Módulo de Detección de Fraude

v.4.2.3

ingenico ePayments

Contenidos

1 ¿Qué es el módulo de detección de fraude?

En la venta a distancia, la lucha contra el fraude requiere niveles máximos de conocimientos técnicos, velocidad y flexibilidad. Para ayudarle a implementar una gestión eficaz de riesgos, el módulo de detección de fraude ofrece un servicio en tiempo real que ofrece toda la información de análisis necesaria. Además, ofrece protección completa y personalizada para gestionar las transacciones sospechosas.

El uso del módulo de detección de fraude, sin embargo, no garantiza la protección frente a todos los fraudes: solo ayuda a evitarlos. El módulo de detección de fraude se puede configurar en función de los riesgos o problemas con fraudes anteriores detectados en su empresa.

1.1 Ventajas

El módulo de detección de fraude le permite:

- Detectar anomalías durante las transacciones
- Bloquear intentos por parte de defraudadores reconocidos de forma inmediata
- Protegerse frente a riesgos específicos del país
- Definir y aplicar políticas de seguridad totalmente personalizadas
- Beneficiarse de una garantía de pago condicional de acuerdo con las políticas de su entidad adquirente individual (3-D Secure)

1.2 Acceso

Puede acceder al módulo de detección de fraude a través del enlace "Detección de fraude" en su menú de cuenta.

1.3 Contenido

El módulo de detección de fraudes cuenta con tres áreas funcionales separadas:

- Activación y configuración de la detección de fraude
- 3-D Secure
- Lista negra/lista blanca/lista gris

IMPORTANTE

Los criterios de VISA/MasterCard descritos en esta documentación no están necesariamente disponibles para todos los métodos de pago. La disponibilidad de "Activación y configuración" depende del método de pago. Para algunos métodos de pago, la configuración está limitada. Le recomendamos que consulte los criterios específicos de selección de sus métodos de pago individuales haciendo clic en el botón "Editar" situado junto al método de pago en la tabla "Activación y configuración de detección de fraude" de su módulo de detección de fraude.

2 Activación y configuración de la detección de fraude

En la tabla "Activación y configuración" verá la distinción entre tarjetas de crédito y otros métodos de pago.

La tabla contiene normas de bloqueo y límites opcionales. "No" indica que no se ha configurado ninguna característica en la página de la opción correspondiente. Si una página se ha configurado ya, el estado será "Sí".

Ahora vamos a examinar con mayor detalle la configuración de las opciones de detección de fraude de las tarjetas de crédito.

2.1 Tarjetas de crédito

Para configurar las opciones de detección del fraude para una tarjeta de crédito específica, haga clic en el botón "Editar" junto al método de pago. A continuación accederá a la página de configuración, con pestañas para las normas de bloqueo y límites.

2.1.1 Normas de bloqueo

Las normas de bloqueo entran en vigor una vez que el cliente ha introducido los detalles de su tarjeta de crédito y hecho clic en el botón procesar.

Si la transacción no cumple con las reglas especificadas, retendremos la transacción y estableceremos su estado en "Autorización rechazada".

2.1.1.1 País de dirección IP

Todos los países de la dirección IP se aceptan de forma predeterminada. Nuestro sistema puede identificar el país de la dirección IP en función de la dirección IP del cliente (aunque este control de IP ofrece resultados positivos en el 94 % de todos los casos, se basa en listados de IP suministrados de forma externa, por lo que existe un mínimo riesgo de error, ya que dependemos de la precisión de esta lista).

Si desea establecer una lista de países de direcciones IP, puede seleccionarlos en la lista del lado derecho de la pantalla y hacer clic en el botón "Añadir".

IMPORTANTE

TLos códigos A1 (Proxy anónimo), AP (Región Asia Pacífico), EU (Red europea) y A2 (Proveedores de satélite) hacen referencia a las direcciones IP cuyo país de origen es dudoso.

EU, por ejemplo, significa que el país de IP exacto es incierto pero pertenece a Europa. La aceptación de EU como país de dirección IP no significa que vaya a aceptar pagos de todos los países de Europa, sino que acepta pagos de direcciones IP gestionadas por instituciones europeas. Si desea aceptar pagos de países específicos de Asia o Europa, deberá añadir los países uno por uno a su lista.

Los proxies anónimos son proveedores de acceso a Internet que permiten a los usuarios de Internet ocultar sus direcciones IP. Le recomendamos que no acepte pagos procedentes de proxies anónimos!

Encima de la lista de países de dirección IP seleccionados, tiene las opciones para establecer su lista en países aceptados (solo aceptar pago de la lista de países) o países rechazados (rechazar pago de la lista de países).

