Fraude Detectie Module

Configuratiegids voor de Fraude Detectie Module v.4.2.3

Inhoud

1 Wat is de Fraudedetectiemodule?

Bij e-commerce vereist de fraudebestrijding het maximale niveau aan kennis, snelheid en flexibiliteit. Om u te helpen tijdens het uitvoeren van effectief risicomanagement, biedt de Fraudedetectiemodule u een real-time service aan die alle noodzakelijke analyse-informatie en een op maat gemaakte bescherming levert voor het omgaan met dubieuze transacties.

Het gebruik van de Fraudedetectiemodule garandeert echter niet de eliminatie van alle fraude. Het helpt enkel bij het bemoeilijken van fraudepleging. De Fraudedetectiemodule kan geconfigureerd worden op basis van risico's of fraudegevallen waarmee u, als bedrijf, bent geconfronteerd.

1.1 Voordelen

De Fraudedetectiemodule laat u toe om:

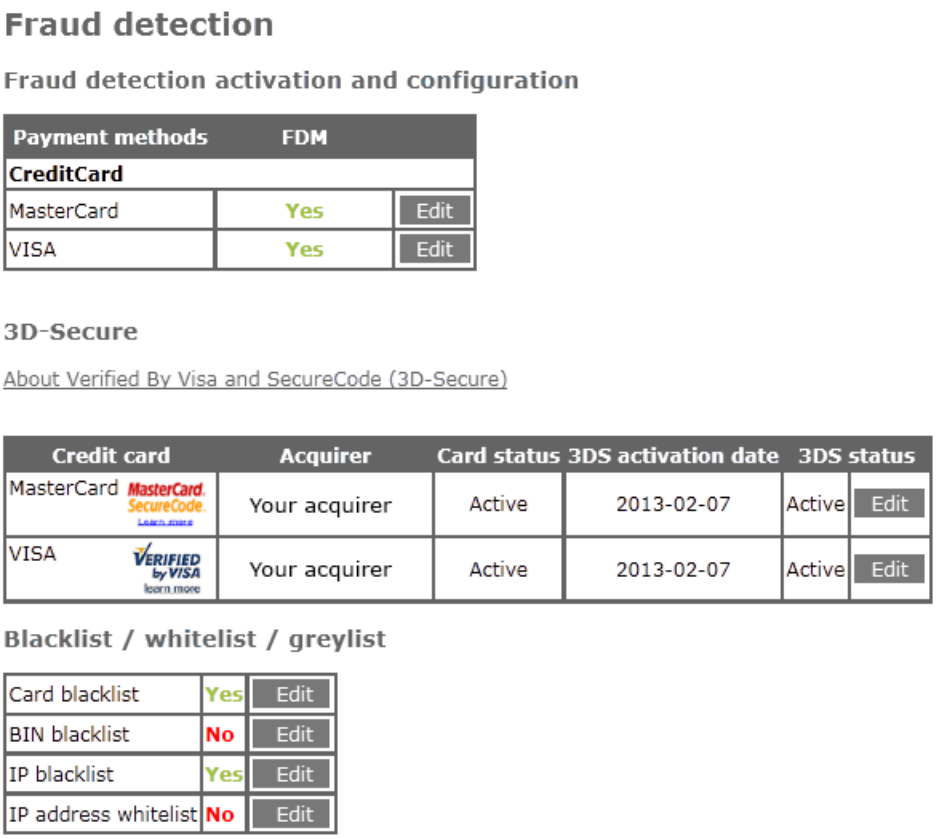
- Afwijkingen tijdens transacties te detecteren
- Pogingen van erkende fraudeurs onmiddellijk te blokkeren
- U te beschermen tegen landspecifieke risico's
- Een volledig op maat gemaakt beveiligingsbeleid te definiëren en toe te passen
- Baat te vinden bij voorwaardelijke betalingsgaranties (zie onderdeel 2.1.2) in overeenstemming met het individuele acquirer beleid (3-D Secure).

1.2 Toegang

U kunt toegang verkrijgen tot de Fraudedetectiemodule via de link "Fraudedetectie" (of Fraud detection) in het menu van uw account.

1.3 Inhoud

De Fraudedetectiemodule bestaat uit drie afzonderlijke functionele gebieden: "Activering en configuratie van fraudedetectie", "3-D Secure" en "Zwarte lijst / witte lijst" (blacklist / whitelist)



Fraud detection

Fraud detection activation and configuration

Payment methods	FDM	
CreditCard		
MasterCard	Yes	Edit
VISA	Yes	Edit

3D-Secure

About Verified By Visa and SecureCode (3D-Secure)

Credit card	Acquirer	Card status	3DS activation date	3DS status	
MasterCard	Your acquirer	Active	2013-02-07	Active	Edit
VISA	Your acquirer	Active	2013-02-07	Active	Edit

Blacklist / whitelist / greylist

Card blacklist	Yes	Edit
BIN blacklist	No	Edit
IP blacklist	Yes	Edit
IP address whitelist	No	Edit

We zullen het configureren van de 3-D Secure modus operandi en de criteria voor VISA en MasterCard creditcards nader bekijken.

