afwijkend van het afleveradres hangt af van de waarde van het extra veld “ADDRMATCH” dat de handelaar ons in de bestelgegevens stuurt. Als de waarde “1” is, worden het factuur- en het afleveradres als identiek beschouwd. Als de waarde “0” is, worden ze als afwijkend beschouwd.	• Factuuradres verschilt van afleveradres
OWNERZIP	De postcode van de klant mag maximaal 10 tekens bevatten.	• Riskante postcodes • Geavanceerde adresverificatie alleen voor specifieke kaartmerken
OWNERTELNO	Telefoonnummer van de klant kan maximaal 30 tekens bevatten voor alle KBC/CBC-Paypage modules, met uitzondering van KBC/CBC-Paypage Batch, dat een maximum van 20 tekens heeft. Speciale tekens (“+” of “/” bijvoorbeeld) zijn toegestaan in dit veld. Het is raadzaam telefoonnummers op een consistente manier te verzenden.	• Telefoonnummer op grijze lijst • Telefoonnummer op zwarte lijst
OWNERCTY	Het land van de factuur van de klant mag maximaal 2 tekens bevatten. Het land in ISO 3166-1-alpha-2-code kan worden gevonden op http://www.iso.org/iso/en/prodsservices/iso3166ma/02iso-3166-code-lists/list-en1.html.	• Aantal verschillende landen
EMAIL	Het e-mailadres van de klant mag maximaal 50 tekens bevatten.	• Witte lijst met e-mailadressen • E-mailadres op zwarte lijst • E-mailadres op grijze lijst • Gratis e-mail • Gebruikslimieten
Generic_BL	De algemene zwarte lijst mag maximaal 50 tekens bevatten.	• Algemene zwarte lijst • Algemene grijze lijst
REMOTE_ADDR	IP-adres van klant. Dit moet alleen worden verzonden wanneer KBC/CBC-Paypage DirectLink wordt gebruikt. Voor KBC/CBC-Paypage e-Commerce wordt het IP-adres automatisch gedetecteerd en geregistreerd.	• IP op witte lijst • IP op grijze lijst • IP op zwarte lijst • Gebruikslimieten • IP-landengroepen • Anonieme proxy • Niet-geautoriseerde combinatie van land kaartuitgever / IP-land • IP-land wijkt af van land kaartuitgever
CUID	Uniek klant-ID Mag maximaal 50 tekens bevatten.	• Uniek klant-ID op witte lijst

CARDNO	Kaart- of accountnummer mag maximaal 21 tekens bevatten. Dit moet alleen worden verzonden wanneer KBC/CBC-Paypage DirectLink wordt gebruikt. Voor KBC/CBC-Paypage e-Commerce wordt het kaartnummer automatisch gedetecteerd en geregistreerd.	• Kaart op grijze lijst • Kaart op zwarte lijst • BIN op zwarte lijst • BIN op grijze lijst • Land kaartuitgever met hoog risico • Land kaartuitgever met gemiddeld risico • Gebruikslimieten
ECOM_SHIPTO_POSTAL_POSTALCODE	Afleverpostcode. Mag maximaal 10 alfanumerieke tekens bevatten.	• Riskante postcodes
ECOM_BILLTO_POSTAL_POSTALCODE	Postcode factuuradres	• Riskante postcodes • Geavanceerde adresverificatie alleen voor specifieke kaartmerken
	LUCHTVAARTMAATSCHAPPIJ/REISGEGEVENS	
AIPASNAME	Naam hoofdpassagier De standaardwaarde is de naam van de creditcardhouder.	• Naam zwarte lijst • Naam grijze lijst • Naam van passagier verschilt van naam van kaarthouder
AIEXTRAPASNAME1	Naam van extra passagier voor PNR's met meerdere passagiers. Dit veld kan maximaal 5 keer worden herhaald (bijvoorbeeld voor 5 extra passagiers), waarbij u het cijfer aan het einde van de veldnaam wijzigt.	• Naam zwarte lijst • Naam grijze lijst • Naam van passagier verschilt van naam van kaarthouder
AIORCITY1	luchthavens van vertrek (kort) is een verplicht veld en mag maximaal 5 tekens bevatten.	• Luchthaven van vertrek niet op lijst vertrouwde luchthavens • Riskant reisschema (luchthavengroepen) • Niet-geautoriseerd IP-land voor reisschema
AIORCITYL1	Luchthaven van vertrek (lang) is een verplicht veld en mag maximaal 20 tekens bevatten.	• Luchthaven van vertrek niet op lijst vertrouwde luchthavens • Riskant reisschema (luchthavengroepen) • niet-geautoriseerd IP-land voor reisschema
AIDESTCITY1	Luchthaven van aankomst (kort) is een verplicht veld en mag maximaal 5 tekens bevatten.	• Riskant reisschema (luchthavengroepen) • Niet-geautoriseerd IP-land voor reisschema
AIDESTCITYL1	Luchthaven van aankomst (lang) is een verplicht veld en mag maximaal 20 tekens bevatten.	• Riskant reisschema (luchthavengroepen) • Niet-geautoriseerd IP-land voor reisschema
AISTOPOV1	Overstappen toegestaan voor luchthaven. Mogelijke waarden: de hoofdletters O en X. O: de passagier mag stoppen en blijven. X: de passagier mag niet blijven.	• Riskant reisschema (luchthavengroepen)