Siempre puede eliminar un país de la lista haciendo clic en la casilla "Supr" situada delante del país y haciendo clic a continuación en el botón "Enviar" situado debajo de la lista.

2.1.1.2 Consistencia de país (solo para VISA, MasterCard, American Express y Diners Club)

Al establecer este parámetro en "Sí", solo permitirá transacciones cuando la dirección IP del cliente pertenezca al mismo país que su emisor de tarjeta de crédito. Es decir: solo si el país de la tarjeta y el país de la dirección IP coinciden. Este control se realiza si la dirección IP pertenece a un proxy anónimo, la red

Asia Pacífico, la red europea o un proveedor por satélite.

2.1.1.3 3-D Secure (solo para Visa/MasterCard/JCB/AmEx)

Este parámetro le permite omitir las normas de bloqueo establecidas antes si el titular de la tarjeta se identifica mediante 3-D Secure.

Cuando una tarjeta de crédito es 3-D Secure y tiene un contrato de este tipo con su entidad adquirente, tendrá una garantía de pago condicional (consulte la sección 2.1.2) para la transacción. Aunque no desee recibir pagos del país X a partir de ahora debido a un alto riesgo de fraude, puede seguir permitiendo transacciones con tarjetas de crédito 3-D Secure del país X, ya que no tendrá ningún riesgo en relación con disputas sobre la no identificación del titular. (No obstante, esto no se aplica a disputas sobre otros asuntos). Véase qui).

2.1.2 Límites

En el módulo de detección de fraude, puede limitar el importe por transacción.

Puede especificar un importe mínimo y máximo. Si el importe de la transacción no está dentro de los límites especificados, retendremos la transacción y estableceremos su estado como Autorización rechazada.

La divisa del límite será la divisa de su cuenta principal. Si tiene varias divisas y una transacción se produce en una distinta a la predeterminada, nuestro sistema convertirá el límite en la otra divisa.

3 3-D Secure

3-D Secure ofrece una seguridad de alto nivel, ya que permite a los clientes identificarse de forma inequívoca a través de tecnologías como, por ejemplo, contraseñas html, Digipass, lectores de tarjeta, biométrica, etc. implementadas por los bancos emisores.

Al ofrecer 3-D Secure, un comerciante se beneficia de una garantía de pago condicional (véase aqui), tal como se describe en el contrato de 3-D Secure con su entidad adquirente. Bajo estas condiciones, la cuenta de un comerciante ya no se carga para disputas sobre la "no identificación del titular". (Esto no se aplica a disputas sobre otros asuntos).

Las siguientes marcas han implementado el protocolo 3-D Secure:

- Visa bajo el nombre de Verified by Visa
- MasterCard bajo el nombre de SecureCode
- JCB bajo el nombre de J-Secure
- American Express bajo el nombre de SafeKey

3.1 General

3.1.1 Solicitud de afiliación

Si en su cuenta no se ha activado 3-D Secure, verá el botón "Request 3-DS" (Solicitar 3DS) en la tabla "3-D Secure".

Si hace clic en este botón "Request 3-DS" (Solicitar 3DS), se enviará un correo electrónico a su entidad adquirente. Si su contrato con la entidad adquirente no ofrece 3-D Secure, puede ponerse en contacto con esta para obtener más información sobre cómo registrarse en 3-D Secure si desea que su entidad adquirente le ofrezca esta opción de pago.

Nota: Para inscribirse en SafeKey, póngase en contacto con American Express o vaya al portal de SafeKey.

Una vez se haya habilitado 3-D Secure en su cuenta, verá la fecha de activación en la tabla. Puede cambiar la configuración para 3-D Secure haciendo clic en el botón de editar situado junto a los métodos de pago.

3.1.2 Procesamiento de transacciones de 3-D Secure estándar

1. Cuando recibamos los detalles de la tarjeta de crédito de su cliente, nuestro sistema enviará una solicitud al directorio VISA/MasterCard/JCB/AmEx para establecer si la tarjeta está registrada. Por ejemplo, si el titular ha recibido algunos medios de identificación vinculados a su tarjeta y, si corresponde, obtiene los datos del servidor de autenticación del emisor.

2. Si la tarjeta está registrada, nuestro sistema redirecciona al cliente al servidor de autenticación del emisor para iniciar la autenticación.

3. Nuestro sistema recibe el resultado de la autenticación y procesa el pago de la forma habitual.

Si la autenticación es satisfactoria, el comerciante podrá beneficiarse de la garantía de pago condicional suministrada por su entidad adquirente.

Si la tarjeta no está registrada, el comerciante recibe algún nivel de garantía de pago condicional suministrada por su entidad adquirente.

