

Módulo de detección de fraude avanzado: Puntuación

v.4.4.7

Contenidos

1	¿Qué es el módulo de detección de fraude?	5
1.1	Ventajas	5
1.2	Acceso	5
1.3	Contenido	5
2	Activación y configuración de la detección de fraude	7
2.1	Grupos de países de tarjeta	7
2.2	Grupos de países de IP	7
2.3	Combinaciones de riesgo de país de IP/país de tarjeta	8
2.4	Límite de cantidad	8
2.5	Límites de uso	8
2.5.1	Utilización de la tarjeta	8
2.5.2	Utilización de la IP	9
2.5.3	Utilización del correo electrónico	9
2.6	Datos de riesgo	9
2.6.1	Códigos postales y direcciones de riesgo	10
2.6.2	Periodos de riesgo (fecha y hora del pedido)	11
2.6.3	Método de envío de riesgo	11
2.6.4	Detalles del método de envío de riesgo	12
2.6.5	Categorías de productos de riesgo	13
2.6.6	Plazo de entrega de riesgo	13
2.6.7	Submarcas de riesgo	14
2.6.8	Números de emisores de riesgo	14
2.7	Duplicar la configuración	14
3	3-D Secure	16
3.1	General	16
3.1.1	Solicitud de afiliación	16
3.1.2	Procesamiento de transacciones de 3-D Secure estándar	16
3.2	Opciones de configuración	17
3.2.1	Problema técnico	17
3.2.2	Servicio de identificación no disponible de forma temporal	17
3.2.3	Fallos de autenticación (solo MasterCard)	17
3.2.4	Activar/desactivar 3-D Secure	17

4	Configuración de listas negras, grises y blancas	18
4.1	Funcionalidades generales de las listas.....	18
4.1.1	Entradas	18
4.1.2	Comentarios	18
4.1.3	Motivo	18
4.1.4	Filtro	18
4.1.5	Descargas de listas	18
4.1.6	Advertencia por resultado en lista negra	19
4.2	Listas blancas	19
4.2.1	Lista blanca de direcciones IP	19
4.2.2	Lista blanca de identificadores únicos de clientes	19
4.2.3	Lista blanca de correo electrónico	19
4.3	Listas negras/listas grises.....	19
4.3.1	Número de tarjeta	20
4.3.2	BIN	20
4.3.3	Dirección IP	20
4.3.4	Dirección de correo electrónico	20
4.3.5	Nombre	20
4.3.6	Número de teléfono	21
4.3.7	Datos genéricos	21
5	Puntuación	22
6	Dispute	24
6.1	Añada los datos de transacción a una lista negra y blanca.....	24
7	Comentarios	27
7.1	Vista de transacciones en el área de administración.....	27
7.1.1	Criterios de selección avanzados	27
7.1.2	Detalles de la transacción	27
7.1.2.1	Disputa	27
7.1.2.2	Ver transacciones desde la misma dirección IP.....	28
7.1.2.3	Ver detalles de puntuación.....	28
7.1.3	Códigos de error	28
7.2	Parámetros de transacción complementarios.....	29
8	Apéndice: Comparación entre parámetros y comprobaciones/reglas	31

9	Apéndice: Datos adicionales a través de e-Terminal (MOTO).....	34
10	Apéndice: CVC2 y AAV.....	35
10.1	CVC2	35
10.2	AAV/AVS	35
10.3	Adaptación de la puntuación a partir del resultado AAV/AVS	35
11	Apéndice: Consejos para informar sobre fraudes.....	37
12	Apéndice: Configuración de grupos y uso compartido de listas negras.....	38
13	Apéndice: Mecanismo de anulación.....	39

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 proporciona 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.

A diferencia del módulo de detección de fraude básico, en el módulo de detección de fraude avanzado, el comerciante configura el comportamiento real de las listas negras, blancas y grises, junto con reglas y límites en la lista de puntuación.

El módulo de detección de fraude básico y el módulo de detección de fraude avanzado son compatibles entre sí, lo que significa que una actualización del módulo avanzado no afecta al comportamiento de bloqueo que ha configurado en el módulo de detección de fraude básico. Por ejemplo:

- Todas las entradas de las listas negras seguirán presentes y los criterios correspondientes en la página de la puntuación estarán configurados como "bloqueo".
- Los países de tarjeta de crédito y de IP que ha configurado para que no se acepten pagos se considerarán como países de riesgo elevado y se configurarán como "bloqueo" en la página de la puntuación.
- Las entradas de lista blanca de direcciones IP seguirán presentes y se establecerá el comportamiento correspondiente (confiar) en la página de la puntuación.

Naturalmente, una vez que se haya actualizado al módulo de detección de fraude avanzado, podrá beneficiarse de funciones y matices adicionales en los criterios que se utilizan para evaluar el riesgo de las transacciones.

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
- Asignar una puntuación a riesgos específicos
- Protegerse frente a riesgos específicos del país
- Definir y aplicar políticas de seguridad totalmente personalizadas
- Beneficiarse de la garantía de pago condicional (consulte [aquí](#)) conforme a sus políticas individuales de entidad adquirente (3-D Secure)

1.2 Acceso

Puede acceder al Módulo de detección de fraude a través de "Avanzado" > "Detección del fraude" en el menú de su 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
- Listas negras/listas grises/listas blancas

Importante

Los criterios de VISA/MasterCard descritos en esta documentación no están necesariamente disponibles para todos los métodos de pago.

La disponibilidad de la configuración multicriterio depende del método de pago. Para algunos métodos de pago, la configuración está limitada.

Le recomendamos que consulte la configuración específica 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 la detección de fraude" de su pantalla de configuración de detección de fraude.

2 Activación y configuración de la detección de fraude

En la tabla "Activación y configuración de la detección de fraude" verá la distinción entre tarjetas de crédito y otros métodos de pago. Ahora vamos a examinar con mayor detalle la configuración de las opciones de detección de fraude de las 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. Entrará en la página de la puntuación de este método de pago con enlaces a las páginas de configuración para los diferentes límites, reglas y listas.

El comportamiento real de estas reglas (es decir, si realmente bloquean las transacciones) depende de los ajustes en la página "Puntuación" (Scoring).

2.1 Grupos de países de tarjeta

Todos los países de la tarjeta se aceptan de forma predeterminada. Aquí, el término "país de la tarjeta" se refiere al país donde se emitió la tarjeta. Nuestro sistema puede identificar el país de tarjeta a partir del código BIN de la tarjeta, es decir, los primeros 6 dígitos de un número de tarjeta de crédito. Un código BIN está vinculado a un banco concreto de un país específico.

Puede establecer un riesgo determinado por país de tarjeta. Hay 3 posibles categorías para clasificar un país de tarjeta:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los países de tarjeta de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los países de tarjeta de riesgo medio pueden causar un aumento en la puntuación; y los países de tarjeta de riesgo bajo no se tendrán en cuenta para la puntuación.

Nota

- Disponible solo para VISA, MasterCard, American Express y Diners Club

2.2 Grupos de países de 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).

Como con los países de tarjeta, puede definir un determinado riesgo por país de IP. Hay 3 posibles categorías para clasificar un país de IP:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los países de IP de riesgo elevado pueden causar el bloqueo de transacciones o la suma a la puntuación; los países de IP de riesgo medio pueden sumar a la puntuación; y los países de IP de riesgo bajo no se tendrán en cuenta para la puntuación.

Además de esos países de IP, también hay proxies anónimos. Los proxies anónimos son proveedores de acceso a Internet que permiten a los usuarios de Internet ocultar sus direcciones IP. Le aconsejamos que bloquee transacciones que se originen en proxies anónimos., en la página de la puntuación.

Importante

"Asia Pacific Network" (Red de Asia Pacífico), "European Network" (Red europea) y "Satellite Provider" (Proveedor de satélite) hacen referencia a las direcciones IP cuyo país de origen es dudoso.