Belangrijk

De VISA/MasterCard criteria, zoals hier beschreven, zijn niet beschikbaar voor alle betaalmethoden. De beschikbaarheid van de “Activering en configuratie” hangt af van de betaalmethode. Voor sommige betaalmethoden is de configuratie beperkt tot de “Limieten” optie. Wij raden u aan de specifieke selectiecriteria voor uw individuele betaalmethoden te controleren. Dit kunt u doen door te klikken op de knop “Wijzig” naast de betaalmethode in de “Activering en configuratie van fraudedetectie” tabel in de Fraudedetectiemodule.

2 Activering en configuratie van fraudedetectie

In de “Activering en configuratie" tabel kunt u het verschil zien tussen creditcards en andere betaalmethoden.

Als optie zijn er blocking rules en limieten. “Nee” geeft aan dat er niets geconfigureerd is in de betreffende optiepagina. Wanneer een pagina reeds geconfigureerd is, dan zal de status “Ja” zijn.

We zullen nu de configuratie van fraudedetectie-opties voor creditcards nader bekijken.

2.1 Creditcards

Om de fraude detectie opties voor een specifieke creditcard te configureren, klik op de “Edit” knop naast de betaalmethode.

U zult dan naar de configuratiepagina, met tabs voor de blocking rules en limieten gaan.

2.1.1 Blocking rules

Blocking rules zijn toepasbaar nadat de klant zijn creditcard gegevens heeft ingevoerd en op de verwerkknop heeft geklikt.

Indien de transactie niet onder de regels valt die u heeft ingesteld, dan zullen wij de transactie tegenhouden en zijn status instellen op “Autorisatie geweigerd”.

2.1.1.1 IP-addressen van een land

Alle IP-adres landen worden standaard aanvaard. Ons systeem kan het IP-adres land identificeren op basis van het IP-adres van uw klant (hoewel deze controle positieve resultaten geeft in 94% van alle gevallen, is de IP-check gebaseerd op extern aangeleverde IP-lijsten, zodat er een klein risico bestaat aangezien er vertrouwd wordt op de juistheid van deze lijst).

Wanneer u een lijst van IP-adres landen wilt selecteren, dan kunt u deze selecteren in de lijst aan de rechterzijde van het scherm en klikken op “Toevoegen”.

BELANGRIJK

De A1 (Anonieme proxy), AP (Azië en het Stille-Oceaan gebied), EU (Europees netwerk) en A2 (Satelliet leveranciers) codes verwijzen naar IP-adressen van waar het land van oorsprong onduidelijk is.

EU, bijvoorbeeld, betekent dat het exacte IP-land onduidelijk is, maar behoort tot Europa. Het accepteren van de EU als IP-adres land betekent niet dat u betalingen aanvaardt van alle landen in Europa. Het betekent dat u betalingen aanvaard van IP-adressen die beheerd worden door Europese instellingen. Wanneer u betalingen wilt accepteren van landen in Azië of Europa, dan moet u deze landen één voor één toevoegen aan uw lijst.

Anonieme proxies zijn internetproviders die aan internetgebruikers toestaan om hun IP-adres te verbergen. Wij raden u aan om geen betalingen te accepteren van anonieme proxy's!

Bovenaan de lijst van geselecteerde IP-adres landen heeft u de optie om landen binnen uw lijst te accepteren (*Enkel betalingen aanvaarden van landen die in de lijst voorkomen*) of landen te weigeren (*Betalingen weigeren die hun oorsprong hebben in landen die in de lijst voorkomen*) in uw lijst.

U kunt altijd een land in de lijst verwijderen door te klikken op het “Del” vakje dat voor het land staat en vervolgens op de “Bevestigen” toets onderaan de lijst te drukken.