Por tanto, en ambos casos y bajo determinadas circunstancias (definidas por VISA; MasterCard y las organizaciones financieras, y tal como se describe en el contrato de 3-D Secure con su entidad adquirente), el comerciante tiene una garantía de pago, incluso sin recibir información de identificación del cliente. Estas reglas de pago condicional se gestionan de forma exclusiva entre el comerciante y su entidad adquirente. Ingenico ePayments solo actúa como intermediario técnico.

3.2 Opciones de configuración

A continuación, se muestran las opciones de configuración para Verified by Visa, MasterCard SecureCode, J-Secure y SafeKey. Dependiendo de su entidad adquirente, algunas (o todas) estas opciones podrían no estar disponibles.

3.2.1 Problema técnico

El comerciante puede elegir continuar con la transacción o interrumpirla si un problema técnico impide la conexión con el directorio VISA/MasterCard/JCB/AmEx durante el control de registro de 3-D Secure.

Si un problema técnico impide que nuestro sistema se conecte al directorio VISA/MasterCard/JCB/AmEx (paso 1), VISA/MasterCard/JCB/AmEx recomienda que el proceso se continúe sin autenticación (opción *continuar*). En este caso, el comerciante no se beneficiará de la garantía de pago condicional (véase aqui).

3.2.2 Servicio de identificación no disponible de forma temporal

El comerciante puede decidir *continuar* o *interrumpir* la transacción si el servicio de identificación del titular de la tarjeta no está disponible de forma temporal.

Si el servidor de autenticación del emisor no está disponible de forma temporal (paso 2 más arriba), será imposible la identificación del titular de la tarjeta. En este caso, VISA/MasterCard/JCB/AmEx recomienda continuar con el proceso (opción *continuar*). En este caso, el comerciante no se beneficiará de la garantía de pago condicional (véase aqui).

3.2.3 Fallos de autenticación (solo MasterCard)

El comerciante puede *continuar* o *interrumpir* la transacción si la autenticación falla.

Si falla la autenticación del titular (paso 3), MasterCard recomienda interrumpir el proceso de pago (opción *Interrumpir*). Si la transacción continúa, el comerciante no se beneficiará de la garantía de pago condicional (véase aqui).

3.2.4 Activar/desactivar 3-D Secure

Aquí el comerciante puede activar/desactivar 3-D Secure para todas las tarjetas VISA/MasterCard/JCB/AmEx. Nota: si 3-D Secure está deshabilitado, el comerciante no se beneficiará de la garantía de pago condicional (véase aqui).

3.2.5 Desactivar BIN específico de 3-D Secure

El comerciante puede introducir determinados intervalos de BIN en los que desee desactivar 3-D Secure, si el titular de tarjeta no está registrado.

Si la tarjeta no está registrada, el comerciante no se beneficiará de la garantía de pago condicional (véase aqui) para pagos realizados con una tarjeta que empieza por estos seis dígitos.

4 Lista negra/lista blanca

En el módulo de detección de fraude, puede generar sus propias listas negras para tarjetas de crédito en función de los códigos BIN, números de tarjeta de crédito y direcciones IP desde las que no desea aceptar transacciones, así como una lista blanca basada en direcciones IP.

"No" indica que no se ha configurado nada en la página de la lista negra/lista blanca correspondiente. Cuando ya se ha configurado una lista negra/blanca, el estado será "Sí".

Si para una nueva transacción en su cuenta el IB, el número de tarjeta de crédito o la dirección IP se han especificado en su lista negra, retendremos la transacción y estableceremos su estado como "Autorización rechazada".

4.1 Tarjetas de crédito

Puede especificar hasta 50 entradas por lista.

Puede añadir un comentario a una entrada de una lista negra o blanca. Puede introducirlo en el momento del envío especificando el comentario en el campo "Comentario". También puede añadir o borrar un comentario en la columna de comentarios haciendo clic en el enlace "...".

Para cada entrada de lista negra puede seleccionar el motivo por el que desea bloquear el elemento: fraude real o disputa comercial.