"European Network" (Red europea), por ejemplo, significa que el país de IP exacto es incierto pero

pertenece a Europa. La aceptación de "European Network" (Red europea) como país de dirección IP no significa que esté aceptando pagos de todos los países de Europa, significa que acepta pagos de direcciones IP gestionadas por instituciones europeas (por ejemplo, un proveedor de Internet que opera en más de un país europeo, la Comisión Europea, etc.).

La mayoría de las veces, el país de dirección IP será idéntico al país de entrega. Las regiones/los países de entrega siguientes se consideran de riesgo en el mundo de la entidad adquirente: Europa del Este, Asia, Indonesia, África y Estados Unidos. No obstante, si hace muchos negocios en estas regiones/estos países o si cuenta con un procedimiento específico de entrega o de pedido para comprobar la identidad del cliente, no necesita establecer un nivel de riesgo elevado para esas regiones/esos países.

2.3 Combinaciones de riesgo de país de IP/país de tarjeta

Todas las combinaciones de países de IP/de tarjeta se aceptan de forma predeterminada.

Para configurar una combinación de país de IP/país de tarjeta, en las listas desplegables seleccione el país de IP y el país de tarjeta que desea combinar.

Del mismo modo que con los países de tarjeta y los países de IP, puede definir un riesgo determinado para la combinación de país de IP/país de tarjeta. Hay 3 posibles categorías para clasificar las combinaciones de países de IP/de tarjeta:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Las combinaciones de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; las combinaciones de riesgo medio pueden causar un aumento en la puntuación; y las combinaciones de riesgo bajo no se tendrán en cuenta para la puntuación.

Nota

- Disponible solo para VISA, MasterCard, American Express y Diners Club

2.4 Límite de cantidad

Para limitar la cantidad por transacción, especifique una cantidad mínima y otra máxima. 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.

2.5 Límites de uso

2.5.1 Utilización de la tarjeta

Puede establecer la opción "Utilización máxima por tarjeta y por periodo" basándose en la cantidad total de transacciones por tarjeta y el número de transacciones por tarjeta.

Debe configurar este límite basándose en su negocio/productos. Por ejemplo, si vende un producto que los clientes no suelen comprar más de una vez a la semana, puede limitar el uso de la tarjeta a una vez por semana.

Ejemplo

Si no desea aceptar más de dos transacciones el mismo día desde una determinada tarjeta de crédito y no desea aceptar más de 250 EUR en esa tarjeta de crédito en un mismo día, puede configurar las opciones:

- *Utilización máxima por tarjeta y por periodo: 1 día(s).*
- *Cantidad total de transacciones por tarjeta, umbral alto: 250 EUR*
- *Número de transacciones por tarjeta, umbral alto: 2*

En un uso avanzado de esta regla, también puede establecer un umbral bajo y otro alto que le permitan definir dos puntuaciones diferentes. Con un umbral bajo solo puede incrementar la puntuación de riesgo; con un umbral alto también puede incrementar la puntuación de riesgo o bloquear directamente.

El límite "Utilización máxima por tarjeta y por periodo" solo se aplica a tarjetas utilizadas en transacciones que dan lugar a uno de los estados siguientes: 9, 91, 92, 5, 51, 52.

2.5.2 Utilización de la IP

Puede establecer la opción "Número de transacciones por tarjeta, umbral alto" basándose en el número de transacciones correctas por dirección IP y el número total de transacciones (aceptadas y rechazadas) por dirección IP.

Los defraudadores suelen trabajar con una lista de tarjetas de crédito robadas, que prueban una a una. El resultado es que las transacciones con diferentes tarjetas se enviarán desde la misma dirección IP. Para poder detectar casos así, puede limitar el número de transacciones (aceptadas y rechazadas) por dirección IP. Cuando se le informa de un "uso excesivo", también es importante examinar el historial de direcciones IP. De este modo, puede detener la entrega de sus mercancías cuando observa demasiadas transacciones desde una dirección IP con tarjetas diferentes en un periodo de tiempo determinado.

Ejemplo

Si no desea aceptar más de una transacción correcta desde la misma dirección IP en un plazo de 3 días, y no quiere aceptar más de 3 intentos desde esa dirección IP en ese periodo, puede configurar:

- *Utilización máxima por dirección IP y por periodo 3 día(s).*
- *Número de transacciones correctas por dirección IP, umbral alto: 1.*
- *Número de transacciones (aceptadas o rechazadas) por cada dirección IP, umbral alto: 3.*

En un uso avanzado de esta regla, también puede establecer un umbral bajo y otro alto que le permitan definir dos puntuaciones diferentes. Con un umbral bajo solo puede incrementar la puntuación de riesgo; con un umbral alto también puede incrementar la puntuación de riesgo o bloquear directamente.

El límite de utilización máxima por dirección IP, por periodo solo se aplica a direcciones IP utilizadas en transacciones que dan lugar a uno de los estados siguientes:

- Transacciones con éxito: 9, 91, 92, 5, 50, 51, 52
- Todas las demás transacciones: 9, 91, 92, 5, 50, 51, 52, 2

2.5.3 Utilización del correo electrónico

Puede definir un valor para la opción "Utilización máxima por dirección de correo electrónico y por periodo"; es decir, puede decidir el número de veces que puede utilizarse una dirección de correo electrónico específica en un periodo determinado.

También puede definir un umbral alto y un umbral bajo para la utilización del correo electrónico, que le permitirá establecer dos puntuaciones diferentes. Con un umbral bajo solo puede incrementar la puntuación de riesgo; con un umbral alto también puede incrementar la puntuación de riesgo o bloquear directamente.

El valor de "Utilización máxima por dirección de correo electrónico y por periodo" se aplica a transacciones con todos los estados.

El límite de utilización máxima por dirección dirección de correo electrónico, por periodo solo se aplica a direcciones direcciones de correo electrónico utilizadas en transacciones que dan lugar a uno de los estados siguientes: 9, 91, 92, 5, 50, 51, 52, 2.

2.6 Datos de riesgo

2.6.1 Códigos postales y direcciones de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración de los códigos postales y las direcciones de riesgo es válida para todos los métodos de pago. Tenga en cuenta que las direcciones incluyen las direcciones de facturación y de envío.

Puede establecer un riesgo determinado para cada código postal y dirección. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los códigos postales o las direcciones de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los códigos postales o las direcciones de riesgo medio pueden causar un aumento en la puntuación; y los códigos postales o las direcciones de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar su lista, seleccione el país, especifique el código postal y la calle, haga clic en el botón "Agregar" y defina el riesgo. Haga clic en "Enviar" para terminar. Para que la regla se evalúe, también será necesario incluir el código de país.

Para utilizar esta funcionalidad, asegúrese de enviar los parámetros siguientes para direcciones de facturación y de envío con los valores asociados en la solicitud de pedido desde su sitio web:

Dirección de facturación

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
OWNERCTY	AN (2)	País del cliente	UK
OWNERZIP	AN (10)	Código postal del cliente	75420
OWNERADDRESS	AN (35)	Primera línea de la dirección del cliente	Baker Street 221B
OWNERADDRESS2	AN (35)	Segunda línea de la dirección del cliente	segunda planta

Q

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
ECOM_BILLTO_POSTAL_COUNTRYCODE	AN (2)	País de facturación	UK
ECOM_BILLTO_POSTAL_POSTALCODE	AN (10)	Código postal de facturación	75420
ECOM_BILLTO_POSTAL_STREET_LINE1	AN (35)	Primera línea de dirección de facturación	Baker Street 221B
ECOM_BILLTO_POSTAL_STREET_LINE2	AN (35)	Segunda línea de dirección de facturación	segunda planta

Dirección de envío

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
ECOM_SHIPTO_POSTAL_COUNTRYCODE	AN (2)	Código de país de envío	UK
ECOM_SHIPTO_POSTAL_POSTALCODE	AN (10)	Código postal de envío	75420
ECOM_SHIPTO_POSTAL_STREET_LINE1	AN (35)	Primera línea de dirección de envío	Baker Street 221B
ECOM_SHIPTO_POSTAL_STREET_LINE2	AN (35)	Segunda línea de dirección de envío	segunda planta

2.6.2 Periodos de riesgo (fecha y hora del pedido)

Importante

- Solo necesita configurar esta página una vez. La configuración de los periodos de riesgo es válida para todos los métodos de pago.
- El huso horario que se utiliza es CET (hora central europea).

