# Betrugserkennungsmodul

Konfigurationshandbuch – Betrugserkennungsmodul v.4.2.3



ingenico ePayments

# Table of Contents

# 1 Das Betrugserkennungsmodul

Im Fernabsatzgeschäft erfordert das Thema Betrugsbekämpfung ein hohes Maß an Know-how, Schnelligkeit und Flexibilität. Ogone möchte seine Kunden bei der Implementierung effektiver Risikomanagementtools unterstützen. Das Ogone Betrugserkennungsmodul bietet einen Echtzeit-Service, der alle notwendigen Analyseinformationen zur Verfügung stellt. Darüber hinaus umfasst das Modul auf den Kunden zugeschnittene Sicherheitsvorkehrungen für die Bearbeitung verdächtiger Transaktionen.

Betrug lässt sich durch den Einsatz eines solchen Instruments nicht völlig eliminieren, es ist jedoch eine effiziente Maßnahme, um Betrugsszenarien entgegenzuwirken. Die Konfiguration des Moduls erfolgt auf der Basis des Risikopotenzials sowie auf den Erfahrungswerten Ihres Unternehmens aus der Vergangenheit.

## 1.1 Leistungen

Das Betrugserkennungsmodul ermöglicht:

- die Erkennung von Unregelmäßigkeiten während der Transaktionsverarbeitung
- die sofortige Sperrung im Falle von Betrugsversuchen
- den Schutz vor länderspezifischen Risiken
- die Festlegung und Anwendung kundenspezifischer Sicherheitsrichtlinien
- eine Zahlungsgarantie für Händler (s. Abschnitt 2.1.2) - in Übereinstimmung mit ihrem individuellen Acquirer Vertrag (3-D Secure).

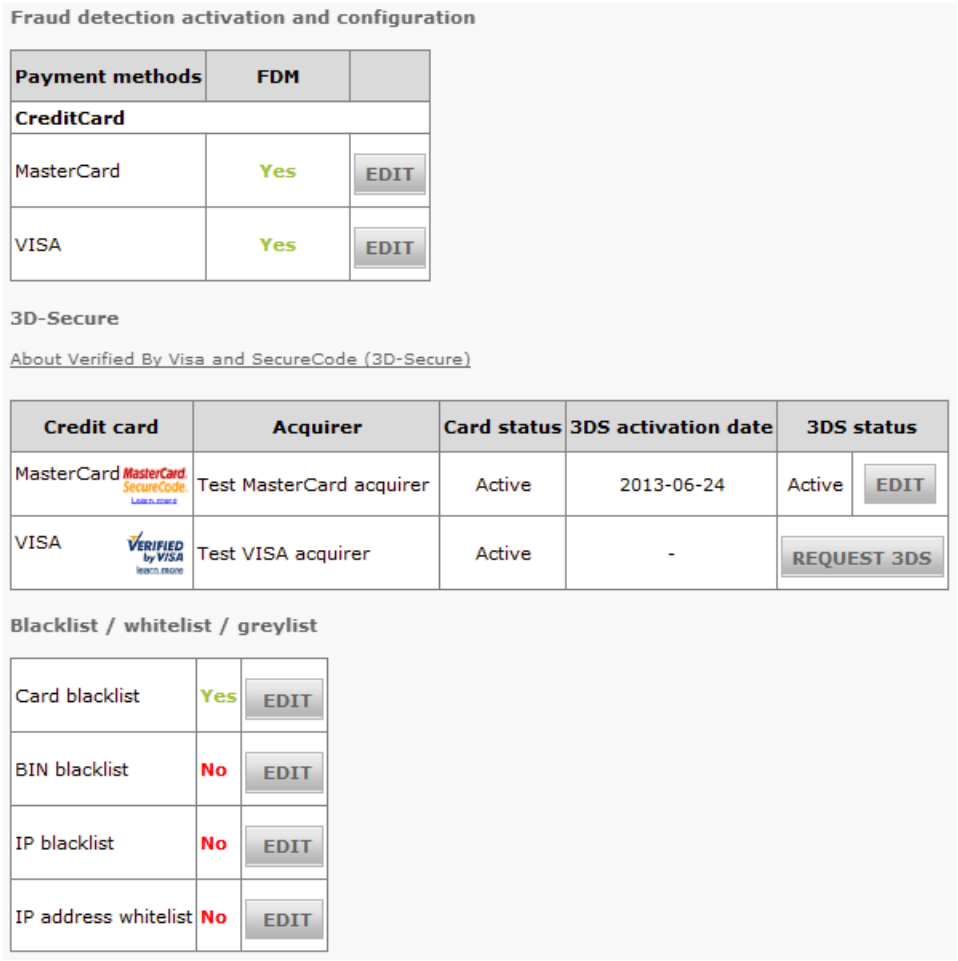
## 1.2 Zugang

Zugang zum Betrugserkennungsmodul erhalten Sie in Ihrem Benutzerkonto über den Link „Betrugserkennung“.

## 1.3 Aufbau

Das Betrugserkennungsmodul besteht aus drei Funktionsbereichen:

- Aktivierung und Konfiguration der Mißbrauchserkennung
- 3-D Secure
- Schwarze Liste / Weiße Liste




Der folgende Abschnitt beschreibt die Konfiguration von 3-D Secure sowie die Kriterien für Visa und MasterCard Kreditkarten.

**Wichtig**

Die in diesem Dokument beschriebenen VISA/MasterCard Kriterien stehen nicht unbedingt für alle Zahlungsmethoden zur Verfügung. Die Verfügbarkeit der „Aktivierung und Konfiguration“ ist abhängig von der jeweiligen Zahlungsmethode. Bei einigen Zahlungsmethoden kann nur die Option „Limite” konfiguriert werden. Wir empfehlen Ihnen, die Auswahlkriterien für Ihre individuellen Zahlungsmethoden zu prüfen. Gehen Sie dazu auf die Schaltfläche „Bearbeiten“. Diese befindet sich in Ihrem Betrugserkennungsmodul in der Tabelle “Aktivierung und Konfiguration der Mißbrauchserkennung” neben der Zahlungsmethode.