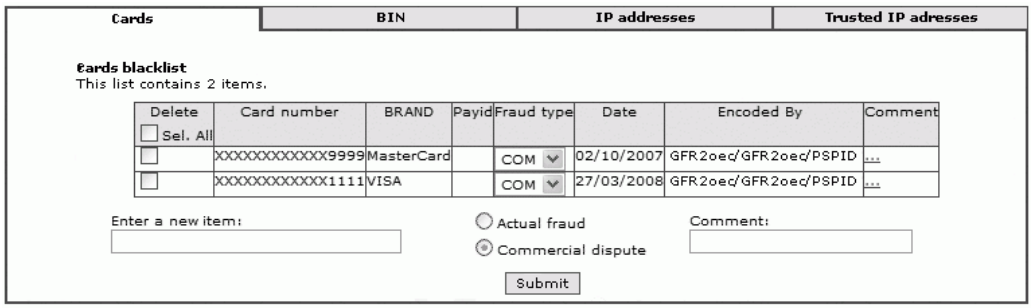
IMPORTANTE

Solo debe seleccionar "fraude real" como tipo si el cliente realmente ha cometido un fraude, por ejemplo, si un titular de tarjeta utiliza una tarjeta que no le pertenece.

4.1.1 Lista negra de tarjetas

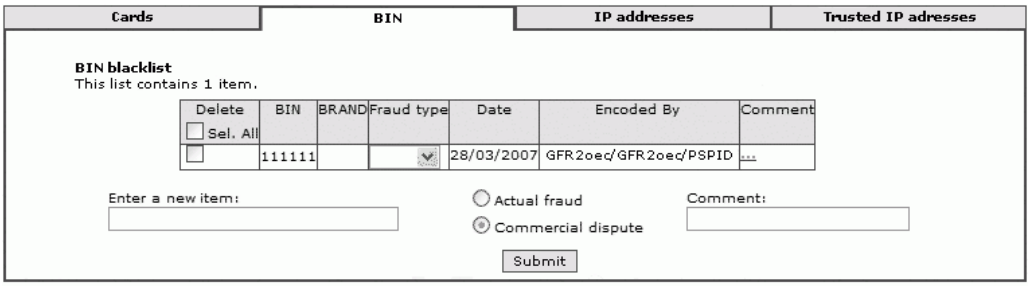
En su lista negra de tarjetas de crédito, debe especificar el número completo de esta. Siempre puede eliminar los números de la tarjeta de crédito que ha introducido en la lista.

Si ha activado el método de pago de transferencias bancarias en su cuenta, la lista negra de tarjetas también se duplicará como lista negra de cuentas para introducir números de cuenta.



4.1.2 Lista negra de BIN

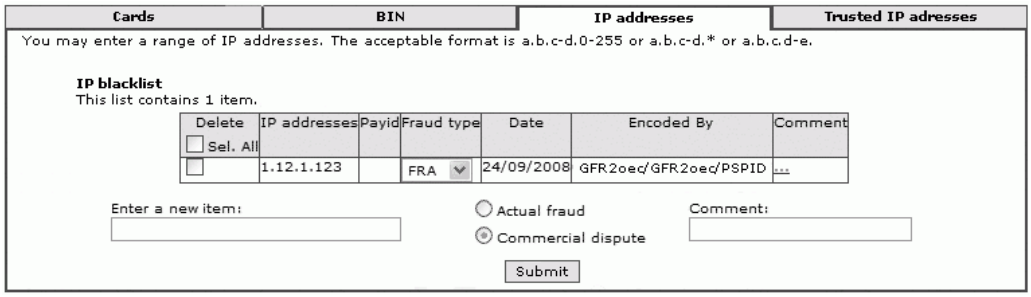
El código BIN son los primeros 6 dígitos del número de la tarjeta de crédito. Un código BIN está vinculado a un banco concreto de un país específico. Por lo tanto, puede especificar todas las tarjetas de crédito emitidas por el banco X en el país Y en su lista negra con tan solo añadir el código BIN. Siempre puede eliminar los códigos BIN que ha introducido en la lista:



4.1.3 Lista negra de IP

En la lista negra de direcciones IP no solo puede introducir una dirección IP específica, sino también un rango de direcciones IP usando los siguientes formatos: a.b.c-d.0-255 o a.b.c-d.* o a.b.c.d-e. Siempre puede eliminar direcciones IP que se hayan especificado en la lista.

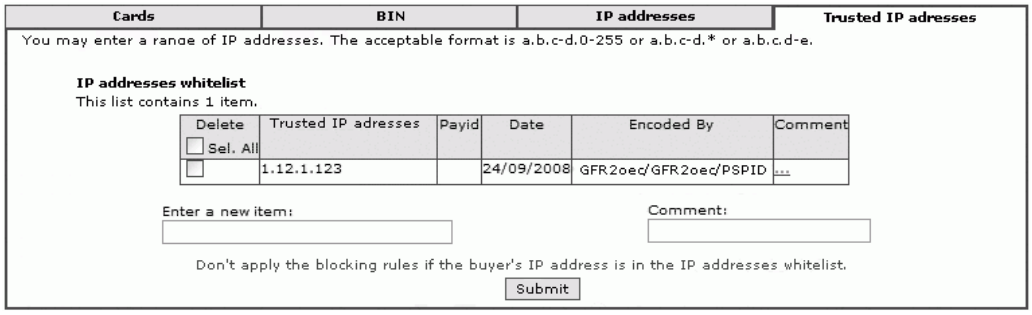
Para que nuestro sistema compruebe la dirección IP del cliente, los comerciantes que trabajen a través de DirectLink deben enviar la dirección IP en el campo "REMOTE_ADDR".