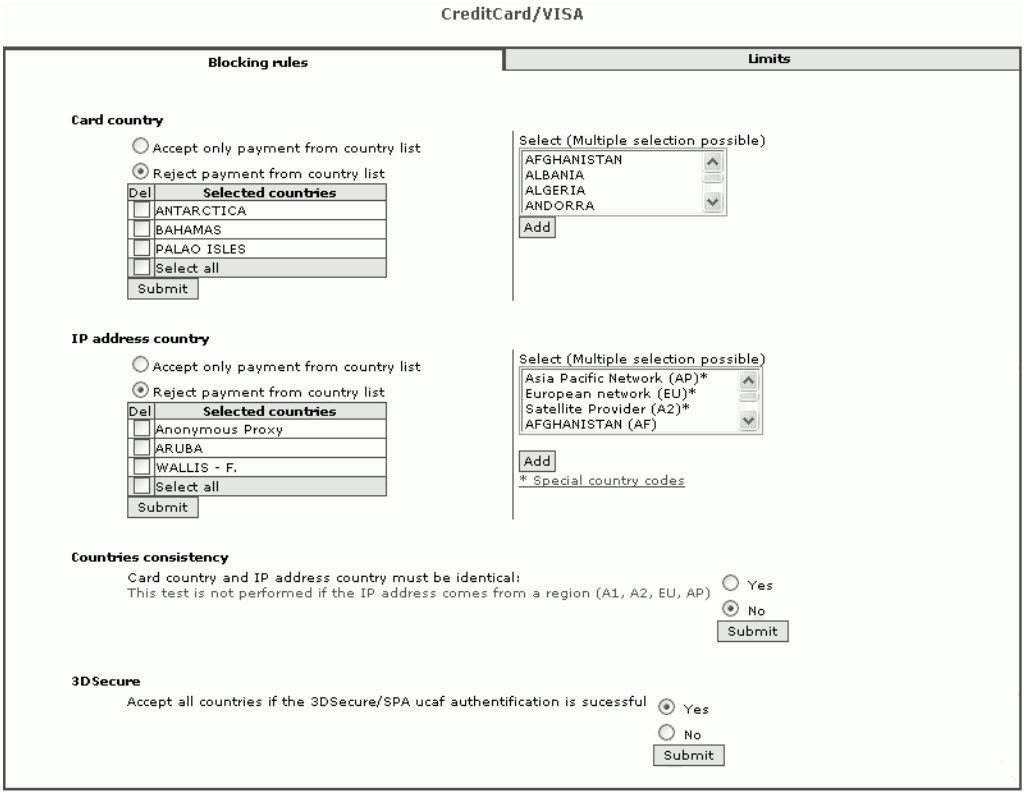
2.1.1.2 Coherentie tussen de landen (alleen voor Visa, MasterCard, American Express en Diners Club)

Wanneer u de parameter op “ja” instelt, dan accepteert u enkel transacties als het IP-adres van de klant in hetzelfde land is als zijn creditcard-uitgever, met andere woorden: alleen als het land van de creditcard en het land van het IP-adres overeenkomstig zijn. Deze controle wordt niet uitgevoerd indien het IP-adres van A1 (Anonieme proxy), AP (Azië en het Stille-Oceaan gebied), EU (Europees netwerk) of A2 (Satelliet leveranciers) afkomstig is.

2.1.1.3 3-D Secure (enkel voor Visa/MasterCard/JCB/AmEx)

Deze parameter laat u toe om de blocking rules te omzeilen wanneer een kaarthouder door 3-D Secure wordt geïdentificeerd.

Wanneer een creditcard 3-D Secure enrolled is en u een 3-D Secure contract heeft met uw acquirer, heeft u een voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) op de transactie. Dit betekent dat wanneer u geen betalingen wenst te ontvangen uit land X, vanwege een hoog risico op fraude, dan kunt u nog steeds transacties toelaten van creditcards die 3-D Secure zijn van land X, aangezien u geen risico loopt op disputen over niet-identificatie van de kaarthouder (hoewel dit niet toepasbaar is op andere disputen, zie hoofdstuk 2)



2.1.2 Limieten

In de Fraude Detectie Module kunt u het bedrag per transactie limiteren. U kunt een minimum en een maximum bedrag ingeven. Wanneer het transactiebedrag niet binnen deze limieten valt, zullen wij de transactie tegenhouden en de status instellen op “Autorisatie geweigerd”.

De currency van de limiet zal uw voornaamste account currency zijn. Wanneer u meerdere currency heeft en de transactie plaats vindt in een andere currency dan de standaard currency, dan zal ons systeem de limiet omzetten naar de andere currency.

3 3-D Secure

3-D Secure biedt u een hoog niveau van beveiliging aan, aangezien het u toelaat klanten ondubbelzinnig te identificeren door middel van technologieën – zoals een html paswoord, digipass, creditcardlezers, biometrie, etc. – die door de uitgevende bank worden toegepast. Door het aanbieden van 3-D Secure, haalt de merchant voordeel uit een voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) omschreven in het 3-D Secure contract met zijn acquirer. Onder deze voorwaarden wordt de rekening van de merchant niet meer gedebiteerd voor geschillen over "niet-identificatie van de kaarthouder" (dit is niet van toepassing op geschillen over andere kwesties! Voor meer info kan u contact opnemen met uw acquirer).

De volgende brands hebben het 3-D Secure protocol toegepast:

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

3.1 Algemeen

3.1.1 Aanvraag affiliatie

Wanneer 3-D Secure niet in uw account is geactiveerd, dan ziet u de “3DS verzoek” knop in de “3-D Secure” tabel. Wanneer u op de “3DS verzoek” knop klikt, dan wordt er naar uw acquirer een e-mail gestuurd. Indien uw contract met uw acquirer 3-D Secure niet voorziet, dan kunt u contact opnemen met uw acquirer voor verdere informatie met betrekking tot het inschrijven voor 3-D Secure, indien u wenst dat uw acquirer u de 3-D Secure betalingsoptie aanbiedt.

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

Wanneer 3-D Secure in uw account is geactiveerd, dan zult u de activeringsdatum in uw tabel zien. U kunt de configuratie van 3-D Secure wijzigen door te klikken op de ‘Edit’ knop naast de betaalmethoden.