AIFLDATE1	Vluchtdatum.	• Tijd tot vertrek 1 • Tijd tot vertrek 2 • Tijd tot vertrek 3

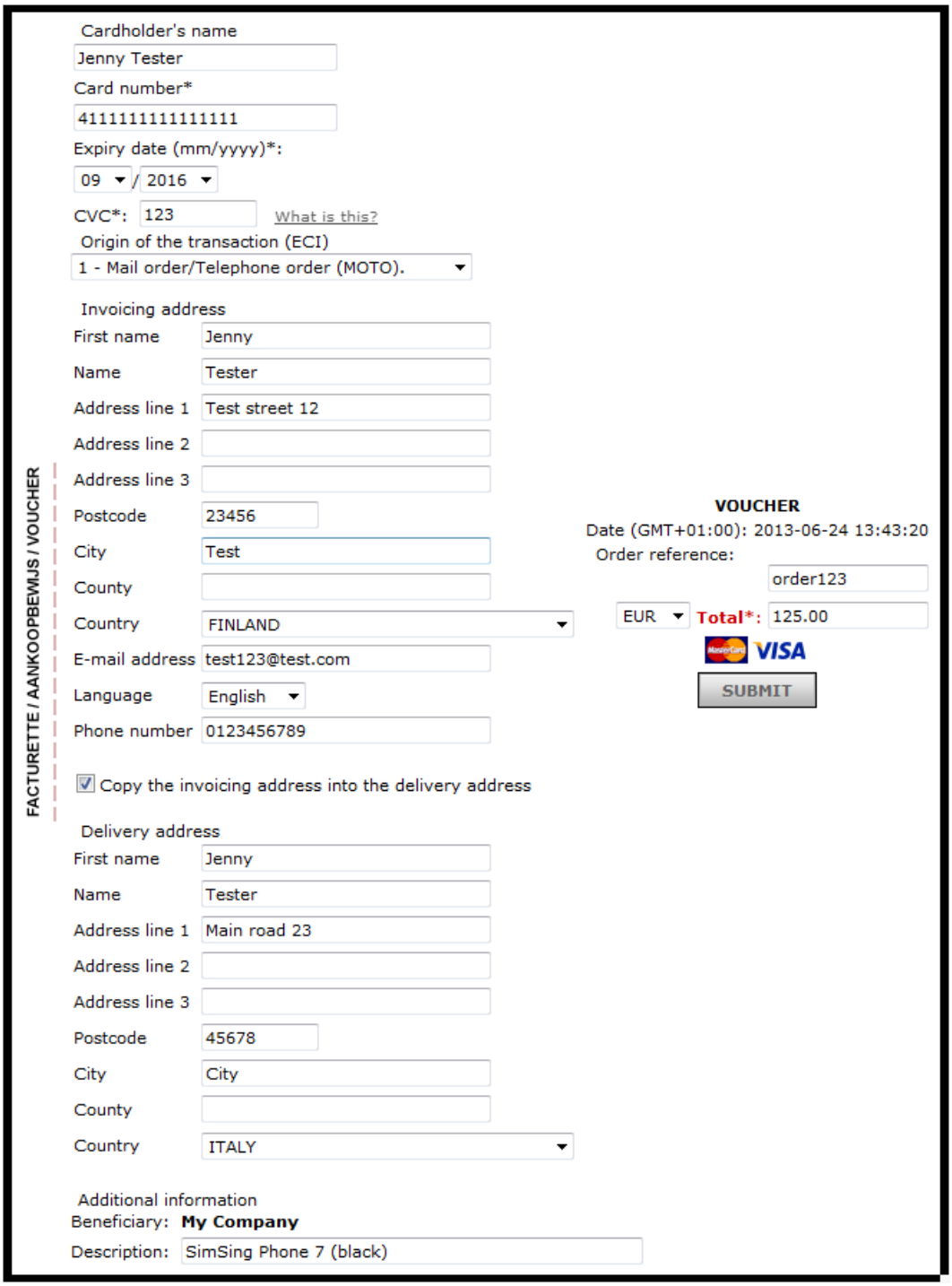
De bovenstaande lijst met reisparameters bevat alleen de parameters die zijn gekoppeld aan regels/ controles in de FDMA-module. Voor de volledige lijst met verplichte reisparameters kunt u de bijlage Speciale reisindeling raadplegen in onze handleiding voor DirectLink of Advanced e-Commerce .