Puede establecer un riesgo determinado por periodo de pedido. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los periodos de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los periodos de riesgo medio pueden causar un aumento en la puntuación; y los periodos de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar la tabla, seleccione el riesgo en la parte inferior de la tabla, marque las casillas a las que desea atribuir ese riesgo y haga clic en el botón "Aplicar".

2.6.3 Método de envío de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración de los métodos de envío de riesgo es válida para todos los métodos de pago.

Puede establecer un riesgo determinado para cada método de envío. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los métodos de envío de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los métodos de envío de riesgo medio pueden causar un aumento en la puntuación; y los métodos de envío de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar su lista, especifique el método de envío, defina el riesgo y haga clic en el botón "Agregar". Haga clic en el botón "Enviar" para terminar.

Para utilizar esta funcionalidad, asegúrese de enviar el parámetro siguiente con el valor asociado en la solicitud de pedido desde su sitio web:

Parámetro de entrada relacionado	de Formato	Explicación	Ejemplo
ECOM_SHIPMETHODTYPE	Valor entero: 1-9	Método de entrega Puede definir y enviar un valor para cada método de envío (entrega).	1: Seleccione un comerciante 2: Punto de recogida (oficina de correos, punto de la empresa Kiala...) 3: Recogida en el aeropuerto, estación de trenes o agencia de viajes 4: Transportista (DHL, UPS...) 5: Descargar 6: Portador de bajo costo 7: Recoger en los armarios de parcelas 8: Militar 9: Electrónica 91: Definido por el comerciante 1 92: Definido por el comerciante 2 93: Definido por el comerciante 3 94: Definido por el comerciante 4 95: Definido por el comerciante 5 96: Definido por el comerciante 6 97: Definido por el comerciante 7 98: Definido por el comerciante 8 99: Definido por el comerciante 9

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

2.6.4 Detalles del método de envío de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración de los detalles del método de envío de riesgo es válida para todos los métodos de pago.

Puede establecer un riesgo determinado por entrada. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los detalles del método de envío de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los detalles del método de envío de riesgo medio pueden causar un aumento en la puntuación; y los detalles del método de envío de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar su lista, seleccione el valor Detalles de método de envío de la lista desplegable, defina el riesgo y haga clic en el botón "Agregar". Haga clic en el botón "Enviar" para terminar.

Para utilizar esta funcionalidad, asegúrese de enviar el parámetro siguiente con el valor asociado en la solicitud de pedido desde su sitio web:

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
ECOM_SHIPMETHODDETAILS	Texto libre (máx.	Identificación del punto de recogida	Oficina de correos KR124

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
	50)		

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

2.6.5 Categorías de productos de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración de las categorías de productos de riesgo es válida para todos los métodos de pago. Las Categorías de productos de riesgo son sólo aplicables a e-Commerce y DirectLink.

Puede establecer un riesgo determinado para cada categoría de productos. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Las categorías de productos de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; las categorías de productos de riesgo medio pueden causar un aumento en la puntuación; y las categorías de productos de riesgo bajo no se tendrán en cuenta para la puntuación.

Para utilizar esta funcionalidad, solo debe enviar el parámetro ITEMFDMPRODUCTCATEGx con sus valores asociados.

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
ITEMFDMPRODUCTCATEGx	Texto libre (máximo 50)	Categoría de producto	Viajar Comida Deportes

Nota:

Sustituya la "x" con un número para enviar varios elementos: ITEMFDMPRODUCTCATEG1, ITEMFDMPRODUCTCATEG2, etc.

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

2.6.6 Plazo de entrega de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración del plazo de entrega de riesgo es válida para todos los métodos de pago.

Puede establecer un riesgo determinado para cada plazo de entrega (en horas). Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los plazos de entrega de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los plazos de entrega de riesgo medio pueden causar un aumento en la puntuación; y los plazos de entrega de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar su lista, especifique la categoría de productos, defina el riesgo y haga clic en el botón

"Agregar". Haga clic en el botón "Enviar" para terminar.

Para utilizar esta funcionalidad, asegúrese de enviar el parámetro siguiente con el valor asociado en la solicitud de pedido desde su sitio web:

Parámetro de entrada relacionado	Formato	Explicación	Ejemplo
ECOM_SHIPMETHODSPEED	Valor entero	El número de horas necesarias para la entrega	24

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

2.6.7 Submarcas de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración de las submarcas de riesgo es válida para todos los métodos de pago.

Puede establecer un riesgo determinado por submarca. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Las submarcas de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; las submarcas de riesgo medio pueden causar un aumento en la puntuación; y las submarcas de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar su lista, especifique la submarca, defina el riesgo y haga clic en el botón "Agregar". Haga clic en el botón "Enviar" para terminar.

2.6.8 Números de emisores de riesgo

Importante

Solo necesita configurar esta página una vez. La configuración de los números de emisores de riesgo es válida para todos los métodos de pago.

Puede establecer un riesgo determinado por número. Hay 3 niveles posibles:

- Riesgo elevado
- Riesgo medio
- Riesgo bajo

Los números de emisor de riesgo elevado pueden causar el bloqueo de transacciones o un aumento en la puntuación; los números de emisor de riesgo medio pueden causar un aumento en la puntuación; y los números de emisor de riesgo bajo no se tendrán en cuenta para la puntuación.

Para configurar su lista, especifique el número del emisor, defina el riesgo y haga clic en el botón "Agregar". Haga clic en el botón "Enviar" para terminar.

2.7 Duplicar la configuración

Junto a cada método de pago en la descripción general "Activación y configuración de la detección de fraude", verá un botón "Duplicar". Este botón permite copiar los ajustes configurados para un método de pago en uno o más de los otros métodos de pago en la lista. En consecuencia, cuando tiene varios métodos de pago en su cuenta, no tiene que llevar a cabo la misma configuración varias veces.

Importante

Si ya ha configurado la detección de fraude para un método de pago en el que desea copiar la configuración de otro método de pago, los ajustes originales se sobrescribirán con los ajustes copiados.

Los ajustes siguientes pueden copiarse, en función de si el método de pago previsto los admite:

- Ponderaciones de los criterios FDMA
- Configuración de límites de uso
- Lista de grupos de países de IP
- Lista de grupos de países de tarjeta
- Ajustes de cantidad mín. y máx.
- Ajuste de tiempo hasta la salida
- Ajuste de plazo de entrega
- Cantidad de países diferentes
- Ajustes de Fraud Expert

Ejemplo

Whenever you copy settings from one payment method to another, the other payment method existing configuration will be erased and replaced. No undo possible.

Features	American Express	Bancontact/Mister Cash	Direct Debits DE	Direct Debits NL	MasterCard	JCB	PAYPAL
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FDMA criteria weights	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Usage limits settings	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP country groups list	n.c.						
Card country groups list	<input type="checkbox"/>	-	-	-	<input checked="" type="checkbox"/>	-	-
Min max amount settings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Time to departure settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Time to delivery settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Number of different countries	n.c.						
Fraud Expert settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="SUBMIT"/>							
<input type="button" value="CLOSE WINDOW"/>							

3 3-D Secure

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

Al ofrecer 3-D Secure, el comerciante se beneficia de una garantía de pago condicional (consulte [aquí](#)) que se describe en el contrato de 3-D Secure con su entidad adquirente. Según estas condiciones, la cuenta de un comerciante ya no recibe cargos por disputas basadas en la "no identificación del titular". (Esto no se aplica a disputas sobre otros asuntos).

Como mínimo, 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](#)

Las reglas de bloqueo y revisión se pueden anular cuando los clientes se identifican correctamente a través de 3-D Secure.

Para obtener información adicional acerca del mecanismo de anulación, consulte el Apéndice: Mecanismo de anulación.