# 2 Aktivierung und Konfiguration der Mißbrauchserkennung

Die Tabelle „Aktivierung und Konfiguration" verdeutlicht den Unterschied zwischen Kreditkarten und anderen Zahlungsmethoden.

Es gibt Blockaderegeln (Sperrrichtlinien) und Limite als Optionen. „Nein" zeigt an, dass unter der entsprechenden Option keine Konfiguration vorgenommen wurde. Liegt eine Konfiguration vor, zeigt der Status „Ja" an.

Im Folgenden wird die Konfiguration von Betrugserkennungsoptionen im Zusammenhang mit Kreditkarten näher betrachtet.

## 2.1 Kreditkarten

Zur Konfiguration der Betrugserkennungsoptionen für eine bestimmte Kreditkarte klicken Sie auf die Schaltfläche „Ändern", die sich neben der Zahlungsmethode befindet. Sie gelangen dann auf die Konfigurationsseite, wo Registerkarten für Blockaderegeln (Sperrrichtlinien) und Limite angezeigt werden.

WICHTIG

Wählen Sie nur dann „tatsächlicher Betrug", wenn Sie eine Rückbelastung mit einem Ursachencode für Betrug erhalten haben.

### 2.1.1 Blockaderegeln (Sperrrichtlinien)

Nachdem der Kunde seine Kreditkartendetails eingegeben hat und auf den Button „Verarbeiten" geklickt hat, können Sie Sperrrichtlinien anwenden.

Entspricht die Transaktion nicht den von Ihnen gesetzten Vorgaben, halten wir diese zurück und setzen den Transaktionsstatus auf „Genehmigung verweigert".

#### 2.1.1.1 IP-adress-Länder

Standardmäßig werden alle IP-Adress-Länder akzeptiert. Unser System kann das IP-Adress-Land anhand der IP-Adresse des Kunden erkennen (obwohl diese Überprüfung in 94 % der Fälle positive Ergebnisse bringt, basiert dieser IP-Check auf externen IP-Listen. Dies ist mit einem gewissen Risiko verbunden, da wir uns auf die Korrektheit dieser externen Liste verlassen müssen).

Wenn Sie eine Liste mit IP-Adress-Ländern festlegen möchten, können Sie die gewünschten Länder auf der rechten Seite des Bildschirms auswählen und durch Klicken des Buttons „Hinzufügen" in Ihre Liste aufnehmen.

WICHTIG

Die Codes A1 (Anonymous Proxy), AP (Asian Pacific Region), EU (European Network) und A2 (Satellite Providers) beziehen sich auf IP-Adressen bei denen das Ursprungsland unsicher ist.

EU bedeutet beispielsweise, dass das genaue IP-Land unsicher ist, jedoch zu Europa gehört. Wenn Sie EU als IP-Adress-Land akzeptieren, heißt dies nicht, dass Sie Zahlungen aus allen europäischen Ländern akzeptieren. Es bedeutet lediglich, dass Sie Zahlungen von IP-Adressen akzeptieren, die von europäischen Institutionen verwaltet werden. Wenn Sie Zahlungen aus asiatischen oder europäischen Ländern akzeptieren möchten, müssen Sie diese Länder Land für Land Ihrer Liste hinzufügen.

Anonyme Proxies sind Internet-Provider, die es Internet-Nutzern ermöglichen, Ihre IP-Adresse zu verbergen. Wir empfehlen Ihnen, keine Zahlungen zu akzeptieren, die von anonymen Proxies stammen!

Oberhalb der Liste der ausgewählten IP-Adress-Länder können Sie angeben, ob Ihre Auswahlliste zu den akzeptierten Ländern gehört (*Nur Zahlung aus gelisteten Ländern akzeptieren*) oder zu den abgelehnten Ländern (*Zahlung aus gelisteten Ländern ablehnen*).

Sie können jederzeit ein Land aus der Auswahlliste entfernen, indem Sie das Kästchen „Del“ anklicken, das sich vor dem Land befindet und dann auf die Schaltfläche „Abschicken“ unterhalb der Liste gehen.

#### 2.1.1.2 Länderübereinstimmung (Nur Visa, MasterCard, American Express und Diners Club)

Wenn Sie diesen Parameter auf „Ja” setzen, akzeptieren Sie ausschließlich Transaktionen, bei denen die Kunden-IP-Adresse identisch ist mit dem Land seiner kartenausgebenden Bank, d.h. nur wenn Kartenland und Land der IP-Adresse übereinstimmen. Diese Prüfung wird nicht durchgeführt, wenn die IP-Adresse von einem anonymen Proxy, dem Asia Pacific Network, dem European Network oder einem Satellite Provider stammt.

#### 2.1.1.3 3-D Secure (Nur Visa/MasterCard/JCB/AmEx)

Mit Hilfe dieses Parameters können Sie die oben festgelegten Sperrrichtlinien umgehen, für den Fall, dass sich der Karteninhaber im Rahmen von 3-D Secure ausweist.

Wenn es sich um eine 3-D Secure Kreditkarte handelt und Sie einen 3-D Secure Vertrag mit Ihrem Acquirer geschlossen haben, profitieren Sie für diese Transaktion von einer Zahlungsgarantie (s. Abschnitt 2.1.2). Selbst wenn Sie – aufgrund eines hohen Betrugsrisikos – keine Zahlungen aus dem Land X erhalten möchten, können Sie dennoch Transaktionen mit 3-D Secure Kreditkarten aus diesem Land zulassen. Sie tragen kein Risiko im Falle von strittigen Transaktionen als Folge einer Nicht-Identifizierung des Karteninhabers (diese Regelung ist jedoch nicht gültig bei Streitfällen im Zusammenhang mit anderen Inhalten, s. Kapitel 2).

### 2.1.2 Limite

Im Rahmen des Betrugserkennungsmoduls können Sie den Betrag pro Transaktion beschränken.

Sie können einen Mindest- und einen Höchstbetrag festlegen. Entspricht der Transaktionsbetrag nicht den von Ihnen festgelegten Werten, halten wir die Transaktion zurück und setzen den Status auf „Genehmigung verweigert“.