4.1.4 Lista blanca de direcciones IP

Si mediante el bloqueo de determinados países o países de direcciones IP en las normas de bloqueo ha bloqueado a un cliente específico del que desea aceptar pedidos, puede especificar su dirección IP en la lista de direcciones IP de confianza. De este modo permitirá que se envíen transacciones usando esta dirección IP, aunque sea de un país que haya bloqueado. Siempre puede eliminar las direcciones IP que ha introducido en la lista.

Para que nuestro sistema compruebe la dirección IP del cliente, los comerciantes que trabajen a través de DirectLink deben enviar la dirección IP en el campo "REMOTE_ADDR".



5 Dispute

La aceptación de transacciones en cualquier entorno conlleva riesgos inherentes como, por ejemplo, el riesgo de devoluciones de cargos. Especialmente al procesar en un entorno tarjeta no presente (CNP), los riesgos de devoluciones de cargos están siempre presentes.

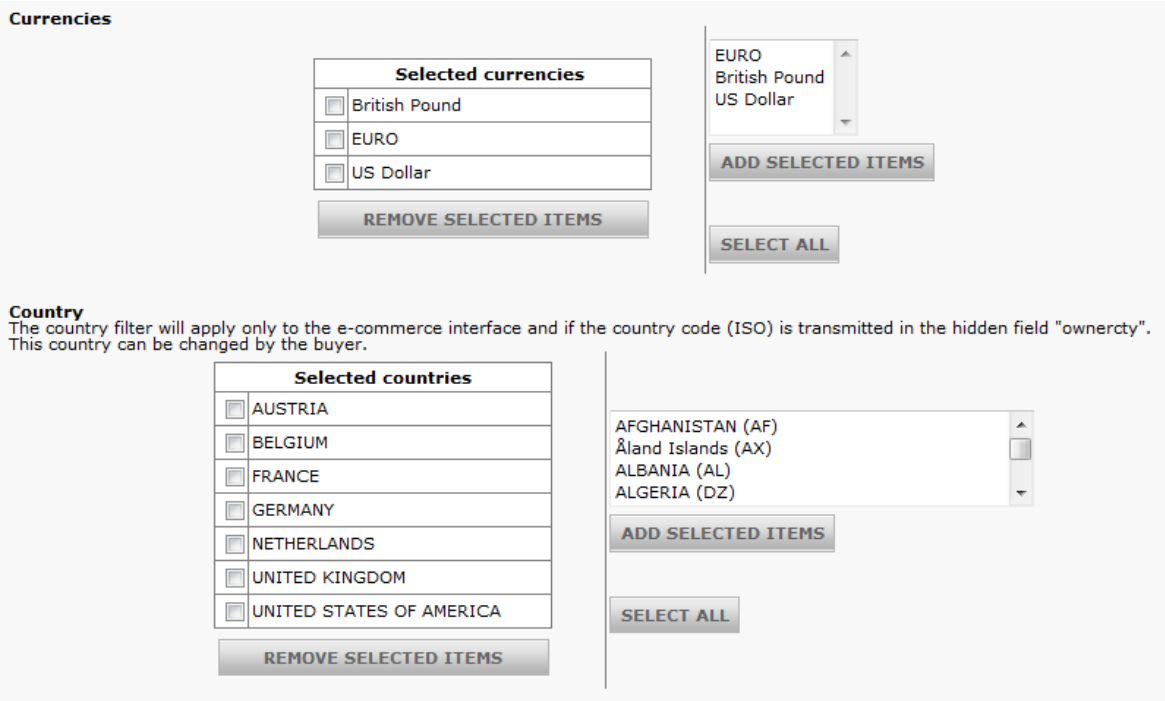
Ingenico ePayments proporciona a los clientes una página de disputa que permite a los comerciantes añadir datos de transacciones a listas negras y blancas con el motivo adecuado tras la disputa. Esto protege a los comerciantes frente a una mayor exposición al fraude y evita que las infracciones se repitan. También mejora la base de datos de Ingenico ePayments Fraud Expert y mejora su rendimiento.

IMPORTANTE

Seleccione solo "fraude real" cuando haya recibido una devolución de cargo con un código de motivo de fraude.