3.1 General



3.1.1 Solicitud de afiliación

Si en su cuenta no se ha activado 3-D Secure, verá el botón "Solicitud de 3-D Secure" en la tabla "3-D Secure".

Si hace clic en este botón "Solicitud de 3-D Secure", 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 ella 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.

3D-Secure				
About Verified By Visa and SecureCode (3D-Secure)				
Credit card	Acquirer	Card status	3DS activation date	3DS status
 MasterCard	Test MasterCard acquirer	Active	-	REQUEST 3DS
 VISA	Test VISA acquirer	Active	-	REQUEST 3DS

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, es decir, 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 redirige al comprador 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. Ogone 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 entre *continuar* o *interrumpir* la transacción 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 (consulte [aquí](#)).

3.2.2 Servicio de identificación no disponible de forma temporal

Si el servicio de identificación del titular está temporalmente no disponible, el comerciante puede elegir *continuar* o *interrumpir* la transacción.

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 recomiendan continuar con el proceso (opción *continuar*). En este caso, el comerciante no se beneficiará de la garantía de pago condicional (consulte [aquí](#)).

3.2.3 Fallos de autenticación (solo MasterCard)

El comerciante puede elegir entre *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 (consulte [aquí](#)).

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.

Advertencia

Si 3-D Secure está deshabilitado, el comerciante no se beneficiará de la garantía de pago condicional (consulte [aquí](#)).

4 Configuración de listas negras, grises y blancas

En el módulo de detección de fraude avanzado, puede generar sus propias listas negras y grises para tarjetas de crédito, basándose en códigos BIN, números de tarjeta de crédito, direcciones de correo electrónico, números de teléfono, nombres, datos genéricos y direcciones IP desde los cuales no desea o puede no desear que se acepten transacciones. También hay tres listas blancas, basadas en direcciones IP, un identificador único de cliente, y un correo electrónico de cliente.

El comportamiento real de estas listas (es decir, si bloquean o no) depende de los ajustes en la página "Puntuación".

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

4.1 Funcionalidades generales de las listas

4.1.1 Entradas

En el módulo de detección de fraude avanzado, no hay límite en el número de entradas en las listas. Puede introducir hasta 1.000 elementos a la vez mediante el cuadro de texto "Envío".

Siempre puede eliminar entradas de sus listas marcando las casillas de la columna "Eliminar" y haciendo clic en el botón "Enviar".

4.1.2 Comentarios

Puede añadir un comentario a una entrada de una lista negra, gris o blanca.

Puede introducirlo en el momento del envío especificando el comentario en el campo "Comentario"). Todos los elementos que haya especificado en ese envío tendrán el mismo comentario.

También puede añadir o borrar un comentario haciendo clic en el enlace "..." en la columna de comentarios.

4.1.3 Motivo

Para cada entrada de la lista negra o la lista gris puede seleccionar el motivo por el que desea introducir datos: fraude real o disputa comercial.

Importante

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

4.1.4 Filtro

Puede filtrar los datos de las listas mediante el botón "Filtro" de la parte superior de la tabla. Puede filtrar por fecha y listar el contenido.

Para quitar el filtro, haga clic en el botón "Eliminar".

4.1.5 Descargas de listas

Para descargar el contenido de la lista en una hoja de cálculo (por ejemplo, un archivo de Excel), haga clic en el botón "Descargar lista" de la parte superior de la tabla.

Si hace clic en el botón "Descargar lista" cuando haya aplicado un filtro, se descargará el contenido filtrado.

4.1.6 Advertencia por resultado en lista negra

En las listas negras, puede habilitar un botón de selección para enviar una advertencia por correo electrónico cuando haya un resultado en lista negra. El correo electrónico con la advertencia se enviará a las direcciones configuradas en "Direcciones de correo electrónico para los correos electrónicos relacionados con la transacción" de la página "Información técnica" de su cuenta.

Importante

Solo necesita habilitar/deshabilitar esta opción una vez. La configuración de esta opción se aplica a todas las listas negras.

4.2 Listas blancas

Listas blancas : contienen datos para clientes privilegiados y datos que se utilizan para anular otras reglas (en función de la configuración de la puntuación del comerciante).

4.2.1 Lista blanca de direcciones IP

Puede especificar las direcciones IP de los clientes desde las que desea recibir pedidos en la lista de direcciones IP de confianza. Si una dirección IP única de cliente está en esta lista blanca, anulará todas las reglas de bloqueo y de revisión relacionadas con la IP (en función de la configuración de la puntuación del comerciante). Para obtener información adicional acerca del mecanismo de anulación, consulte el [Apéndice: Mecanismo de anulación](#).

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

Puede especificar rangos de direcciones IP, en el formato "a.b.c-d.0-255", "a.b.c-d.*" o "a.b.c.d-e".

4.2.2 Lista blanca de identificadores únicos de clientes

El identificador único de cliente (CUI) es un identificador asignado al cliente por el comerciante. Puede ser un nombre, un número de cliente, una dirección de correo electrónico, etc. Si el comerciante desea utilizarlo, debe enviarnos el CUI en un campo adicional llamado "CUID" (alfanumérico, máx. 50 caracteres).

Si un CUI único de cliente está en esta lista blanca, anulará casi todas las demás reglas de bloqueo y de revisión (en función de la configuración de la puntuación del comerciante). Para obtener información adicional acerca del mecanismo de anulación, consulte el [Apéndice: Mecanismo de anulación](#).

4.2.3 Lista blanca de correo electrónico

Puede incluir en la lista blanca el correo electrónico del cliente simplemente añadiendo el correo electrónico a la lista blanca. Para que nuestro sistema pueda comprobar la dirección de correo electrónico del cliente, también debe enviar la dirección de correo electrónico en los detalles del pedido. Si ya lo ha hecho, la comprobación se realizará automáticamente.

Si un correo electrónico de cliente está en esta lista blanca, anulará casi todas las demás reglas de bloqueo y de revisión (en función de la configuración de la puntuación del comerciante). Para obtener información adicional acerca del mecanismo de anulación, consulte el [Apéndice: Mecanismo de anulación](#).

4.3 Listas negras/listas grises

La lista negra le permite (en función de su configuración de reglas) bloquear transacciones, forzar revisión de transacciones y añadir puntuación de riesgo a las transacciones. La lista gris le permite (en función de su configuración de reglas) forzar revisión de transacciones y añadir puntuación de riesgo a las transacciones.

Ejemplo. ha tenido problemas con transacciones que se originan en una dirección IP específica, pero no está seguro de si esta dirección IP es una dirección IP dedicada que pertenece a una persona. La dirección IP también puede representar a toda una compañía o todo un edificio, o el proveedor puede atribuirle a otra persona en el futuro.

En ese caso, no deseará poner esa dirección IP en la lista negra de direcciones IP directamente, porque no desea perjudicar/bloquear a otros clientes potenciales. Puede poner la dirección IP en la lista gris de

direcciones IP hasta que esté seguro sobre si debe moverla a la lista negra de direcciones IP o eliminarla de la lista gris.

Para mover los datos de la lista gris a la lista negra, marque las casillas de la columna "Mover a lista negra" en la lista gris y haga clic en "Enviar".

4.3.1 Número de tarjeta

En su lista negra/lista gris de tarjetas de crédito, debe especificar el número completo de estas.

En la lista negra de tarjetas puede habilitar un botón de selección para que se incluyan en la lista gris las direcciones IP de transacciones con una coincidencia en la lista negra de tarjetas.

Si ha activado los métodos de pago de domiciliaciones bancarias NL, DE o AT en su cuenta, la lista negra/lista gris de tarjetas también se duplicará como una lista negra/lista gris de cuentas para introducir números de cuenta.

4.3.2 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, con tan solo añadir el código BIN.

4.3.3 Dirección IP

En la lista negra o en la lista gris 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.

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".