3.1.2 Standaard 3-D Secure transactieverwerking

1. Wanneer we de creditcarddetails van uw klant ontvangen, zendt ons systeem een aanvraag naar de VISA/MasterCard/JCB/AmEx directory om vast te stellen of de kaart enrolled (geregistreerd) is, i.e. of de kaarthouder een vorm van identificatie heeft ontvangen, gekoppeld aan zijn/haar kaart, Indien van toepassing, krijgt ons systeem de authenticatie server gegevens van de kaartuitgever.

2. Wanneer de kaart enrolled is, dan wordt de koper naar de authenticatieserver van de uitgever geleid om de authenticatie te beginnen.

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

Als de authenticatie succesvol is, dan kan de merchant genieten van de voorwaardelijke betalingsgarantie die voorzien is door zijn acquirer.

Als de kaart niet enrolled is, dan krijgt de merchant een bepaald niveau van voorwaardelijke betalingsgarantie dat door de acquirer voorzien wordt.

In beide gevallen heeft de merchant, onder bepaalde condities (bepaald door VISA, MasterCard en financiële instellingen, en zoals omschreven in het 3-D Secure contract met zijn acquirer), een betalingsgarantie, zelfs zonder het ontvangen van de identificatie-informatie van de klant. Deze voorwaardelijke betalingsgarantie regels worden enkel tussen de merchant en zijn acquirer geregeld. Ogone handelt alleen als technisch tussenpersoon.

3.2 Configuratieopties

Het volgende hoofdstuk beschrijft de configuratieopties voor: Verified by Visa, MasterCard SecureCode, J-Secure en SafeKey. Afhankelijk van uw acquirer is het mogelijk dat sommige (of alle) opties niet ondersteund worden.

3.2.1 Technisch probleem

De merchant kan bij een technisch probleem, dat de verbinding naar de VISA/MasterCard/JCB/AmEx directory tijdens de 3-D Secure enrollment verificatie verhindert, kiezen tussen het *Voortzetten* of *Onderbreken* van de transactie.

Als een technisch probleem ervoor zorgt dat ons systeem geen connectie kan maken met de VISA/ MasterCard/JCB/AmEx directory (stap 1 in 2.1.2), dan raadt VISA/MasterCard/JCB/AmEx aan het proces zonder authenticatie verder te zetten (optie *Voortzetten*). In dit geval zal de merchant niet genieten van de voorwaardelijke betalingsgarantie (zie Sectie 2.1.2).

3.2.2 Identificatiedienst tijdelijk niet beschikbaar

De merchant kan kiezen tussen *Voortzetten* of *Onderbreken* van de transactie, wanneer de service voor de kaarthouderidentificatie tijdelijk onbeschikbaar is.

Wanneer de authenticatieserver van de kaartuitgever tijdelijk onbeschikbaar is (stap 2 in 2.1.2), dan is kaarthouderidentificatie onmogelijk. In dit geval raden VISA/MasterCard/JCB/AmEx aan het proces te verder te zetten (optie *Voortzetten).* De merchant zal dan niet genieten van de voorwaardelijke betalingsgarantie (zie Sectie 2.1.2).

3.2.3 Authenticatie faalt (enkel bij MasterCard)

De merchant kan kiezen tussen het *Voortzetten* of *Onderbreken* van de transactie, wanneer de authenticatie faalt.

Wanneer de kaarthouder authenticatie faalt (stap 3 in 2.1.2), dan raadt MasterCard aan het betalingsproces te onderbreken (optie *Onderbreken*). Wanneer de transactie wordt verder gezet zal de merchant dan niet genieten van de voorwaardelijke betalingsgarantie (zie Sectie 2.1.2).

3.2.4 Activering / deactivering 3-D Secure

Hier kan de merchant de 3-D Secure voor alle VISA/MasterCard/JCB/AmEx-kaarten aan/uitschakelen. Onthoud dat wanneer 3-D Secure is uitgeschakeld, de merchant niet geniet van de voorwaardelijke betalingsgarantie (zie Sectie 2.1.2).

3.2.5 Deactivering 3-D Secure specifieke BIN

De merchant kan bepaalde BIN-ranges instellen waarvoor hij 3-D Secure wil uitschakelen, indien de kaarthouder niet geregistreerd (enrolled) is.

Wanneer de kaarthouder niet geregistreerd is, zal de merchant niet genieten van de voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) voor betalingen die gemaakt worden met kaarten die beginnen met die 6 cijfers.

4 Zwarte lijst / witte lijst

In de Fraudedetectiemodule heeft u de mogelijkheid om een witte lijst (of whitelist), op basis van IP-adressen, en een zwarte lijst (of blacklist), op basis van BIN codes, creditcardnummers en IP-adressen, aan te maken.

“Nee” geeft aan dat niets geconfigureerd werd in de blacklist/whitelist. Wanneer een blacklist/whitelist al geconfigureerd is, zal de status “Ja” zijn.