Die Währung, die den Limiten zu Grunde liegt, ist die Hauptwährung Ihres Kontos. Wenn Sie mehrere Währungen haben und eine Transaktion vorliegt, die eine andere Währung als unsere Standardwährung aufweist, dann konvertiert unser System das Limit in die andere Währung.

# 3 3-D Secure

3-D Secure bietet ein hohes Maß an Sicherheit, da sich mit Hilfe von Technologien (HTML-Passwörter, Digipass, Kartenleser, biometrische Daten etc.), die von den kartenausgebenden Banken implementiert werden, die Kundenidentität eindeutig ermitteln lässt.

Händler, die 3-D Secure anbieten, profitieren von einer Zahlungsgarantie (s. Abschnitt 2.1.2). Die Bedingungen, die dafür zu Grunde liegen, regelt der 3-D Secure Vertrag mit dem Acquirer. Bei Einhaltung dieser Bedingungen entfällt für den Händler das Rückbelastungsrisiko im Zusammenhang mit Streitfällen über die „Nicht-Identifikation des Karteninhabers". (Diese Regelung ist nicht gültig bei Streitigkeiten, denen ein anderer Inhalt zu Grunde liegt!).

Folgende Unternehmen haben das 3-D Secure Protokoll implementiert:

- Visa unter der Bezeichnung Verified by Visa
- MasterCard unter der Bezeichnung SecureCode
- JCB unter der Bezeichnung J-Secure
- American Express unter der Bezeichnung SafeKey

## 3.1 Allgemeines

### 3.1.1 Beantragung

Sollte 3-D Secure für Ihr Konto nicht aktiviert sein, finden Sie in der „3-D Secure" Tabelle die Schaltfläche „Anfrage 3D-S".

Wenn Sie auf die Schaltfläche „Anfrage 3D-S" klicken, wird eine E-Mail an Ihren Acquirer gesendet. Sollte Ihr Acquirer Vertrag die Option 3-D Secure nicht beinhalten, kontaktieren Sie - bei Interesse - Ihren Acquirer und bitten Sie ihn um Informationen über eine 3-D Secure Registrierung.

Anmerkung: Um sich für SafeKey anzumelden, kontaktieren Sie bitte American Express oder gehen Sie zum SafeKey-Portal.

Sobald 3-D Secure für Ihr Konto aktiviert wurde, sehen Sie das Aktivierungsdatum in der Tabelle. Wenn Sie die Konfiguration für 3-D Secure ändern möchten, klicken Sie neben der Zahlungsmethode auf die Schaltfläche „Ändern".

### 3.1.2 Standard 3-D Secure Transaktionsverarbeitung

1. Wenn wir die Kreditkartendetails von Ihrem Kunden erhalten, sendet unser System eine Anfrage an das VISA-/MasterCard-/JCB-/AmEx-Directory. Die Anfrage dient dazu, festzustellen, ob die Karte registriert ist, d.h. der Karteninhaber ein Identifikationsmittel (Passwort) in Verbindung mit seiner Karte erhalten hat und, sofern zutreffend, um die Daten vom Authentifizierungsserver des kartenausgebenden Instituts zu erhalten.

2. Ist die Karte registriert, wird der Käufer – zwecks Authentifizierung - von unserem System zum Authentifizierungsserver des kartenausgebenden Instituts geleitet.

3. Unser System erhält das Authentifizierungsergebnis und verarbeitet die Zahlung auf die übliche Art und Weise.

War die Authentifizierung erfolgreich, kann der Händler von einer Zahlungsgarantie profitieren, die von seinem Acquirer zur Verfügung gestellt wird.

War die Karte nicht registriert, erhält der Händler eine „eingeschränkte" Zahlungsgarantie von seinem Acquirer.

In beiden Fällen hat der Händler unter bestimmten Bedingungen (festgelegt von VISA, MasterCard und Finanzinstituten und wie in dem 3-D Secure Vertrag mit dem Acquirer beschrieben) eine Zahlungsgarantie – auch ohne den Erhalt von Ausweisinformationen des Kunden. Die Regeln, die einer solchen Zahlungsgarantie zu Grunde liegen, werden ausschließlich zwischen dem Händler und seinem

Acquirer verhandelt. Ogone hat nur die Funktion eines technischen Vermittlers.

## 3.2 Konfigurationsoptionen

Im Folgenden werden die Konfigurationsoptionen für Verified by Visa, MasterCard SecureCode, J-Secure und SafeKey beschrieben. Abhängig von Ihrem Acquirer werden einige (oder alle) dieser Optionen unterstützt.

### 3.2.1 Technische Probleme

Bei einem technischen Problem, das – während der Überprüfung der 3-D Secure Registrierung - eine Verbindung zum VISA-/MasterCard-/JCB-/AmEx-Directory verhindert, entscheidet der Händler, ob er die Transaktionsabwicklung fortsetzt (*Weiter*) oder abbricht *(Unterbrechung)*.

Sollte ein technisches Problem unser System an einer Verbindung zum VISA-/MasterCard-/JCB-/AmEx-Directory (Schritt 1 in Abschnitt 2.1.2) hindern, empfiehlt VISA/MasterCard/JCB/AmEx, die Transaktion ohne Authentifizierung (Option *Weiter*) abzuwickeln. In diesem Fall profitiert der Händler jedoch nicht von einer Zahlungsgarantie (s. Abschnitt 2.1.2).

### 3.2.2 Identifizierungsservice vorübergehend nicht verfügbar

Der Händler entscheidet, ob er eine Transaktion fortsetzt (*Weiter*) oder abbricht *(Unterbrechung)*, wenn der Karteninhaber-Identifizierungsservice vorrübergehend nicht zur Verfügung steht.

Wenn der Authentifizierungsserver des kartenausgebenden Instituts vorrübergehend nicht verfügbar ist (Schritt 2 in Abschnitt 2.1.2), kann die Identität des Karteninhabers nicht geprüft werden. Für diesen Fall empfiehlt VISA/MasterCard/JCB/AmEx die Fortsetzung (Option *Weiter*) der Transaktionsabwicklung. Der Händler würde dann jedoch nicht von einer Zahlungsgarantie (s. Abschnitt 2.1.2) profitieren.