El límite de utilización máxima por dirección IP, por periodo solo se aplica a direcciones IP utilizadas en transacciones que dan lugar a uno de los estados siguientes:

- Transacciones con éxito: 9, 91, 92, 5, 50, 51, 52
- Todas las demás transacciones: 9, 91, 92, 5, 50, 51, 52, 2

4.3.4 Dirección de correo electrónico

La dirección de correo electrónico puede ser una dirección fija o toda una gama de direcciones (dominio) que utilizan un asterisco ("*") antes del signo "@". La dirección de correo electrónico especificada por el comerciante aparecerá en la columna "Correo electrónico". Basándose en esta dirección de correo electrónico, nuestro sistema generará una "Coincidencia parcial".

Para que nuestro sistema pueda comprobar la dirección de correo electrónico del cliente, el comerciante también debe enviar la dirección de correo electrónico en los detalles del pedido.

El límite de utilización máxima por dirección dirección de correo electrónico, por periodo solo se aplica a direcciones direcciones de correo electrónico utilizadas en transacciones que dan lugar a uno de los estados siguientes: 9, 91, 92, 5, 50, 51, 52, 2.

4.3.5 Nombre

El comerciante puede especificar nombres de clientes en la lista negra o en la lista gris. El nombre especificado por el comerciante aparecerá en la columna "Nombre". Basándose en ese nombre, nuestro sistema generará otras dos versiones del nombre: el "Nombre limpio" y la "Coincidencia parcial".

Para que nuestro sistema pueda comprobar el comerciante nombre del titular de tarjeta, nombre de envío y nombre de facturación.

4.3.6 Número de teléfono

El comerciante puede especificar el número de teléfono de clientes en la lista negra o en la lista gris. El número de teléfono especificado por el comerciante aparecerá en la columna "Número de teléfono". Basándose en ese número de teléfono, nuestro sistema generará otras dos versiones: el "Número neto" y la "Coincidencia parcial".

Para que nuestro sistema pueda comprobar el número de teléfono del cliente, el comerciante también debe enviar el número de teléfono en los detalles del pedido.

4.3.7 Datos genéricos

La lista negra y la lista gris de datos genéricos permiten al comerciante tener una lista totalmente personalizada en la que puede agregar los datos que desea que se tengan en cuenta para la puntuación de fraude de las transacciones. Los datos deben ser alfanuméricos y no deben tener más de 50 caracteres.

Para que nuestro sistema pueda comprobar los datos genéricos, el comerciante también debe enviar los datos a lo largo del campo "GENERIC_BL" en el pedido (alfanumérico, máx. 50 caracteres).

5 Puntuación

Encontrará la lista de criterios en la página de configuración de la puntuación, que contiene todos los criterios que pueden establecerse en el módulo de detección de fraude avanzado.

Importante

En contraste con el módulo de detección de fraude básico, en el que el comportamiento de bloqueo se establece en listas negras/listas blancas, reglas de bloqueo, etc., el comerciante configura el comportamiento real de las listas negras/listas grises/listas blancas, junto con los límites y las reglas, en la lista de puntuación.

Por criterio, puede configurarse una de las acciones siguientes:

- *Incremento de la ponderación del riesgo.* cuando los criterios incrementan el riesgo, puede sumarse una ponderación de 0 a 5.
- *Reducción de la ponderación del riesgo.* cuando los criterios reducen el riesgo, puede restarse una ponderación de 0 a 5, 10 o 20.
- *Forzar análisis.* para todos los criterios, es posible forzar una revisión de la transacción. "Force review" (Forzar revisión) también supone un valor de +3 en la puntuación, además de las otras reglas. La transacción se pondrá de color naranja si la puntuación está en verde o naranja, o permanecerá de color rojo si la puntuación total está por encima del umbral rojo y si se cumplen otros criterios de bloqueo.
- *Bloquear transacción.* para determinados criterios, también existe la opción de bloquear la transacción. En consecuencia, las reglas establecidas por el comerciante bloquearán la transacción o influirán en la puntuación global de la transacción. La puntuación final es la ponderación total de los diversos criterios. Cuanto más alta es la puntuación, mayor es el riesgo.
- Anulación de bloqueo y revisión

El comerciante puede establecer un valor de puntuación determinado como límite superior para la puntuación intermedia, es decir, antes de que se autorice la transacción. Ese valor indica que todas las transacciones con esa puntuación o superior deben bloquearse antes del procedimiento de autorización. La comprobación de AAV y CVC se produce después de que enviemos la transacción a la entidad adquirente (es decir, después de la autorización), de modo que esos valores de puntuación no se tendrán en cuenta para ese límite de puntuación intermedia.

La suma de los valores antes de la autorización y los valores de las puntuaciones AAV y CVC dan la puntuación final y general. El comerciante puede decidir las categorías de puntuación basándose en este valor de puntuación final, vinculado a colores: verde (riesgo bajo), naranja (riesgo medio) y rojo (transacción bloqueada). Estos colores se mostrarán en la respuesta al comerciante.

Si la transacción se bloquea en función de los ajustes, estableceremos su estado en "Autorización rechazada".

Condiciones: como determinada información se origina en listados proporcionados externamente, confiamos en su precisión pero no podemos garantizar un resultado 100 % correcto.

A continuación se indica una selección (no exhaustiva) de criterios de puntuación:

- *3-D Secure.* cuando el titular de la tarjeta tiene autenticación 3-D Secure completa (identificación correcta) y el titular de la tarjeta no está registrado. 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. En consecuencia, incluso si no desea recibir pagos de determinados países de tarjeta o IP a causa de un elevado riesgo de fraude, podrá seguir permitiendo las transacciones con tarjetas de crédito 3-D Secure de esos países, porque el riesgo es muy inferior.
- *Proxies anónimos.* 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.
- *Correo electrónico gratuito.* los defraudadores utilizan casi exclusivamente cuentas de correo electrónico falsas creadas en servicios de correo electrónico gratuito. Nuestro sistema comprobará (basándose en listados proporcionados externamente) si la dirección de correo electrónico del cliente es gratuita o no. El comerciante puede decidir añadir una puntuación de riesgo a las transacciones en las que la dirección de correo electrónico del cliente es de una cuenta gratuita. Para que nuestro sistema pueda comprobar la dirección de correo electrónico del cliente, el comerciante también debe enviar la dirección de correo electrónico en los detalles del pedido.
- *Cantidad de países diferentes.* Número de países: El comerciante puede indicar el número de países permitido y puede definir la acción de puntuación si el número supera el límite establecido en función de lo

siguiente:

- País de la tarjeta de crédito (para VISA, MasterCard, American Express y Diners Club)
- País de la IP (si está disponible)
- Direcciones de facturación y envío (si se han enviado)
- Aeropuertos de salida (si procede y se han enviado)
- *El país de IP es diferente del país de tarjeta* (solo para VISA, MasterCard, American Express y Diners Club): al establecer este parámetro en "Block transaction" (Bloquear transacción), 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 no se realiza si la dirección IP procede de un proxy anónimo, la red Asia Pacífico, la red europea o un proveedor por satélite.
- *La dirección de facturación es diferente de la dirección de entrega*: indica si la dirección de facturación se considera diferente de la dirección de entrega, y se basa en el valor del campo adicional "addMatch" que el comerciante nos envía en los detalles del pedido. Si el valor es "1", las direcciones de facturación y de entrega se considerarán idénticas. Si el valor es "0", se considerarán diferentes entre sí.
- *Limite de cantidad, limites de utilización*
- *Identificación de lista blanca de CUI*
- *Lista blanca de correo electrónico*
- *Direcciones IP de confianza*
- *Tarjeta/BIN/dirección IP/correo electrónico/teléfono/nombre del titular de la tarjeta/datos genéricos en las listas negra y gris*
- *Países de tarjeta de riesgo elevado y medio, países de IP de riesgo elevado y medio, códigos postales de riesgo elevado y medio, fecha y hora del pedido de riesgo elevado y medio*

Importante

Recomendamos encarecidamente establecer los criterios de puntuación siguientes en "Bloquear transacción" en la página de la puntuación:

- Tarjeta en lista negra
- Proxy anónimo (en país de IP)

6 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 Fraud Expert y mejora su rendimiento.