Indien voor een nieuwe transactie in uw account de BIN, het creditcardnummer of het IP-adres dat is ingevoerd in uw blacklist staat, dan zullen wij deze transactie weerhouden en de status op “Autorisatie geweigerd” zetten.

4.1 Creditcards

U kunt tot 50 items per lijst toevoegen.

U kunt een commentaar toevoegen aan een blacklist of whitelist item door iets in te vullen in het “Commentaar” veld wanneer u een item aan de lijst toevoegt. U kunt ook een commentaar achteraf toevoegen of verwijderen door op de “...” link te klikken in de “Commentaar” kolom.

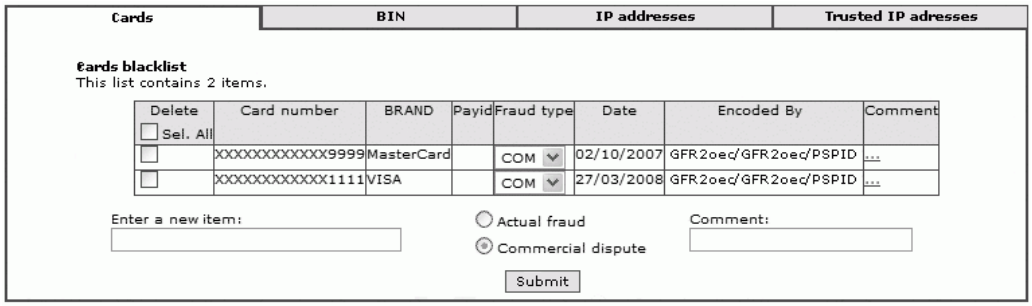
Voor elke blacklist toevoeging kan u de reden waarom u een item wilt blokkeren selecteren: daadwerkelijke (echte) fraude of commercieel geschil.

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

4.1.1 Kaart blacklist

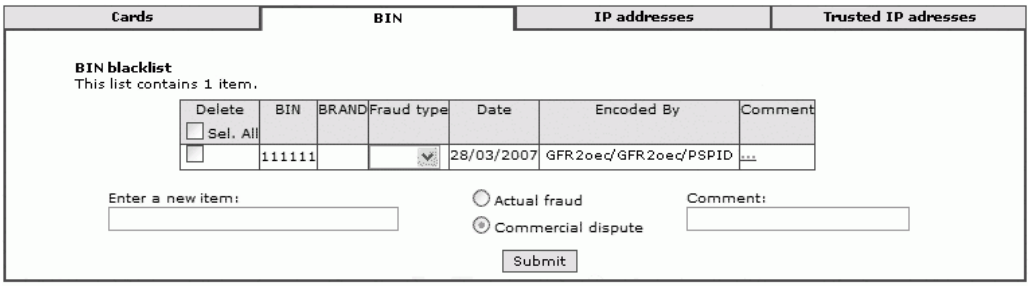
In uw creditcard blacklist moet u het volledige creditcardnummer invoeren. U kunt altijd creditcardnummers verwijderen die u hebt ingevoerd in uw lijst.

Indien u Direct Debits NL, Direct Debits DE of Direct Debits AT als betaalmethode in uw account hebt geactiveerd, kunt u naast creditcards ook rekeningnummers in deze blacklist invoeren.



4.1.2 BIN blacklist

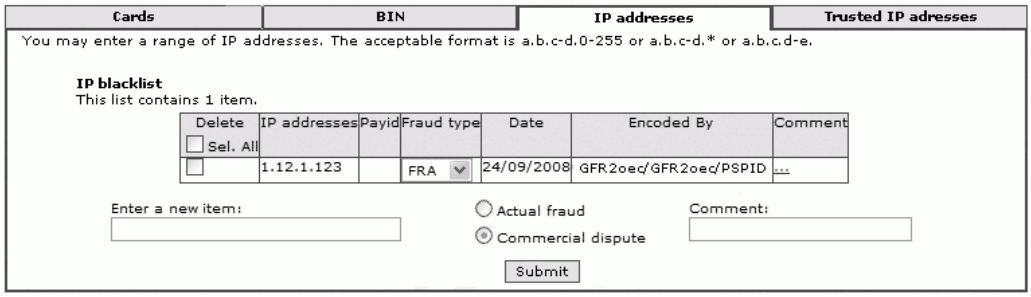
De BIN code zijn de eerste 6 cijfers van een creditcardnummer. Een BIN code is gekoppeld aan een specifieke bank in een specifiek land. Als gevolg daarvan kunt u alle creditcards die uitgegeven worden door bank x in land y in uw blacklist invoeren, door enkel de BIN-code in te voeren. U kunt altijd BIN-codes verwijderen die u heeft ingevoerd in uw lijst.



4.1.3 IP blacklist

In uw blacklist van IP-adressen kunt u niet alleen een specifiek IP-adres invoeren, maar ook een reeks (range) van IP-adressen, door gebruik te maken van de volgende formaten: a.b.c-d.0-255 of a.b.c-d.* of a.b.c.d-e. U kunt altijd ingevoerde IP-adressen uit uw lijst verwijderen.