### 3.2.3 Authentifizierung fehlgeschlagen (Nur MasterCard)

Wenn eine Authentifizierung fehlgeschlagen ist, kann der Händler entscheiden, ob er die Transaktionsabwicklung fortsetzt (*Weiter*) oder abbricht *(Unterbrechung)*.

Sollte eine Karteninhaber-Authentifizierung fehlgeschlagen sein (Schritt 3 in Abschnitt 2.1.2), empfiehlt MasterCard den Abbruch (Option *Unterbrechung*) des Zahlungsprozesses. Wird die Abwicklung der Transaktion dennoch fortgesetzt, profitiert der Händler nicht von der Zahlungsgarantie (s. Abschnitt 2.1.2).

### 3.2.4 3-D Secure aktivieren/deaktivieren

Hier kann der Händler 3-D Secure für alle VISA-/MasterCard-/JCB-/AmEx-Karten aktivieren/deaktivieren. Hinweis: Wenn 3-D Secure deaktiviert ist, profitiert der Händler nicht von der Zahlungsgarantie (s. Abschnitt 2.1.2).

### 3.2.5 Deaktivierung von 3-D Secure für bestimmte BINs

Der Händler kann bestimmte BIN-Nummernkreise eingeben, für die er 3-D Secure deaktivieren möchte, wenn der Karteninhaber nicht registriert ist.

Wenn die Karte nicht registriert ist, profitiert der Händler - für Transaktionen, die mit einer Karte getätigt wurden, deren Kartennummer mit diesen sechs Ziffern beginnt - nicht von der Zahlungsgarantie (s. Abschnitt 2.1.2).

# 4 Schwarze Liste / Weiße Liste

Mit Hilfe des Betrugserkennungsmoduls können Sie eigene Kreditkarten-Blacklists erstellen. Die Blacklists basieren auf BIN-Codes, Kreditkartennummern und IP-Adressen, für die Sie keine Transaktionen akzeptieren möchten. Den Whitelists liegen IP-Adressen zu Grunde.

„Nein" zeigt an, dass keine Konfiguration für eine Blacklist/Whitelist vorliegt. Wurde eine Konfiguration vorgenommen, zeigt der Status „Ja" an.

Falls bei einer neuen Transaktion in Ihrem Konto, die BIN, Kreditkartennummer oder IP-Adresse in Ihrer Blacklist eingetragen ist, halten wir die Transaktion zurück und setzen den Status auf „Genehmigung verweigert".

## 4.1 Kreditkarten

Maximal sind 50 Einträge pro List möglich.

Sie können einen Kommentar zu einem Eintrag in eine Blacklist oder Whitelist hinzufügen. Sie können dies tun, während Sie einen Eintrag in die Liste vornehmen; der Kommentar kommt in das Feld "Kommentar". Sie können einen Kommentar hinzufügen oder löschen, indem Sie in der Spalte "Kommentar" auf "..." klicken.

Sie können für jeden Blacklist Eintrag einen Grund auswählen, warum Sie die Datei sperren möchten: Tatsächlicher Betrug (Actual fraud) oder kommerzieller Streitfall (Commercial dispute).

WICHTIG

Wählen Sie nur „Tatsächlichen Betrug" (Actual fraud) als Grund aus, wenn der Kunde in der Tat betrügerische Umsätze getätigt hat. Zum Beispiel wenn der Kunde eine Karte einsetzt, die ihm nicht gehört.

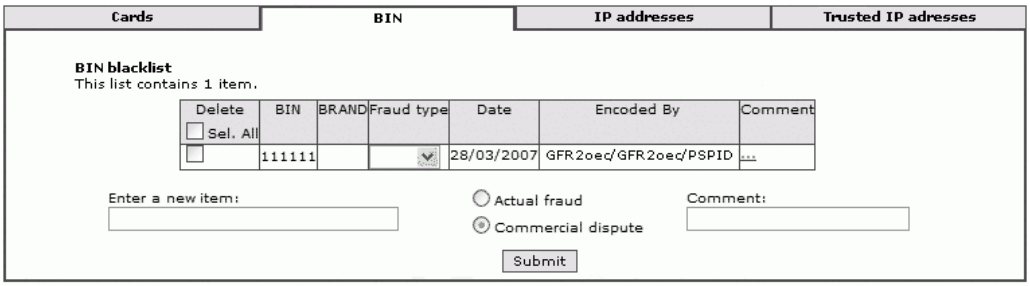
### 4.1.1 Karten-blacklist

Sie müssen die vollständige Kreditkartennummer in Ihre Kreditkarten-Blacklist eintragen. Kreditkartennummern, die Sie auf Ihrer Liste hinterlegt haben, können Sie jederzeit löschen.

Wenn Sie die Zahlungsmethoden Direct Debits NL, ELV (Direct Debits DE) oder Direct Debits AT in Ihrem Ogone-Konto aktiviert haben, fungiert die „Karten Blacklist" gleichzeitig als „Konten Blacklist" zum Eintrag von Kontonummern.


### 4.1.2 BIN-blacklist

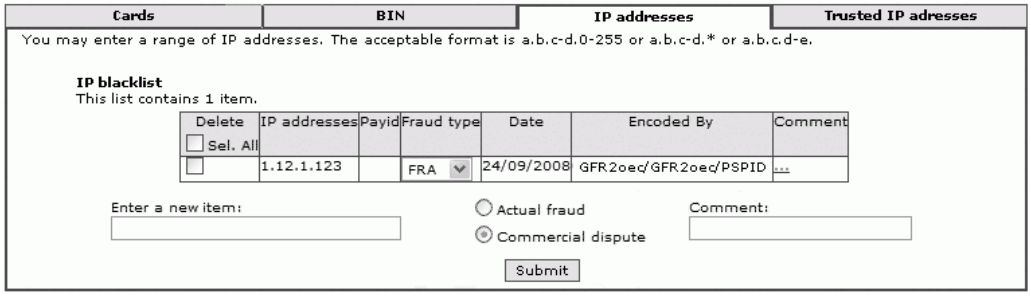
Bei einer BIN handelt es sich um die ersten sechs Stellen einer Kreditkartennummer. Eine BIN bezieht sich auf ein bestimmtes kartenausgebendes Institut in einem bestimmten Land. Folglich können Sie alle Kreditkarten, die von der Bank X in dem Land Y emittiert werden, auf Ihrer Blacklist eintragen. Hinterlegen Sie einfach den BIN-Code auf der Liste. Die auf Ihrer Liste eingetragenen BINs können jederzeit wieder gelöscht werden:




## 4.1.3 IP-blacklist

Auf Ihrer IP-Adress-Blacklist können Sie nicht nur eine bestimmte IP-Adresse eintragen, sondern eine Auswahl von IP-Adressen – unter Verwendung der folgenden Formate: a.b.c-d.0-255 oder a.b.c-d.* oder a.b.c.d-e. IP-Adressen, die Sie auf Ihrer Liste eingetragen haben, können Sie jederzeit wieder löschen.