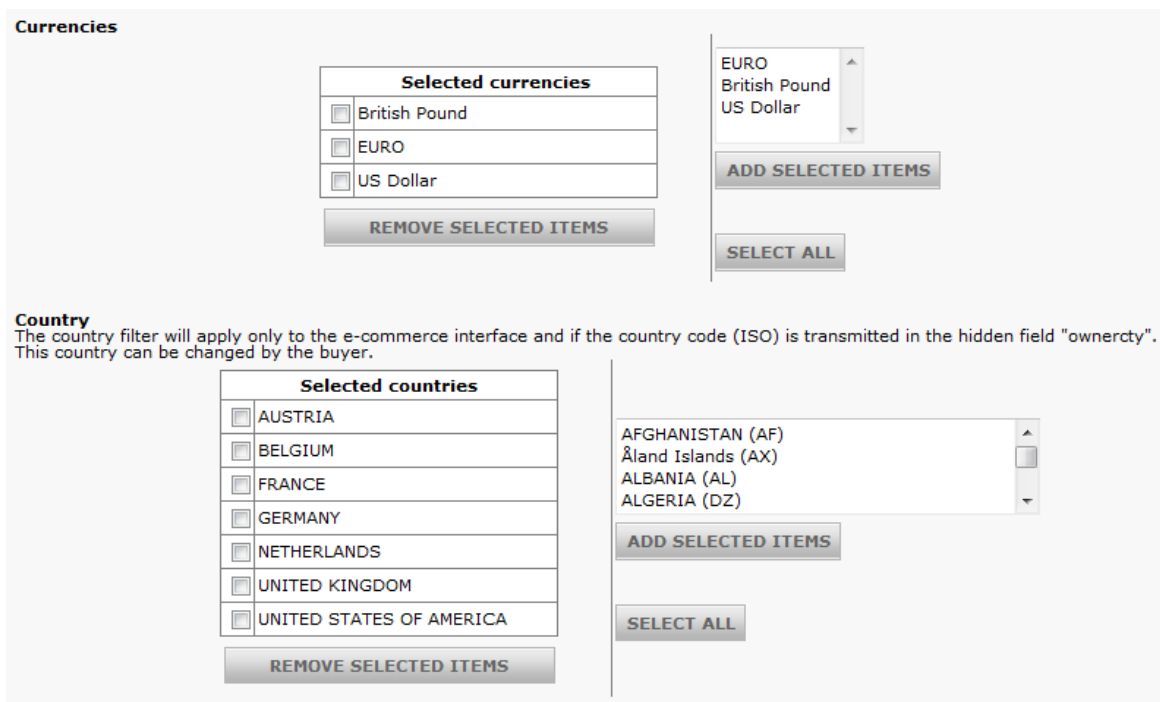
IMPORTANTE

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

Ref.: 722004653			
Order reference: order_123			
Total charge: 84 EUR			
Status: 9			
Order date : 2013-06-06 11:53:31			
Data	Value	Comment	Add to the blacklist
Card/Account number	670397-XXXXXXXX-09		<input type="checkbox"/>
IP address	84.193.187.225		<input type="checkbox"/>
			<input checked="" type="radio"/> Commercial dispute <input type="radio"/> Actual fraud
			DISPUTE

6.1 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.



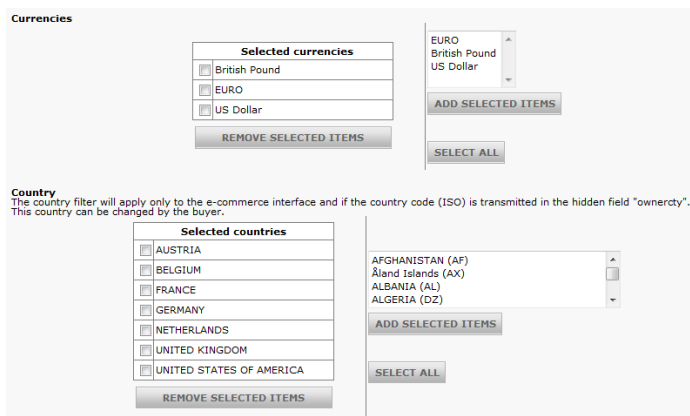
- Haga clic en el botón "DISPUTE" para enumerar los datos recibidos para la transacción que se pueden añadir a la lista negra y blanca.
- Acceda a la página de disputas y elija la lista que desea añadir a los datos de transacción (Lista negra o Lista blanca). A continuación, seleccione el motivo de la 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.



- Guarde y confirme para añadir los datos a la lista adecuada. La comprobación de fraude surte efecto de inmediato.

Currencies

Selected currencies	
<input type="checkbox"/>	British Pound
<input type="checkbox"/>	EURO
<input type="checkbox"/>	US Dollar

REMOVE SELECTED ITEMS

EURO
British Pound
US Dollar

ADD SELECTED ITEMS

SELECT ALL

Country
The country filter will apply only to the e-commerce interface and if the country code (ISO) is transmitted in the hidden field "ownership". This country can be changed by the buyer.

Selected countries	
<input type="checkbox"/>	AUSTRIA
<input type="checkbox"/>	BELGIUM
<input type="checkbox"/>	FRANCE
<input type="checkbox"/>	GERMANY
<input type="checkbox"/>	NETHERLANDS
<input type="checkbox"/>	UNITED KINGDOM
<input type="checkbox"/>	UNITED STATES OF AMERICA

REMOVE SELECTED ITEMS

AFGHANISTAN (AF)
Åland Islands (AX)
ALBANIA (AL)
ALGERIA (DZ)

ADD SELECTED ITEMS

SELECT ALL

Desde la página de disputa también puede seleccionar los datos (p. ej., perteneciente a su centro de llamadas, cliente VIP, etc.) que añadir a la lista blanca. Si selecciona datos que estaban anteriormente en la lista negra, se añadirán automáticamente a la lista blanca. La comprobación de fraude surte efecto de inmediato.

7 Comentarios

7.1 Vista de transacciones en el área de administración

7.1.1 Criterios de selección avanzados

Al buscar una transacción a través del enlace "Ver transacciones" o "Historial financiero" del menú de su cuenta, encontrará dos criterios adicionales en "Criterios de selección avanzados": categoría de riesgo y dirección IP. En la puntuación, puede seleccionar entre tres categorías: rojo, naranja, verde. 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.

7.1.2 Detalles de la transacción

En los detalles de transacción (página de finanzas), verá información adicional como, por ejemplo, el resultado del código de verificación de la tarjeta (si el cliente ha introducido el CVC), el país de la tarjeta, el país de la dirección IP y la dirección IP recibida. Además de esto, verá la puntuación final y la categoría de puntuación, junto con el botón "Ver detalles de puntuación", por si desea obtener más información sobre la puntuación.

The screenshot displays a transaction details interface. At the top, there are two buttons: "DISPUTE" with the text "Mark as a dispute or fraud and add to blacklists." and "VIEW TRANSACTIONS FROM SAME IP ADDRESS". Below these is a table with a header "Fraud detection" and a row with a green background showing "Scoring: 14" and "Scoring category: Green (G)". A button "VIEW SCORING DETAILS" is positioned below the table. Underneath, the text "E-commerce with SSL encryption" is shown, followed by transaction details: "Card verification code : CVC received: Unknown result", "Card country: CH (SWITZERLAND)", "IP address country: GB (UNITED KINGDOM)", and "Received IP address: 94.118.170.40".

Hay dos botones situados por encima de la tabla con información adicional: "Dispute" (Disputa) y "View transactions from same IP address" (Ver transacciones desde la misma dirección IP)

7.1.2.1 Disputa

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

También puede simplemente marcar la transacción como fraude o disputa comercial.

Importante

Seleccione "Fraude real" solo si el cliente realmente ha cometido fraude con esta tarjeta, por ejemplo si un titular de tarjeta ha utilizado una tarjeta que no le pertenece.