5.1 Añada los datos de transacción a una lista negra y blanca

1. Haga clic en el "PAYID" en la vista de transacción para buscar las transacciones que desea notificar para disputa comercial, fraude real o sospecha de fraude.



2. Haga clic en el botón "DISPUTE" para enumerar los datos recibidos para la transacción que se pueden añadir a la lista negra y blanca.

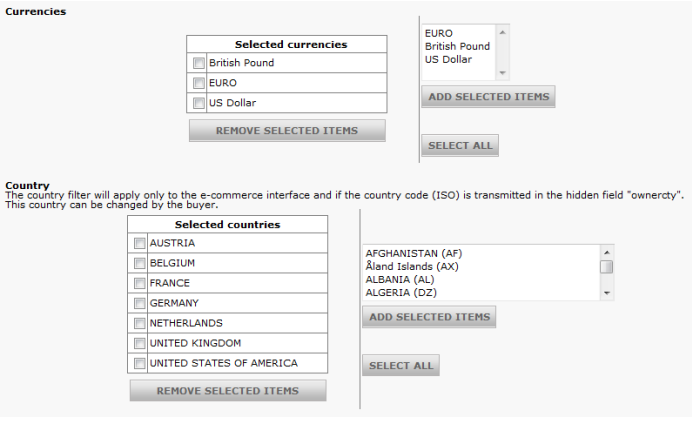
3. Acceda a la página de disputas y elija la lista que desea añadir a los datos de transacción (Lista negra o Lista blanca). A continuación, seleccione el motivo de la disputa.

   Puede marcar la transacción como:

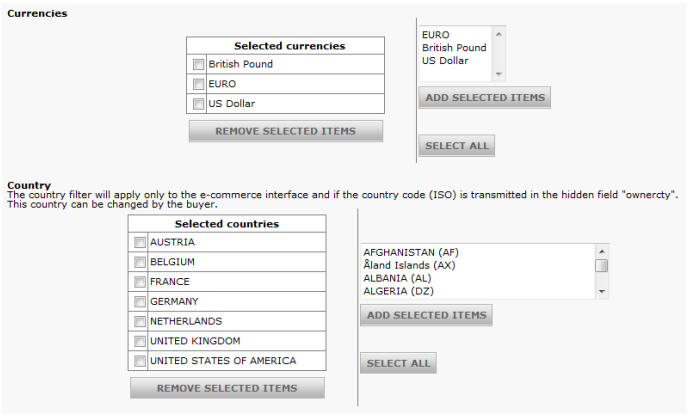
   - Disputa comercial cubre todas las devoluciones de cargo que el comerciante ha recibido que no están relacionadas con fraude.
   - El fraude real es cuando recibe una devolución de cargo por fraude.
   - La sospecha de fraude es cuando tiene sospechas y desea evitar una transacción fraudulenta.

   Seleccionar un botón u otro afecta a la base de datos de fraudes de modo distinto.

   Nota: El fraude real solo se aplica a la devolución de cargo de fraude.



4. Save and confirm to add the data to the appropriate List. The fraud check takes into effect immediately.



From the dispute page, you can also select the data (e.g., belonging to your call center, VIP client, etc.) to be added in the whitelist. If you select data that were previously in the blacklist, they will automatically be added to the whitelist. The fraud check takes into effect immediately.

6 Comentarios

6.1 Vista de transacciones en el área de administración

6.1.1 Criterios de selección avanzados

Al buscar una transacción a través del enlace "Ver transacciones" o "Historial financiero" del menú de su cuenta, aparecerá "Dirección IP" en una opción extra de los "Criterios de selección avanzados". Puede utilizar el campo de la dirección IP para buscar todas las transacciones desde la misma dirección IP o desde direcciones IP que empiecen por los mismos dígitos.

6.1.2 Transaction List

Si no hay resultado de puntuación para la transacción, por ejemplo, cuando la autorización se ha rechazado, observará puntos verdes y (si ha activado 3-D Secure en su cuenta) medios puntos en la lista.

El punto completo  , en el que el pulgar está hacia arriba, representa una transacción de 3-D Secure en la que el cliente ha pagado con una tarjeta de crédito registrada con esta tecnología. Con estas transacciones, su entidad adquirente le ofrece una garantía de pago condicional.

El medio punto  representa una transacción de 3-D Secure en la que el cliente ha pagado con una tarjeta de crédito que no está registrada con esta tecnología. Estas transacciones conllevan un determinado grado de garantía de pago condicional, que depende de los detalles específicos del contrato de 3-D Secure con su entidad adquirente.