9 Bijlage: Extra gegevens via e-Terminal (MOTO)

Als u onze oplossing MOTO e-Terminal gebruikt naast de standaard bestelgegevens, kunt u ook contact-/ adresgegevens invoeren. Er wordt met deze gegevens rekening gehouden voor de FDMA, waardoor uw fraudepreventie wordt verbeterd.

Selecteer in uw backoffice onder 'Operations' (Bewerkingen) de optie 'New transaction' (Nieuwe transactie). U ziet de voucher waarin u de standaardgegevens (naam, kaartnummer, CVC enz.) kunt invoeren.

U ziet de aanvullende factuur- en afleveradresgegevens:



10 Bijlage: CVC2 en AAV

10.1 CVC2

CVC2 is een authenticatieprocedure die door creditcardbedrijven wordt gebruikt ter preventie van creditcardfraude bij internettransacties. Naargelang het merk heeft deze code een andere naam (CVC2 of Card Validation Code (kaartvalidatiecode) voor MasterCard, CVV2 of Card Verification Value (kaartverificatiecode) voor VISA, CID of Card Identification Number (kaartidentificatienummer) voor American Express). De code wordt echter doorgaans 'CVC' genoemd. De functionaliteit van de CVC2 is dezelfde voor alle merken.

De verificatiecode is een unieke code die is gekoppeld aan het kaartnummer, maar is geen onderdeel van het kaartnummer zelf. Afhankelijk van het merk van de kaart is de verificatiecode een code van 3 of 4 cijfers op de voor- of achterkant van de kaart, een uitgiftenummer, een ingangsdatum of een geboortedatum. Voor MasterCard en VISA staat bijvoorbeeld een code van 3 cijfers op de achterkant van de kaart in de handtekeningstrook, achter het volledige rekeningnummer of de laatste 4 cijfers van het rekeningnummer.

Het is strikt verboden voor handelaaars en PSP's om de CVC2-codes van klanten in een database op te slaan. Wanneer de kaarthouder niet persoonlijk aanwezig is, dat wil zeggen voor transacties zonder creditcard, en hem wordt gevraagd zijn CVC2-code en zijn kaartnummer in te voeren, helpt deze verificatiecode bepalen of de klant die de bestelling plaatst de kaart in zijn bezit heeft en of de rekening van de kaart legitiem is.

10.2 AAV/AVS

AAV is een authenticatieprocedure die beschikbaar is op sommige markten en wordt gebruikt ter preventie van creditcardfraude bij internettransacties. Afhankelijk van het merk, heeft deze authenticatieprocedure een andere naam (AVS of Address Verification Service/System voor VISA/MasterCard; AAV of Automated Address Verification voor American Express), maar functionaliteit van de AAV is hetzelfde voor alle merken.

De adrescontrole vindt plaats wanneer de acquirer de kaartuitgever verzoekt de numerieke componenten (huisnummer en postcode) van het adres van de klant (factuur of levering) die door de handelaar is gestuurd te vergelijken met die van het factuuradres dat door de klant is verstrekt aan de kaartuitgever bij de aanvraag voor de kaart.

American Express voert deze controle automatisch uit wanneer ze adresgegevens bij een transactie ontvangen. Het hangt ervan af of de acquirer de adrescontrole al dan niet uitvoert. Onder alle omstandigheden is het raadzaam het adres van de klant samen met de bestelgegevens naar ons systeem te sturen.

Hoewel een transactie niet wordt geweigerd vanwege het resultaat van een adrescontrole, kan de handelaar deze uitkomst wel gebruiken om te beslissen of de bestelling wordt geleverd of de klant om meer informatie vraagt vóór verzending.

Opmerking: De simulaties in AAV/AVS-controles werken niet zoals verwacht in een TEST-omgeving.