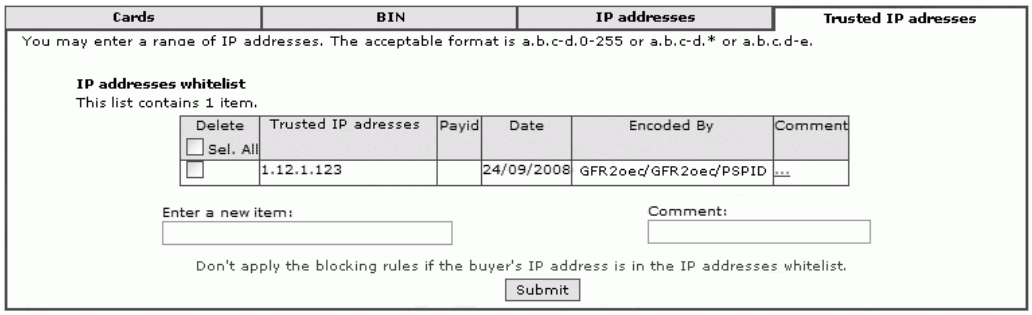
Damit unser System die IP-Adresse des Kunden prüfen kann, müssen Händler, die über DirectLink arbeiten, die IP-Adresse in dem Feld „REMOTE_ADDR" mitsenden.




## 4.1.4 IP-whitelist

Falls Sie durch das Blockieren von Ländern oder IP-Adress-Ländern einen bestimmten Kunden gesperrt haben, von dem Sie jedoch Aufträge entgegennehmen möchten, können Sie seine IP-Adresse in die Liste der vertrauenswürdigen IP-Adressen eintragen. Auf diese Art und Weise können Sie Transaktionen von IP-Adressen akzeptieren, selbst wenn diese aus einem Land stammen, das Sie gesperrt haben. IP-Adressen, die Sie auf Ihrer Liste eingetragen haben, können Sie jederzeit wieder löschen.

Damit unser System die IP-Adresse des Kunden prüfen kann, müssen Händler, die über DirectLink arbeiten, die IP-Adresse in dem Feld „REMOTE_ADDR" mitsenden.



# 5 Dispute

Das Akzeptieren von Transaktionen in einer Umgebung ist mit inhärenten Risiken, wie beispielsweise dem Risiko von Rückbelastungen, verbunden. Insbesondere bei der Durchführung von Transaktionen in einer „Card-Not-Present“ (CNP) Umgebung (Karte nicht vorhanden) ist das Risiko von Rückbelastungen stets präsent.

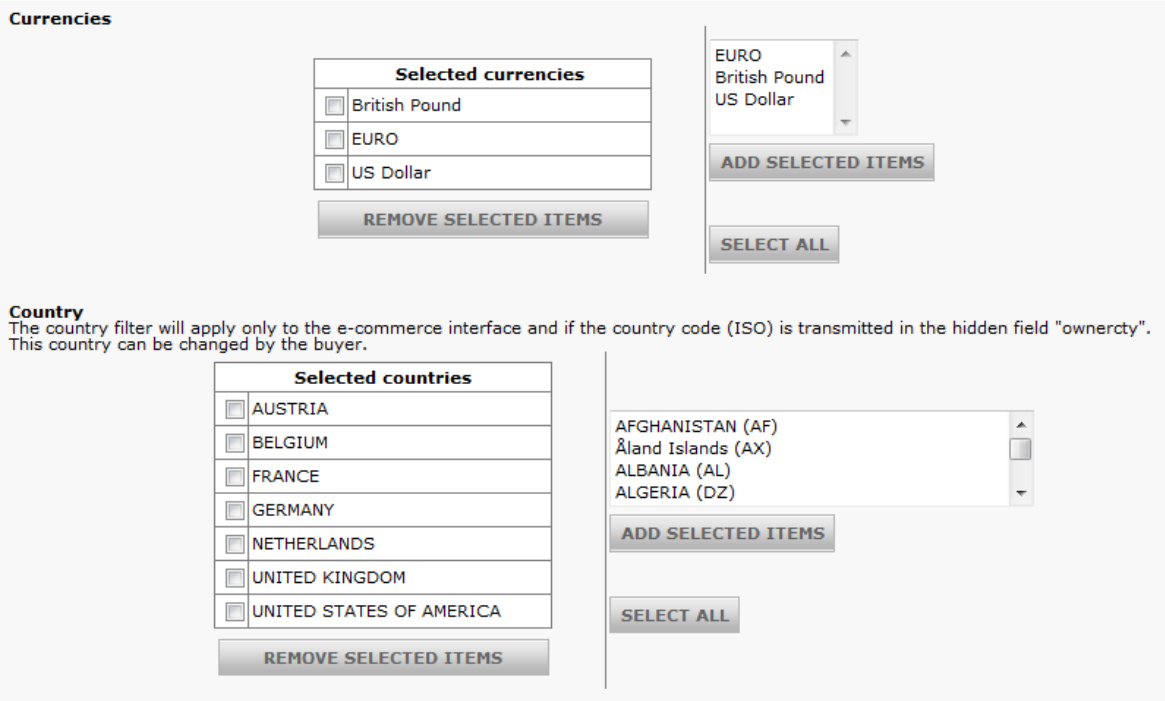
Ogone stellt Kunden eine „Dispute”-Seite bereit, auf der Händler Transaktionsdaten in eine Black- oder Whitelist eintragen und ihren Eintrag entsprechend begründen können. Dies schützt Händler vor weiteren Betrugsrisiken und wiederholten Vergehen. Zudem vergrößert es die Ogone Fraud Expert Datenbank und steigert ihre Performance.