Las transacciones sin ningún punto, medio o completo, son aquellas que no se han procesado con 3-D Secure. La garantía de pago condicional no se aplicará a estas transacciones.

Las transacciones con un signo de exclamación  indican transacciones en las que ha fallado la autenticación del cliente. La garantía de pago condicional no se aplicará a transacciones para las que haya elegido*continue*(continuar) en las que haya fallado la autenticación (para MasterCard, consulte aquí).

Para obtener más información sobre la garantía de pago condicional, consulte aquí.

6.1.3 Detalles de la transacción

En los detalles de transacción (página Finanzas), verá información adicional como, por ejemplo, el resultado del código de verificación de la tarjeta (si el cliente ha introducido el código CVC), el país de la tarjeta, el país de la dirección IP y la dirección IP.

El botón "Disputa" sobre la tabla con la información adicional le llevará a una página en la que podrá añadir determinados detalles de la transacción a sus listas negras con un clic. Esta opción le permite, por ejemplo, añadir el número de tarjeta usado para una transacción a su lista negra sin tener que conocer todo el número de la tarjeta.

También puede marcar la transacción como fraude o disputa comercial.

IMPORTANTE

Solo debe seleccionar "fraude real" como tipo si el cliente realmente ha cometido un fraude (por ejemplo, si un titular utiliza una tarjeta que no le pertenece).

Disputa:

6.1.4 Códigos de error

Cuando el sistema retiene una transacción siguiendo las normas establecidas en el módulo de detección de fraude, encontrará el motivo en el mensaje de error de la transacción. Con algunas excepciones, todos los códigos de error relacionados con la detección de fraudes empezarán por "300011", seguidos por dos dígitos más.

Puede encontrar más información sobre estados y códigos de error en su cuenta de Ogone. Basta con iniciar sesión y acceder a: Asistencia > Integración y manuales de usuario > Guías del usuario > Lista de estados de pago y códigos de error.

La siguiente lista no completa contiene algunos de los ejemplos más relevantes:

3 / 30001100 País del cliente no autorizado

3 / 30001120 Dirección IP en la lista negra del comerciante

3 / 30001130 BIN en la lista negra del comerciante

3 / 30001140 Tarjeta en la lista negra del comerciante

6.2 Parámetros de transacción complementarios

En sus solicitudes de posventa, redirecciones con respuesta, descargas de archivos y respuestas XML de DirectLink, se devolverán parámetros de transacción relativos a Puntuación.

La lista de parámetros complementarios se define a continuación.

Estos campos estarán vacíos si se ha producido un error de validación de formato para los detalles de la transacción.

Parámetro	Valor
IPCTY	País de origen de la dirección IP. Formato: Código ISO alfabético de 2 caracteres. Si este parámetro no está disponible, se devolverá "99" en la respuesta. Esta comprobación de la IP se basa en listas de IP obtenidas de forma externa, por lo que existe un ligero riesgo, ya que tenemos que fiarnos de la precisión de esta lista. La

Parámetro	Valor
	comprobación proporciona resultados positivos en el 94 % de los casos.
CCCTY	País de origen de la tarjeta de crédito. Solo está disponible para VISA, MasterCard, American Express y Diners Club. Este valor estará vacío para todos los demás métodos de pago/marcas. Formato: Código ISO alfabético de dos caracteres. Si este parámetro no está disponible, se devolverá "99" en la respuesta. Esta comprobación del país de la tarjeta de crédito se basa en listas obtenidas de forma externa, por lo que existe un ligero riesgo debido a que tenemos que fiarnos de la corrección de esta lista. La comprobación proporciona resultados positivos en el 94 % de los casos.
ECI	Indicador de comercio electrónico. Los posibles valores de ECI y su significado se definen a continuación: 1 Introducción manual 2 Pagos recurrentes 3 Pagos a plazos 5 Identificación del titular de la tarjeta correcta 6 El comerciante admite la identificación, pero no al titular de la tarjeta; se aplican las normas de garantía de pago condicional (véase aqui) 7 Comercio electrónico con cifrado SSL 9 Periódico tras primera transacción de comercio electrónico 12 El comerciante admite la identificación, pero no al titular de la tarjeta; se aplican las normas de garantía de pago condicional (véase here) (idem 6) 91 ¡¡¡Identificación del titular FALLIDA!!! (Se puede aplicar la garantía de pago condicional (véase aqui) Consulte con su entidad adquirente). 92 Sitio de autenticación del banco emisor no disponible de forma temporal, pero se ha continuado con la transacción
CVCCHECK	Resultado de la comprobación del código de verificación de la tarjeta. Valores posibles: KO El CVC se ha enviado, pero la entidad adquirente ha respondido negativamente a la comprobación del CVC. Es decir, el CVC es incorrecto. OK 1. 1. El CVC ha sido enviado y la entidad adquirente ha respondido positivamente a la comprobación del CVC, es decir, el CVC es correcto O 2. 2. La entidad adquirente envió un código de autorización pero no devolvió un resultado específico para la comprobación del CVC. NO Cualquier otro caso. Por ejemplo, no se ha transmitido el CVC; la entidad adquirente ha respondido que no era posible realizar la comprobación del CVC; la entidad adquirente rechaza la autorización pero no proporciona un resultado específico para la comprobación del CVC; etc.
AAVCHECK	Resultado de una verificación de dirección automática. Esta verificación no está disponible en la actualidad para American Express. Valores posibles: KO La dirección se ha enviado, pero la entidad adquirente ha respondido negativamente a la comprobación de dirección. Es decir, la dirección es incorrecta. OK 1. La dirección se ha enviado y la entidad adquirente ha respondido positivamente a la comprobación de dirección, es decir, la dirección es correcta O 2. La entidad adquirente envió un código de autorización pero no una respuesta específica para la comprobación de dirección. NO Cualquier otro caso. Por ejemplo, no se ha transmitido la dirección, la entidad adquirente ha respondido que no era posible realizar la comprobación de dirección;