Ref.: 722004653			
Order reference: order_123			
Total charge: 84 EUR			
Status: 9			
Order date : 2013-06-06 11:53:31			
Data	Value	Comment	Add to the blacklist
Card/Account number	670397-XXXXXXXX-09		<input type="checkbox"/>
IP address	84.193.187.225		<input type="checkbox"/>
			<input checked="" type="radio"/> Commercial dispute
			<input type="radio"/> Actual fraud
			DISPUTE

7.1.2.2 Ver transacciones desde la misma dirección IP

Cuando haga clic en el botón "Ver transacciones desde la misma dirección IP", se mostrará una lista que contiene todas las transacciones que se originan desde la misma dirección IP dentro de un periodo determinado.

7.1.2.3 Ver detalles de puntuación

Al hacer clic en el botón "Ver detalles de puntuación", podrá consultar información adicional relacionada con el cálculo de la puntuación. Verá una lista de criterios de puntuación que se han tenido en cuenta para el cálculo, junto con el resultado de la puntuación. Los criterios que se cumplen se resaltan en negrita en la lista de criterios.

Análisis de fraude-rastreo

En la página de detalles de puntuación puede comparar las transacciones que se han registrado con el mismo número de tarjeta, BIN, dirección IP, dirección de correo electrónico, nombre del titular de la tarjeta, país de la tarjeta de crédito y país de dirección IP, en un periodo determinado que habrá definido.

Puede marcar una o más casillas de criterios de búsqueda y seleccionar el operador lógico que desea aplicar a los criterios de búsqueda seleccionados (AND u OR). Al hacer clic en el botón "Iniciar búsqueda", recuperaremos todas las transacciones que cumplen los criterios seleccionados. La búsqueda cubre todas las transacciones desde el momento en que se inicia (no desde la fecha de la transacción original).

La primera búsqueda se basará en los valores de la transacción original, de modo que para cada criterio comprobaremos un valor. Cuando lleve a cabo la siguiente búsqueda ("Iniciar búsqueda 2", "Iniciar búsqueda 3", etc.), buscaremos en los resultados de la búsqueda anterior. En búsquedas sucesivas, los criterios pueden tener varios valores, lo cual multiplica los resultados y descubre posibles rastros de fraude.

7.1.3 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.

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

La siguiente lista no completa contiene algunos de los ejemplos de códigos de error 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
- 3 / 30131002 Ha alcanzado la cantidad total permitida
- 3 / 30001102 Cantidad de países diferentes demasiado elevada
- 3 / 30001141 Correo electrónico en la lista negra
- 3 / 30001142 Nombre de pasajero en la lista negra
- 3 / 30001143 Nombre en la lista negra
- 3 / 30001144 Nombre del pasajero distinto al nombre del propietario
- 3 / 30001145 Hora de salida demasiado breve
- 3 / 30001154 Ya ha alcanzado el límite de uso permitido
- 3 / 30001155 Ya ha alcanzado el límite de uso permitido
- 3 / 30001180 Máxima puntuación alcanzada

7.2 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	<p>País de origen de la dirección IP.</p> <p>Formato: Código ISO alfabético de 2 caracteres. Si este parámetro no está disponible, se devolverá "99" en la respuesta.</p> <p>Esta comprobación de la IP se basa en listas de IP obtenidas de forma externa, por lo que existe un ligero riesgo de error, ya que tenemos que fiarnos de la precisión de esta lista. La comprobación proporciona resultados positivos en el 94 % de los casos.</p>
CCCTY	<p>País de origen de la tarjeta de crédito.</p> <p>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 2 caracteres. Si este parámetro no está disponible, se devolverá "99" en la respuesta.</p> <p>Esta comprobación del país de la tarjeta de crédito se basa en listas obtenidas de forma externa, por lo que existe un ligero riesgo de error debido a que tenemos que fiarnos de la precisión de esas listas. La comprobación proporciona resultados positivos en el 94 % de los casos.</p>
ECI	<p>Indicador de comercio electrónico. Los posibles valores de ECI y sus significados se definen a continuación:</p> <ul style="list-style-type: none"> 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 (consulte aquí) 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 (consulte aquí) (como en 6) 91 ¡¡¡ Identificación del titular FALLIDA!!! (Puede aplicarse la garantía de pago

Parámetro	Valor
	condicional (consulte aquí). Consulte con su entidad adquirente) 92 Sitio de autenticación del banco emisor no disponible de forma temporal, pero se ha continuado con la transacción
CVCHECK	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. 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. 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; 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.

Campos avanzados

NBRUSAGE	Número de veces que una tarjeta de crédito se ha utilizado durante un periodo determinado (si se ha configurado la regla "Maximum utilisation per card, per period" [Utilización máxima por tarjeta y por periodo]).
NBRIPUSAGE	Número de veces que una dirección IP se ha utilizado durante un periodo determinado (si se ha configurado la regla "Maximum utilisation per IP address, per period" [Utilización máxima por dirección IP y por periodo]).
SCORING	La puntuación final para la transacción, es decir, el total de las puntuaciones otorgadas a cada elemento descrito en la lista de puntuación
SCO_CATEGORY	El color de la categoría a la que pertenece la puntuación final, que se basa en la configuración de la página de la puntuación. Los posibles valores son G (del inglés "green", verde), O (del inglés "orange", naranja) y R (del inglés "red", rojo).

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

8 Apéndice: Comparación entre parámetros y comprobaciones/reglas

Ogone Parámetro de	Descripción	Reglas/ comprobaciones en FDMA
CN	El nombre del titular de la tarjeta puede contener un máximo de 35 caracteres. Este parámetro puede enviarse a través de Ogone e-Commerce, DirectLink y Batch. Recuerde que para Ogone e-Commerce, el nombre del titular de la tarjeta también se capturará a través de la página de pago de Ogone, en la que el nombre del titular de la tarjeta es un campo obligatorio.	<ul style="list-style-type: none"> • Lista negra de nombres • Lista gris de nombres • Nombre del pasajero distinto al nombre del titular de la tarjeta
OWNERADDRESS	La dirección del cliente puede contener un máximo de 35 caracteres.	<ul style="list-style-type: none"> • La dirección de facturación es un apartado de correos
ADDRMATCH	El hecho de que la dirección de facturación se considere diferente de la dirección de entrega se basa en el valor del campo adicional "ADDRMATCH" que el comerciante nos envía en los detalles del pedido. Si el valor es "1", las direcciones de facturación y de entrega se considerarán idénticas. Si el valor es "0", se considerarán diferentes entre sí. (Como alternativa, se puede utilizar el parámetro "ADDMATCH").	<ul style="list-style-type: none"> • Dirección de facturación distinta a la dirección de envío
OWNERZIP	El código postal del cliente puede contener un máximo de 10 caracteres.	<ul style="list-style-type: none"> • Códigos postales de riesgo • La verificación avanzada de la dirección solo comprueba marcas de tarjeta específicas
OWNERTELNO	El número de teléfono del cliente puede contener un máximo de 30 caracteres para todos los módulos de Ogone con excepción de Ogone Batch, en el que puede tener un máximo de 20 caracteres. En este campo se permiten caracteres especiales (por ejemplo, "+" o "/"). Es conveniente utilizar un formato consistente para enviar números de teléfono.	<ul style="list-style-type: none"> • Lista gris de números de teléfono • Lista negra de números de teléfono
OWNERCTY	El país de facturación del cliente puede contener un máximo de 2 caracteres. El país según el código ISO 3166-1-alpha-2 que se puede encontrar en http://www.iso.org/iso/en/prodsservices/iso3166ma/02iso-3166-code-lists/list-en1.html .	<ul style="list-style-type: none"> • Cantidad de países diferentes
EMAIL	La dirección de correo electrónico del cliente puede contener un máximo de 50 caracteres.	<ul style="list-style-type: none"> • Lista blanca de correo electrónico • Correo electrónico en lista negra • Correo electrónico en lista gris • Correo electrónico gratuito • Límites de utilización
Generic_BL	La lista negra genérica puede contener un máximo de 50 caracteres.	<ul style="list-style-type: none"> • Lista negra genérica • Lista gris genérica
REMOTE_ADDR	Dirección IP del cliente. Solo debe enviarse cuando se utiliza Ogone DirectLink. En Ogone e-Commerce, la dirección IP se detecta y se registra automáticamente.	<ul style="list-style-type: none"> • Lista blanca de IP • Lista gris de IP • Lista negra de IP • Límites de utilización • Grupos de países de