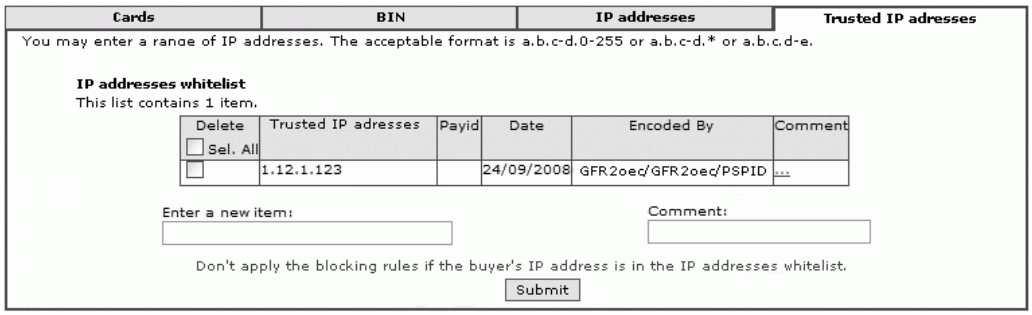
Om ons systeem in staat te stellen het IP adres van de klant te controleren, moeten merchants die werken met DirectLink (*) het IP-adres meesturen in het veld “REMOTE_ADDR”.



4.1.4 IP whitelist

Indien u door het blokkeren van bepaalde landen of IP-adressen in de blocking rules een bepaalde klant heeft geblokkeerd waarvan u wel graag bestellingen aanvaardt, dan kunt u het IP-adres van de klant opnemen in de te vertrouwen IP-adressenlijst (Vertrouwde IP-adressen). Op deze manier kunt u transacties toestaan van een IP-adres dat afkomstig is uit een land dat u geblokkeerd heeft. U kunt altijd IP-adressen verwijderen die u in de lijst heeft opgenomen.

Om ons systeem in staat te stellen het IP-adres van de klant te controleren, moeten merchants die werken met DirectLink het IP-adres meesturen in het veld “REMOTE_ADDR”.



5 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.

5.1 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.

6 Fraudedetectiemodule Feedback

6.1 Transactieoverzicht in de backoffice

6.1.1 Geavanceerde selectiecriteria

Wanneer u een transactie opzoekt via de “Beheer Transacties” of “Dagtotalen” (Financiële historiek) link in uw account-menu, zult u een extra optie hebben in de “Geavanceerde selectiecriteria”: IP-adres. U kunt het veld IP-adres gebruiken om alle transacties op te zoeken die van hetzelfde IP-adres afkomstig zijn, of van IP-adressen met dezelfde begincijfers.

6.1.2 3-D Secure in de transactielijst

Wanneer u uw transactielijst via “Beheer transacties” of “Dagtotalen” (Financiële historiek) in uw back-office weergeeft, zult u volle en halve groene bolletjes in uw lijst zien (indien u 3-D Secure in uw account heeft geactiveerd).

01/04/2006 19:45:21	9-Payment requested	002168	11/04/2006	159.15 EUR		Bill Smith
01/04/2006 19:50:02	9-Payment requested	095978	11/04/2006	44.95 EUR		Patricia Applegate
01/04/2006 19:50:46	9-Payment requested	218041	11/04/2006	39.75 EUR		Bill Smith

Het volledige bolletje , waar de duim omhoog staat, vertegenwoordigt een 3-D Secure transactie waar de klant door middel van een 3-D Secure geregistreerde creditcard betaald heeft. Voor deze transactie voorziet uw acquirer u van een voorwaardelijke betalingsgarantie (zie Sectie 2.1.2).

Het halve bolletje geeft een 3-D Secure transactie weer waar betaald is met een creditcard die niet 3-D Secure enrolled is. Voor deze transacties is er een bepaald niveau van voorwaardelijke betalingsgarantie (zie Sectie 2.1.2), gebaseerd op de specifieke details van het 3-D Secure contract dat u met uw acquirer heeft.

Transacties zonder een (half) bolletje zijn transacties die verwerkt zijn zonder gebruik te maken van 3-D Secure. De voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) is niet van toepassing op deze transacties.

Transacties met het waarschuwingsteken geven transacties weer waar de authenticatie niet geslaagd is. De voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) is niet van toepassing op de transacties waarbij u gekozen heeft om verder te gaan (*Voortzetten*), maar waarvan de authenticatie heeft gefaald (voor MasterCard, zie Sectie 2.2.3).