Parámetro	Valor
	la entidad adquirente rechaza la autorización pero no proporciona un resultado específico para la comprobación de dirección, etc.
VC	Tarjeta virtual. Valores posibles: ECB: Para E Carte Bleue ICN: Para Internet City Number NO: Cualquier otro caso. Por ejemplo, la tarjeta no es una tarjeta virtual; la tarjeta es un tipo de tarjeta virtual no conocida para nosotros, etc.
IP	La dirección IP del cliente, según la haya detectado nuestro sistema en una integración de nivel 3 o haya sido proporcionada por el comerciante en una integración de nivel 2.

Puede encontrar más información acerca de estos campos en su cuenta de Ogone. Basta con iniciar sesión y acceder a: Asistencia > Integración > Manuales de usuario > Guías técnicas > Libro de parámetros.

7 Apéndice: CVC2 y AAV

7.1 CVC2

CVC2 es un procedimiento de autenticación establecido por las empresas de tarjetas de crédito para ayudar a evitar el uso fraudulento de tarjetas de crédito en transacciones de Internet. Este código se denomina de distinta forma dependiendo de la marca (CVC2 o código de validación de tarjeta para MasterCard, CVV2 o valor de verificación de tarjeta para VISA, CID o número de identificación de tarjeta para American Express). No obstante, el código se denomina generalmente "CVC". La funcionalidad del CVC2 es igual para todas las marcas.

El código de verificación es un código de autenticación asociado de forma única al número de tarjeta, aunque no forma parte de este. Dependiendo de la marca de la tarjeta, el código de verificación tendrá 3 o 4 dígitos en la parte delantera o posterior de la tarjeta, una fecha de inicio o una fecha de nacimiento. Para MasterCard y VISA, por ejemplo, hay un código de 3 dígitos en la parte posterior de la tarjeta sobre la banda de la firma, después del número de cuenta completo del cliente o después de los 4 últimos dígitos del número de cuenta del cliente.

Está estrictamente prohibido que los comerciantes y PSP almacenen los códigos CVC2 de los clientes en una base de datos. Cuando el titular de la tarjeta no está presente en persona, por ejemplo, para transacciones de "tarjeta no presente", y se le pide que introduzca su código CVC2 junto con el número de tarjeta de crédito, este código de verificación ayuda a confirmar que el cliente que realiza el pedido tiene la tarjeta real a mano y que la cuenta de la tarjeta es válida.

7.2 AAV

AAV es un procedimiento de autenticación disponible en algunos mercados para ayudar a evitar el uso fraudulento de tarjetas de crédito en transacciones de Internet. Dependiendo de la marca, este procedimiento de autenticación tendrá un nombre diferente (AVS o Servicio de verificación de dirección/ Sistema para VISA/MasterCard; AAV o Verificación de dirección automática para American Express). No obstante, la funcionalidad del AAV es igual para todas las marcas.

La comprobación de la dirección tiene lugar cuando la entidad adquirente solicita al emisor de la tarjeta comparar los componentes numéricos (número fijo y código postal) de la dirección (de facturación o entrega) del cliente que el comerciante nos envió con los de la dirección de facturación ofrecida por el cliente al emisor al solicitar la tarjeta.

Nota: Las simulaciones en las comprobaciones AAV/AVS no funcionan como se espera en un entorno de PRUEBA.