WICHTIG

Wählen Sie nur dann „tatsächlicher Betrug“, wenn Sie eine Rückbelastung mit einem Ursachencode für Betrug erhalten haben.


## 5.1 Eingabe von Transaktionsdaten in eine Black- oder Whitelist

1. Klicken Sie auf die „PAYID“ unter der Transaktionsansicht, um nach der Transaktion zu suchen, für die Sie Handelsstreitigkeiten, einen tatsächlichen Fall von Betrug oder einen Verdacht auf Betrug berichten wollen.




2. Klicken Sie auf die Schaltfläche „DISPUTE“, um die Daten aufzulisten, die Sie in Bezug auf die Transaktion erhalten haben und die in die Black- oder Whitelist aufgenommen werden können.

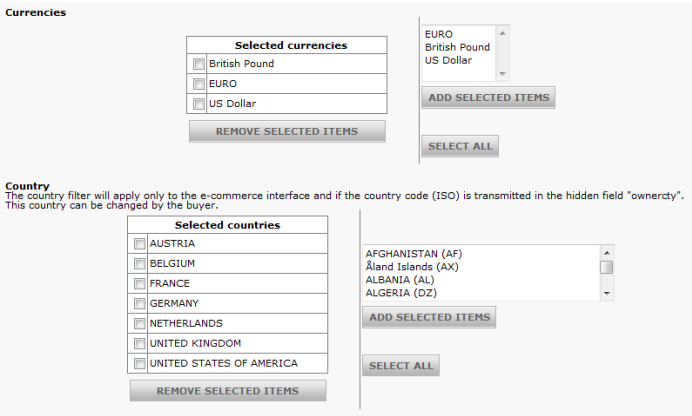
3. Gehen Sie auf die „Dispute”-Seite und wählen Sie die Liste, in die Sie die Transaktionsdaten eingeben wollen (Blacklist oder Whitelist). Wählen Sie dann den Grund für den Disput bzw. Streifall.

   Sie können die Transaktion markieren als:

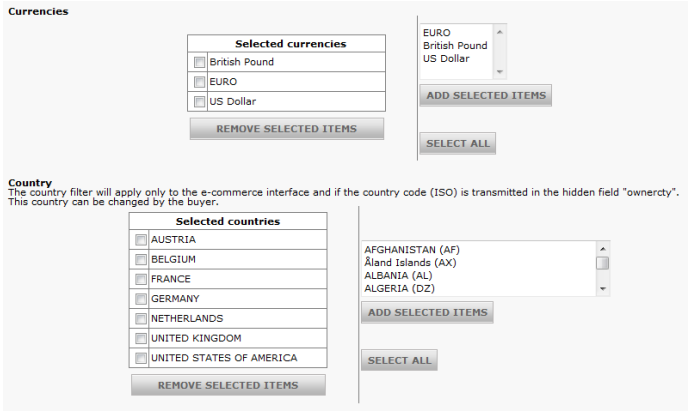
   - Handelsstreitigkeit umfasst alle Rückbelastungen, die der Händler erhalten hat und die keinen Betrugsfall darstellen.
   - Tatsächlicher Betrug bedeutet, dass Sie eine Rückbelastung aufgrund eines Betrugs erhalten haben.
   - Verdacht auf Betrug bedeutet, dass Sie aufgrund eines Verdachts eine betrügerische Transaktionen verhindern wollen.

   Die jeweilige Auswahl der Schaltfläche ist mit unterschiedlichen Auswirkungen auf die Betrugsdatenbank verbunden.

   Anmerkung: Tatsächlicher Betrug findet nur im Falle einer Rückbelastung aufgrund eines Betrugs Anwendung.



4. Speichern und bestätigen Sie Ihre Auswahl, um die Daten der entsprechenden Liste hinzuzufügen. Die Betrugsprüfung wird sofort wirksam.




Auf der „Dispute"-Seite können Sie ebenfalls die Daten auswählen (z. B. die zu Ihrem Callcenter oder VIP-Kunden gehören), die in die Whitelist aufgenommen werden sollen. Wenn Sie Daten auswählen, die zuvor in der Blacklist waren, dann werden sie der Whitelist automatisch hinzugefügt. Die Betrugsprüfung wird sofort wirksam.

# 6 Betrugserkennungsmodul - Feedback

## 6.1 Transaktionen ansehen im back-office

### 6.1.1 Erweiterte Auswahlkriterien

Wenn Sie über den Link „Transaktionsansicht" oder den Link „Finanzielle Historie" eine Transaktion in Ihrem Kontomenü suchen, steht Ihnen unter „Erweiterte Auswahlkriterien" die Extraoption „IP-Adresse" zur Verfügung. Verwenden Sie das IP-Adressfeld für die Suche nach IP-Adressen. Eine Suche nach den ersten Stellen einer IP-Adresse ist ebenfalls möglich.

### 6.1.2 3-D Secure in Transaktionslisten

Wenn Sie in Ihrem Back-Office-Menü Ihre Transaktionsliste über „Transaktionsansicht" oder „Finanzielle Historie" anzeigen, sehen Sie grüne Punkte sowie halbe Punkte in der Liste (falls 3-D Secure für Ihr Konto aktiviert ist).

Der volle Punkt mit dem Daumen nach oben stellt eine 3-D Secure Transaktion dar, die von Ihrem Kunden mit einer Kreditkarte bezahlt wurde, die für 3-D Secure registriert war. Für diese Transaktionen gewährt Ihnen Ihr Acquirer eine Zahlungsgarantie (s. Abschnitt 2.1.2).

Der halbe Punkt steht für eine 3-D Secure Transaktion, die mit einer Kreditkarte bezahlt wurde, die nicht für die Teilnahme am 3-D Secure Service registriert war. Für diese Transaktionen gibt es eine „eingeschränkte" Zahlungsgarantie (s. Abschnitt 2.1.2). Basis dafür bilden die Vertragsdetails, die dem 3-D Secure Vertrag zu Grunde liegen, den Sie mit Ihrem Acquirer geschlossen haben.