6.1.3 Transactiedetails

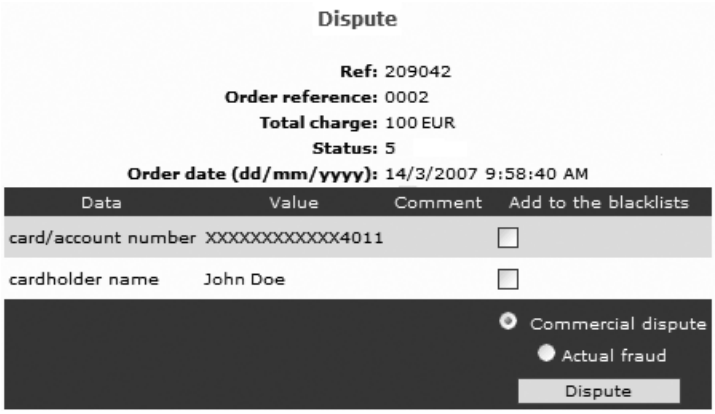
In de transactiedetails (financiële pagina), kunt u bijkomende informatie zoals het resultaat van kaart verificatiecode (als de CVC code is ingevoerd door de klant), land van de kaart, land van het IP-adres en IP-adres terug vinden.

De "Geschil" toets boven de tabel met bijkomende informatie, leidt u naar een pagina waar u in één klik bepaalde transactiedetails kunt toevoegen aan uw blacklist. Deze optie staat u bijvoorbeeld toe om het kaartnummer dat gebruikt is voor de transactie toe te voegen aan de kaart blacklist zonder het volledige kaartnummer te kennen.

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

Belangrijk

Selecteer enkel "echte fraude" wanneer de klant ook daadwerkelijk fraude heeft gepleegd met deze kaart, d.w.z wanneer een kaarthouder een kaart gebruikt die hem niet toebehoort.



6.1.4 Foutcodes

Wanneer een transactie wordt tegengehouden door ons systeem, op basis van de door u ingestelde regels in de Fraudedetectie, dan kunt u de reden achterhalen in de foutmelding voor de transactie. Met inbegrip van een paar uitzonderingen beginnen alle foutcodes die gerelateerd zijn aan de Fraudedetectie met "300011", gevolgd door twee cijfers.

Meer informatie over statussen en foutcodes vindt u in uw KBC/CBC-Paypage account. Log in en ga naar: Ondersteuning > Integratie- en gebruikershandleidingen > Gebruikershandleidingen > Lijst van betalingsstatussen en foutcodes.

De volgende lijst bevat voorbeelden van de meest voorkomende foutmeldingen:

3 / 30001100 Land van de koper niet toegelaten

3 / 30001120 IP adres in de blacklist van de handelaar

3 / 30001130 BIN in de blacklist van de handelaar

3 / 30001140 Kaartnummer in de blacklist van de handelaar

6.2 Aanvullende transactieparameters

In uw post sale requests, redirecties met feedback, file downloads en DirectLink XML antwoorden, zullen aanvullende transactieparameters, die betrekking hebben op de Fraude Detectie Module, worden teruggegeven.

De lijst met aanvullende transactieparameters wordt hieronder weergegeven. Deze velden zullen leeg zijn in geval van een formaatvalidatiefout voor de transactiedetails.

Parameter	Waarde
IPCTY	Land van herkomst van het IP-adres Formaat: 2 tekens alfabetische ISO-code. Als deze parameter onbeschikbaar is, dan wordt “99” als antwoord weergegeven. De IP-controle is gebaseerd op extern aangeleverde IP-lijsten. Er is dus een klein risico, aangezien wij vertrouwen op de juistheid van deze lijsten. De controle geeft in 94% van alle gevallen positieve resultaten .
CCCTY	Land van herkomst van de creditcard. Dit is alleen beschikbaar voor VISA, MasterCard, American Express en Diners Club. Deze waarde zal leeg zijn voor alle andere brands/betaalmethoden. Formaat: 2 tekens alfabetische ISO-code. Als deze parameter onbeschikbaar is, dan wordt “99” als antwoord weergegeven. De IP-controle is gebaseerd op extern aangeleverde IP-lijsten. Er is dus een klein risico, aangezien wij vertrouwen op de juistheid van deze lijsten. De controle geeft in 94% van alle gevallen positieve resultaten .
ECI	Electronic Commerce Indicator. Mogelijke ECI-waarden en hun betekenis worden hieronder weergeven: 1 MOTO (kaart niet aanwezig) 2 Periodieke betalingen, afkomstig van MOTO 3 Afbetaling in termijnen 5 Kaarthouderidentificatie succesvol 6 Merchant ondersteunt identificatie, maar niet de kaarthouder, voorwaardelijke betalingsgarantie regels zijn van toepassing (zie Sectie 2.1.2) 7 E-commerce met SSL-beveiliging 9 Periodieke betalingen komende van e-commerce 12 Merchant ondersteunt identificatie, maar de kaarthouder niet, voorwaardelijke betalingsgarantie regels zijn van toepassing (zie Sectie 2.1.2) 91 Identificatie kaarthouder GEFAALD!!!! (voorwaardelijke betalingsgarantie (zie Sectie 2.1.2) misschien van toepassing, overleg met uw acquirer) 92 Autenticatiesite van de uitgevende bank tijdelijk onbeschikbaar, maar de transactie ging verder