10.3 Score aanpassen op basis van AAV/AVS-resultaat

Op basis van de uitkomst van de AAV/AVS, kunt u de FDMA-score beïnvloeden. U kunt selecteren welke actie u ons systeem wilt laten toepassen per mogelijk antwoord:

Antwoord	Actie
Resultaat OK	Geen / Waarde aftrekken van risicoscore
Resultaat KO	Geen / Waarde toevoegen aan risicoscore / Controle opleggen / Blokkeren (controle indien in de modus 'Direct sale' (Rechtstreekse verkoop))
Postcode KO, Adres OK	Geen / Waarde toevoegen aan risicoscore / Controle opleggen / Blokkeren (controle indien in de modus 'Direct sale' (Rechtstreekse verkoop))

Antwoord	Actie
Postcode OK, adres KO	Geen / Waarde toevoegen aan risicoscore / Controle opleggen / Blokkeren (controle indien in de modus 'Direct sale' (Rechtstreekse verkoop))
Resultaat niet ontvangen of onbekend	Geen / Waarde toevoegen aan risicoscore / Controle opleggen

Opmerking

Het antwoord 'Result not received or unknown' (Resultaat niet ontvangen of onbekend) kan worden optreden wanneer uw acquirer de AAV/AVS-controle ondersteunt, maar de uitgever van de klant (bank) niet. Overweeg dit bij de configuratie van de FDMA.

11 Bijlage: Tips voor fraudemeldingen

Creditcardfraude moet door de kaarthouder zelf aan zijn uitgevende bank worden gemeld. Dat is de bank waar hij zijn creditcard heeft aangevraagd.

Als een handelaar een van zijn klanten verdenkt van fraude, moet hij dat melden aan zijn acquirer.

Als een handelaar een oplichter bij de politie wilt aangeven, heeft hij het creditcardnummer niet nodig. De informatie die nuttig is voor de politie, is het IP-adres van de klant dat tijdens de transactie is gebruikt, met de datum, tijd en tijdzone. Als de handelaar het afleveradres aan die informatie kan toevoegen, is de politie beter in staat de oplichter op te sporen. Let op: het IP-adres kan nep zijn en het afleveradres kan slechts het adres van een tussenpersoon zijn die de artikelen naar het buitenland moet sturen. Dit maakt het lastiger voor de politie om de oplichter op te sporen.

12 Bijlage: Groepsconfiguratie en zwarte lijst delen

Handelaars met een groepsaccount, waarbij verschillende individuele accounts (PSPID's) onder één hoofdaccount zijn opgenomen, kunnen profiteren van overlappende PSPID-fraudebeheeropties.

Deze opties stellen de handelaar in staat om:

- Zwarte lijsten, grijze lijsten en witte lijsten te delen tussen de verschillende PSPID's die in de groepsaccount van de handelaar zijn opgenomen.
- De configuratie van de FDMA te delen (criteria, regels, limieten enz.) en lijsten (landgroepen, riskante postcodes enz.)

Activering

- Als u Group Manager gebruikt en groepfraudeconfiguratie en delen wilt inschakelen, kunt u contact opnemen met our Customer Care
- Als u Group Manager nog niet gebruikt, maar diverse PSPID's hebt, kunt u deze samenvoegen in één groepsaccount om groepfraudeconfiguratie en delen te kunnen gebruiken. Neem voor meer informatie contact op met ons Customer Care Team .

13 Bijlage: Deactiveringsmechanisme

De volgende tabel bevat alle deactiveerbare criteria:

Criterium	Deactiveerbaar door 3-D Secure/CUI op witte lijst/Witte lijst met e-mailadressen	Deactiveerbaar door IP-adres op witte lijst
Adres is een postbus Box	✓	
Bedrag - hoger dan bereik	✓	
Bedrag - lager dan bereik	✓	
BIN op zwarte lijst	✓	
BIN op grijze lijst	✓	
Kaartland - hoog risico	✓	
Kaartland - middelhoog risico	✓	
Kaart op grijze lijst	✓	
Submerk kaart - hoog risico	✓	
Submerk kaart - middelhoog risico	✓	
Naam van kaarthouder op zwarte lijst met namen – gedeeltelijke overeenkomst	✓	
Naam van kaarthouder op zwarte lijst met namen – volledige overeenkomst	✓	
Naam van kaarthouder op grijze lijst met namen – gedeeltelijke overeenkomst	✓	
Naam van kaarthouder op grijze lijst met namen – volledige overeenkomst	✓	
Gegevens op generische zwarte lijst	✓	
Gegevens op generische grijze lijst	✓	
Digitale authenticatie niet ontvangen	✓	
Digitale authenticatie standaard niet vereist	✓	
Digitale authenticatie niet vereist - transactie Niveau	✓	
Categorie Digitale authenticatie-profiel – hoog risico	✓	
Categorie Digitale authenticatie-profiel – verdacht	✓	
E-mailadres op zwarte lijst - gedeeltelijke overeenkomst	✓	
E-mailadres op zwarte lijst - volledige overeenkomst	✓	
E-mailadres op grijze lijst - gedeeltelijke overeenkomst	✓	
E-mailadres op grijze lijst - volledige	✓	