Transaktionen ohne einen (halben) Punkt wurden nicht im Rahmen von 3-D Secure abgewickelt. Für diese Transaktionen gibt es keine Zahlungsgarantie (s. Abschnitt 2.1.2).

Positionen mit einem Ausrufezeichen kennzeichnen Transaktionen, bei denen die Karteninhaber-Authentifizierung fehlgeschlagen ist. Es besteht keine Zahlungsgarantie (s. Abschnitt 2.1.2) für Transaktionen, deren Verarbeitung sie fortsetzen, bei denen jedoch die Authentifizierung fehlgeschlagen ist (für MasterCard, s. Abschnitt 2.2.3).

### 6.1.3 Transaktionsdetails

In den Transaktionsdetails (Finanz-Seite) werden zusätzliche Informationen angezeigt, wie etwa das Ergebnis des Card Verification Codes (falls der CVC-Code von dem Kunden angegeben wurde), Kartenland, IP-Adress-Land und IP-Adresse.


Mit Hilfe des Buttons „Dispute" oberhalb der Tabelle mit den Zusatzinformationen, gelangen Sie auf eine Seite, auf der Sie mit einem Klick Ihren Blacklists bestimmte Transaktionsdetails hinzufügen können. Diese Option ermöglicht Ihnen beispielsweise, Ihrer Blacklist die Kartennummer hinzuzufügen, die für die Transaktion verwendet wurde, ohne dass Sie die vollständige Kartennummer kennen müssen.

Darüber hinaus können Sie die Transaktion als kommerziellen Streitfall (Commercial dispute) oder als betrügerische Transaktion (Actual fraud) kennzeichnen.

WICHTIG

Kennzeichen Sie nur eine Transaktion als “Tatsächlichen Betrug” (Actual fraud), wenn der Kunde in der Tat diese Karte für betrügerische Umsätze genutzt hat. Dies ist zum Beispiel der Fall, wenn jemand eine Karte einsetzt, die ihm nicht gehört.


### 6.1.4 Fehlercodes

Wenn unser System - auf Basis der Parameter, die Sie im Betrugserkennungsmodul festgelegt haben – eine Transaktion zurückgehalten hat, erhalten Sie eine Fehlermeldung, aus der Sie den Grund entnehmen können.

Die folgende Liste zeigt Beispiele der wichtigsten Fehlermeldungen / Codes. (Bitte beachten Sie, dass die Liste keinen Anspruch auf Vollständigkeit erhebt):

3 / 30001100 Land des Käufers ist nicht freigeschaltet

3 / 30001120 IP-Adresse in Sperrliste des Händlers

3 / 30001130 BIN in Sperrliste des Händlers

3 / 30001140 Karte in Kartensperrliste des Händlers

Liste der Status- und Fehlermeldungen

## 6.2 Zusätzliche Transaktionsparameter

In Ihren Post-Sale-Anfragen, Umleitungen mit Feedback, Datei-Downloads und DirectLink XML-Antworten werden mit Bezug auf das Betrugserkennungsmodul zusätzliche Transaktionsparameter zurückgesendet.

Nachfolgend die Liste der zusätzlichen Parameter.

Die Felder sind leer, falls im Rahmen der Format-Validierung ein Fehler bei den Transaktionsdetails auftritt.

| Parameter | Wert |
|---|---|
| IPCTY | Das Herkunftsland der IP-Adresse.<br>Format: Zweistelliger alphabetischer ISO-Code. Falls dieser Parameter nicht verfügbar ist, wird in der Antwort der Wert „99” zurückgesendet.<br>Diese IP-Prüfung arbeitet mit externen IP-Listen. Aus diesem Grund ist mit der Prüfung ein |

| Parameter | Wert |
|---|---|
| | geringfügiges Risiko verbunden, da wir uns auf die Korrektheit dieser Listen verlassen müssen. Die Prüfungen führen in 94 % der Fälle zu positiven Ergebnissen. |
| CCCTY | Herkunftsland der Kreditkarte.<br>Ausschließlich für VISA, MasterCard American Express und Diners Club verfügbar. Bei allen anderen Marken/Zahlungsmethoden ist dieses Feld leer. Format: Zweistelliger alphabetischer ISO-Code. Falls dieser Parameter nicht verfügbar ist, wird in der Antwort der Wert „99" zurückgesendet<br>Die Prüfung des Kreditkartenlandes arbeitet mit externen IP-Listen. Aus diesem Grund ist mit der Prüfung ein geringfügiges Risiko verbunden, da wir uns auf die Korrektheit dieser Listen verlassen müssen. Die Prüfungen führen in 94 % der Fälle zu positiven Ergebnissen. |
| ECI | Electronic Commerce Indicator. Mögliche ECI-Werte und ihre Bedeutung:<br>1 Manuelle Eingabe: Mail Order/Telephone Order (MOTO)<br>2 Wiederkehrende Zahlungen, von MOTO abstammend<br>3 Ratenzahlungen<br>5 Karteninhaber-Authentifizierung erfolgreich<br>6 Händler unterstützt Authentifizierung, Karteninhaber jedoch nicht, Anwendung der Zahlungsgarantierichtlinien (s. Abschnitt 2.1.2)<br>7 E-Commerce mit SSL-Verschlüsselung<br>9 Wiederkehrend nach erster E-Commerce-Transaktion<br>1 Händler unterstützt Authentifizierung,<br>2 Karteninhaber jedoch nicht, Anwendung der Zahlungsgarantierichtlinien (s. Abschnitt 2.1.2) (identisch mit 6)<br>9 Karteninhaber-Authentifizierung<br>1 FEHLGESCHLAGEN !!!! (Zahlungsgarantie (s. Abschnitt 2.1.2) kann gegebenenfalls angewendet werden, mit Acquirer prüfen)<br>9 Authentifizierungsstelle der<br>2 kartenausgebenden Bank zeitweise nicht verfügbar, Transaktionsabwicklung jedoch fortgesetzt |
| CVCCheck | Ergebnis des Kartenprüfnummer-Checks (Card Verification Code - CVC). Mögliche Werte:<br>KO: Der CVC wurde gesendet, der Acquirer hat allerdings nach Überprüfung eine negative Antwort erteilt, d.h. der CVC ist falsch.<br>OK:<br>1. Der CVC wurde gesendet, der Acquirer hat nach Überprüfung eine positive Antwort gegeben, d.h. der CVC ist korrekt ODER<br>2. Der Acquirer hat einen Genehmigungscode gesendet, hat jedoch kein spezielles Ergebnis für eine CVC-Prüfung zurückgesandt.<br>NO: Alle anderen Fälle. Zum Beispiel: kein CVC übermittelt, der Acquirer hat geantwortet, dass keine CVC-Prüfung möglich war, der Acquirer hat die Autorisierung abgelehnt, jedoch kein |