Parameter	Waarde
CVCCheck	Resultaat van de kaart verificatie code check. Mogelijke waarden: KO: De CVC is verzonden, maar de acquirer heeft negatief geantwoord op de CVC-controle, d.w.z. de CVC is onjuist. OK: 1. De CVC is verzonden en de acquirer heeft positief geantwoord op de CVC-controle, d.w.z. de CVC is juist, OF 2. De acquirer heeft een autorisatiecode verzonden, maar heeft geen duidelijk resultaat voor de CVC-controle. NO: Alle andere gevallen. Bijvoorbeeld, geen CVC verzonden, de acquirer heeft geantwoord dat een CVC-controle niet mogelijk was, de acquirer heeft de autorisatie afgewezen maar heeft geen specifiek resultaat voor de CVC-controle geleverd, ...
AAVCheck	Resultaat van de automatische adresverificatie. Deze verificatie is op dit moment alleen verkrijgbaar voor American Express. Mogelijke waardes: KO: Het adres is verzonden maar de acquirer heeft negatief geantwoord op de adres controle, d.w.z. het adres is onjuist. OK: 1. Het adres is verzonden en de acquirer heeft positief geantwoord op de adres-controle, d.w.z. het adres is correct OF 2. De acquirer heeft een autorisatiecode verzonden, maar heeft geen bepaald resultaat voor de adres-controle. NO: Alle andere gevallen. Bijvoorbeeld, geen adres verzonden, de acquirer heeft geantwoord dat een adres-controle niet mogelijk was. De acquirer heeft de autorisatie afgewezen maar heeft geen specifiek resultaat voor de adres-controle geleverd.
VC	Virtuele kaart. Mogelijke waardes: ECB: voor E Carte Bleue ICN: voor Internet City Number NO: voor alle andere gevallen. Bijvoorbeeld, de kaart is niet virtueel, de virtuele kaart is ons onbekend...
IP	IP-adres van de klant, zoals door ons systeem gedetecteerd in een 3-tier integratie, of aan ons verzonden door een merchant in een 2-tier integratie.

7 Appendix 1: CVC2 en AAV

7.1 CVC2

CVC2 is een authenticatieprocedure, ingesteld door de creditcardbedrijven, om een bijdrage te leveren aan het voorkomen van frauduleus gebruik van creditcards bij internettransacties. Afhankelijk van de het merk (de "brand") heeft deze code een andere naam (CVC2 of Card Validation Code voor MasterCard, CVV2 of Card Verification Value voor VISA, CID of Card Identification Number voor American Express). De code wordt normaal benoemd als “CVC”. De functionaliteit van de CVC2 is hetzelfde voor alle brands.

De verificatiecode is op een unieke wijze aan het kaartnummer verbonden, maar is geen onderdeel van het kaartnummer zelf. Afhankelijk van de brand is de verificatiecode een 3- of 4-cijferige code aan de voorzijde of achterzijde van de kaart, een uitgavenummer (issue number), een startdatum, of een geboortedatum. Voor MasterCard en VISA bijvoorbeeld is een 3-cijferige code op de achterzijde van de kaart in de handtekeninglijn aanwezig, achter het volledige klantrekeningnummer of de laatste 4 cijfers van het klantrekeningnummer.

Het is strict verboden aan merchants en PSP's om de CVC2-codes van klanten in hun database te bewaren. Wanneer een kaarthouder niet in persoon aanwezig is, d.w.z voor "kaart niet aanwezig" (card not present-) transacties, en hij gevraagd wordt de CVC2-code in te voeren samen met zijn kaartnummer, dan helpt deze verificatiecode om er zeker van te zijn dat diegene die de order plaatst de kaart ter hand heeft en dat de kaart echt bestaat.

7.2 AAV

AAV is een authenticatieprocedure, beschikbaar in sommige markten, om bij te dragen tot het voorkomen van frauduleus gebruik van creditcards bij internettransacties. Afhankelijk van het merk (de "brand") heeft deze authenticatieprocedure een andere naam: AVS of Address Verification Service/System voor VISA/ MasterCard; AAV of Automated Address Verification voor American Express. De functionaliteit van de AAV is hetzelfde voor alle brands.

De adrescontrole vindt plaats wanneer de acquirer de kaartuitgever verzoekt om de numerieke bestanddelen te vergelijken (huisnummer en postcode) van het facturatie- of verzendadres van de klant dat de merchant ons heeft toegestuurd, met de gegevens die de klant aan de kaartuitgever heeft doorgegeven bij de registratie.

American Express voert deze controle automatisch uit bij het ontvangen van adresdetails in een transactie. Voor andere brands hangt het van de acquirer af of zij de controle uitvoeren. Onder alle omstandigheden raden wij aan ons de adresdetails samen met de besteldetails voor de transactie toe te sturen.

Hoewel een transactie op basis van het resultaat van de adrescontrole niet geweigerd wordt, kan een merchant besluiten deze informatie te gebruiken bij het beslissen of hij zijn handelswaar wel dan niet verzendt of, om de klant om meer informatie te verzoeken voor hij overgaat tot verzending.

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