Criterium	Deactiveerbaar door 3-D Secure/CUI op witte lijst/Witte lijst met e-mailadressen	Deactiveerbaar door IP-adres op witte lijst
overeenkomst		
Expertscore niet beschikbaar	✓	
Eerste luchthaven van vertrek niet op lijst vertrouwde luchthavens	✓	
Gratis e-mail	✓	
Factuuradres anders dan leveringsadres	✓	
IP-adres op zwarte lijst	✓	✓
IP-adres op grijze lijst	✓	✓
IP-land - anonieme proxy	✓	✓
IP-land - hoog risico	✓	✓
IP-land - middelhoog risico	✓	✓
IP-land anders dan kaartland	✓	✓
Nummer uitgever - hoog risico	✓	
Nummer uitgever - middelhoog risico	✓	
Max. bedrag/kaart - hoge drempel	✓	
Max. bedrag/kaart - middelhoge drempel	✓	
Max. e-mailgebruik - hoge drempel	✓	
Max. e-mailgebruik - middelhoge drempel	✓	
Max. IP-gebruik alle statussen - hoge drempel	✓	✓
Max. IP-gebruik alle statussen - middelhoge drempel	✓	✓
Max. gebruik/kaart - hoge drempel	✓	
Max. gebruik/kaart - middelhoge drempel	✓	
Max. gebruik/IP - hoge drempel	✓	✓
Max. gebruik/IP - middelhoge drempel	✓	✓
Aantal verschillende landen	✓	
Ticket enkele reis	✓	
Passagiersnaam verschilt van naam kaarthouder	✓	
Passagiersnaam op zwarte lijst met namen – gedeeltelijke overeenkomst	✓	
Passagiersnaam op zwarte lijst met namen – volledige overeenkomst	✓	
Passagiersnaam op grijze lijst met namen – gedeeltelijke overeenkomst	✓	

Criterium	Deactiveerbaar door 3-D Secure/CUI op witte lijst/Witte lijst met e-mailadressen	Deactiveerbaar door IP-adres op witte lijst
Passagiersnaam op grijze lijst met namen – volledige overeenkomst	✓	
Telefoon op zwarte lijst - gedeeltelijke overeenkomst	✓	
Telefoon op grijze lijst - gedeeltelijke overeenkomst	✓	
Postcode en adres - hoog risico	✓	
Postcode en adres - middelhoog risico	✓	
Productcategorie - hoog risico	✓	
Productcategorie - middelhoog risico	✓	
Risicotraject (groepen luchthavens) - luchthaven met hoog risico	✓	
Risicotraject (groepen luchthavens) - luchthaven met middelhoog risico	✓	
Verzendingsmethode - hoog risico	✓	
Verzendingsmethode - middelhoog risico	✓	
Gegevens verzendingsmethode - hoog risico	✓	
Gegevens verzendingsmethode - middelhoog risico	✓	
Tijdstip van de bestelling - periode met hoog risico	✓	
Tijdstip van de bestelling - periode met middelhoog risico	✓	
Levertijd - strikt minder dan X uur	✓	
Levertijd - strikt minder dan Y uur	✓	
Levertijd - strikt minder dan Y uur	✓	
Vertrektijd - strikt minder dan X dagen	✓	
Vertrektijd - strikt minder dan Y dagen	✓	
Vertrektijd - strikt minder dan Z dagen	✓	
Niet geautoriseerde combinatie kaartland/IP-land - hoog risico	✓	✓
Niet geautoriseerde combinatie kaartland/IP-land - middelhoog risico	✓	✓
IP-land niet geautoriseerd voor traject	✓	✓

Opmerking:
- Het criterium “Card in blacklist” (kaart op zwarte lijst) kan nooit worden gedeactiveerd.
- De post-acquirer-regels (AVS/CVC) worden niet gedeactiveerd.
- De scorecategorie (blokkeren of controleren) kan worden gedeactiveerd door de criteria 3-D Secure/CUI op witte lijst, en witte lijst met e-mailadressen.
- Er worden drie punten toegevoegd aan de score, zelfs als een controleregel wordt gedeactiveerd.