| Parameter | Wert |
|---|---|
| | spezielles Ergebnis einer CVC-Prüfung zurückgesandt ... |
| AAVCheck | Ergebnis der automatischen Adressprüfung. Die Adressprüfung steht derzeit nur für American Express Karten zur Verfügung. Mögliche Werte:<br>KO: Die Adresse wurde gesendet, aber der Acquirer hat nach Prüfung der Adresse eine negative Antwort gegeben, d.h. die Adresse ist falsch.<br>OK:<br>1. Die Adresse wurde gesendet und der Acquirer hat nach Prüfung der Adresse eine positive Antwort gegeben, d.h. die Adresse ist korrekt ODER<br>2. Der Acquirer hat einen Autorisierungscode gesendet, hat jedoch keine spezielle Antwort in Bezug auf die Adressprüfung gegeben.<br>NO: Alle anderen Fälle. Zum Beispiel: keine Adresse übermittelt; der Acquirer hat geantwortet, dass eine Adressprüfung nicht möglich war; der Acquirer hat die Autorisierung abgelehnt, hat jedoch kein spezielles Ergebnis in Bezug auf eine Adressprüfung mitgeteilt ... |
| VC | Virtuelle Karte. Mögliche Werte:<br>ECB: Für E Carte Bleue<br>ICN: Für „Internet City Number“ (Internet Stadt-Nummer)<br>NO: Alle anderen Fälle. Zum Beispiel: die Karte ist keine virtuelle Karte, die Karte ist eine Art von virtueller Karte, die wir nicht kennen ... |
| IP | Kunden-IP-Adresse, von unserem System anhand eines dreistufigen Integrationsprozesses ermittelt - oder vom Händler im Rahmen eines zweistufigen Integrationsprozesses an uns gesendet. |

# 7 Anhang 1: CVC2 und AAV

## 7.1 CVC2

CVC2 ist ein Authentifizierungsprozess, der von den Kreditkartenunternehmen zur Verhinderung von Kreditkartenmissbrauch bei Internet-Transaktionen eingeführt wurde. Der Code hat unterschiedliche Bezeichnungen, je nach Marke (MasterCard: CVC2 oder Card Validation Code; VISA: CVV2 oder Card Verification Value; American Express: CID oder Card Identification Number). Im Allgemeinen wird der Code jedoch als „CVC" bezeichnet. Die CVC2-Funktionalität ist für alle Marken identisch.

Der Verifizierungscode ist mit der Kartennummer verbunden, ist jedoch nicht Bestandteil der Kartennummer selbst. Je nach Kartenmarke handelt es sich um einen drei- oder vierstelligen Code, der sich auf der Vorder- oder Rückseite der Karte befindet, eine Ausgabenummer, ein Beginn- oder ein Geburtsdatum. Im Falle von MasterCard und VISA ist es beispielsweise ein dreistelliger Code im Unterschriftsfeld auf der Kartenrückseite, im Anschluss an die vollständige Kartennummer oder im Anschluss an die letzten vier Stellen der Kartennummer.

Für Händler und deren Service Provider ist es strengstens verboten, den CVC2-Code von Kunden in einer Datenbank zu speichern. Wenn der Karteninhaber nicht persönlich anwesend ist, d.h. im Falle von Fernabsatztransaktionen („Card Not Present"), wird er gebeten, zusammen mit seiner Kartennummer die Kartenprüfnummer (CVC2-Code) anzugeben. Mit Hilfe des Verifizierungscodes kann sichergestellt werden, dass dem Kunden, der den Auftrag erteilt, die tatsächliche Karte vorliegt und er der rechtmäßige Inhaber des Kartenkontos ist.

## 7.2 AAV

AAV ist eine Authentifizierungsmethode, die in einigen Märkten zur Verfügung steht und dazu beitragen soll, den missbräuchlichen Einsatz von Kreditkarten bei Internet-Transaktionen zu verhindern. Die Bezeichnungen für diesen Service unterscheiden sich je nach Marke. VISA / MasterCard: AVS oder Address Verification Service/System; Amercian Express: AAV oder Automated Address Verification). Die Funktionalität von AAV ist jedoch für alle Marken gleich.

Die Adressprüfung findet statt, wenn der Acquirer das kartenausgebende Institut bittet, die nummerischen Komponenten (Hausnummer und PLZ) der Kundenadresse (Rechnungs- oder Versandadresse), die uns der Händler gesendet hat, mit der Rechnungsadresse zu vergleichen, die der Kunde dem kartenausgebenden Institut bei der Kartenbeantragung angegeben hat.

American Express führt diese Prüfung automatisch durch, wenn das Unternehmen Adressdetails mit einer Transaktion erhält. Bei den anderen Kartenorganisationen hängt es davon ab, ob der Acquirer die Adressprüfung durchführt oder nicht. Wir empfehlen in jedem Fall, zusammen mit den Auftragsdetails, die Sie an unser System senden, auch die Adressdetails des Kunden zu übermitteln.

Eine Transaktion wird aufgrund des Ergebnisses der Adressprüfung niemals abgelehnt. Dennoch kann das Ergebnis für die Entscheidung des Händlers eine Rolle spielen, ob er die Ware an den Kunden ausliefert oder den Kunden vor dem Versand um weitere Informationen bittet.