		<ul style="list-style-type: none"> IP Proxy anónimo Combinación de país de tarjeta y de IP no autorizada El país de IP es diferente del país de tarjeta
CUID	Identificador único de cliente. Puede contener un máximo de 50 caracteres.	<ul style="list-style-type: none"> Lista blanca de identificadores únicos de cliente
CARDNO	El número de tarjeta o el número de cuenta pueden contener un máximo de 21 caracteres. Solo debe enviarse cuando se utiliza Ogone DirectLink. En Ogone e-Commerce, el número de tarjeta se detecta y se registra automáticamente.	<ul style="list-style-type: none"> Lista gris de tarjetas Lista negra de tarjetas Lista negra de BIN Lista gris de BIN País de tarjeta de riesgo elevado País de tarjeta de riesgo medio Límites de utilización
ECOM_SHIPTO_POSTAL_POSTALC ODE	Código postal de entrega. Puede contener hasta 10 caracteres alfanuméricos.	<ul style="list-style-type: none"> Códigos postales de riesgo
ECOM_BILLTO_POSTAL_POSTALC ODE	Código postal de facturación	<ul style="list-style-type: none"> Códigos postales de riesgo La verificación avanzada de la dirección solo comprueba marcas de tarjeta específicas
	DATOS DE LÍNEA AÉREA/VIAJE	
AIPASNAME	Nombre del pasajero principal. El valor predeterminado es el nombre del titular de la tarjeta de crédito.	<ul style="list-style-type: none"> Lista negra de nombres Lista gris de nombres Nombre del pasajero distinto al nombre del titular de la tarjeta
AIEXTRAPASNAME1	Nombre del pasajero adicional para PNR con más de un pasajero. Este campo se puede repetir hasta 5 veces (por ejemplo, 5 pasajeros adicionales), cambiando el dígito al final del nombre del campo.	<ul style="list-style-type: none"> Lista negra de nombres Lista gris de nombres Nombre del pasajero distinto al nombre del titular de la tarjeta
AIORCITY1	El aeropuerto de salida (corto) es un campo obligatorio y puede contener un máximo de 5 caracteres.	<ul style="list-style-type: none"> El aeropuerto de salida no se encuentra en la lista de aeropuertos de confianza Itinerario de riesgo (grupos de aeropuertos) País de IP no autorizado para el itinerario
AIORCITYL1	El aeropuerto de salida (largo) es un campo obligatorio y puede contener un máximo de 20 caracteres.	<ul style="list-style-type: none"> El aeropuerto de salida no se encuentra en la lista de aeropuertos

		de confianza <ul style="list-style-type: none"> • Itinerario de riesgo (grupos de aeropuertos) • País de IP no autorizado para el itinerario
AIDESTCITY1	El aeropuerto de llegada (corto) es un campo obligatorio y puede contener un máximo de 5 caracteres.	<ul style="list-style-type: none"> • Itinerario de riesgo (grupos de aeropuertos) • País de IP no autorizado para el itinerario
AIDESTCITYL1	El aeropuerto de llegada (largo) es un campo obligatorio y puede contener un máximo de 20 caracteres.	<ul style="list-style-type: none"> • Itinerario de riesgo (grupos de aeropuertos) • País de IP no autorizado para el itinerario
AISTOPOV1	Escala permitida para aeropuerto. Posibles valores: las letras mayúsculas O y X. O: el pasajero puede pararse y permanecer. X: el pasajero no puede permanecer.	<ul style="list-style-type: none"> • Itinerario de riesgo (grupos de aeropuertos)
AIFLDATE1	Fecha de vuelo.	<ul style="list-style-type: none"> • Tiempo hasta la salida 1 • Tiempo hasta la salida 2 • Tiempo hasta la salida 3

La lista anterior de parámetros de viaje solo contiene los parámetros que están vinculados a las reglas/comprobaciones en el módulo FDMA. Para obtener la lista completa de parámetros de viaje obligatorios, compruebe el apéndice Formato especial para viajes en nuestras guías de DirectLink o Advanced e-Commerce .

9 Apéndice: Datos adicionales a través de e-Terminal (MOTO)

Si utiliza nuestra solución MOTO e-Terminal, además de los datos de pedidos predeterminados también podrá especificar detalles de contacto/dirección. Estos datos se tendrán en cuenta para FDMA y mejorarán sus posibilidades de prevención del fraude.

En su área de administración, bajo "Operaciones", seleccione "Nuevo pago". Verá el vale donde pueden especificarse los detalles predeterminados (nombre, número de tarjeta, CVC, etc.).

Verá los detalles adicionales de dirección de entrega y facturación:

FACTURETTE / AANKOOPBEWIJS / VOUCHER

Cardholder's name

Card number*

Expiry date (mm/yyyy)*:
 /

CVC*: [What is this?](#)

Origin of the transaction (ECI)

Invoicing address

First name

Name

Address line 1

Address line 2

Address line 3

Postcode

City

County

Country

E-mail address

Language

Phone number

Copy the invoicing address into the delivery address

Delivery address

First name

Name

Address line 1

Address line 2

Address line 3

Postcode

City

County

Country

Additional information
Beneficiary: **My Company**
Description:

VOUCHER
 Date (GMT+01:00): 2013-06-24 13:43:20
 Order reference:

EUR **Total*:**

10 Apéndice: CVC2 y AAV

10.1 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.

10.2 AAV/AVS

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), pero la funcionalidad de AAV es la misma 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 envió con los de la dirección de facturación proporcionada por el cliente al emisor al solicitar la tarjeta.

American Express realiza esta comprobación de forma automática cuando recibe los detalles de dirección con una transacción; para otras marcas, depende de si la entidad adquirente realiza o no la comprobación de la dirección. En todas las circunstancias, recomendamos que los detalles de la dirección del cliente se proporcionen junto con los detalles del pedido que envía a nuestro sistema.

Aunque una transacción no será denegada debido a los resultados de una comprobación de dirección, el comerciante puede usar estos resultados para decidir si entregar las mercancías o solicitar al cliente más información antes de enviarlas.

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

10.3 Adaptación de la puntuación a partir del resultado AAV/AVS

Basándose en los resultados de AAV/AVS, puede influir en la puntuación de FDMA. Puede seleccionar qué acción desea que aplique nuestro sistema en cada posible respuesta:

Respuesta	Acción
Resultado OK	Ninguna / Restar el "valor" de la puntuación de riesgo

Respuesta	Acción
Resultado KO	Ninguna / Sumar el "valor" a la puntuación de riesgo / Forzar revisión / Bloquear (revisión si está en modo de venta directa)
Código postal KO, dirección OK	Ninguna / Sumar el "valor" a la puntuación de riesgo / Forzar revisión / Bloquear (revisión si está en modo de venta directa)
Código postal OK, dirección KO	Ninguna / Sumar el "valor" a la puntuación de riesgo / Forzar revisión / Bloquear (revisión si está en modo de venta directa)
Resultado no recibido o desconocido	Ninguna / Sumar el "valor" a la puntuación de riesgo / Forzar revisión

Nota

La respuesta "Resultado no recibido o desconocido" puede deberse a que el emisor del cliente (banco) no admite la comprobación AAV/AVS mientras que su entidad adquirente sí la admite. Téngalo en cuenta para la configuración de FDMA.

11 Apéndice: Consejos para informar sobre fraudes

El uso fraudulento de una tarjeta de crédito debe ser comunicado por el propio titular de la tarjeta a su banco emisor (por ejemplo, el banco en el que solicitó su tarjeta de crédito).

Si un comerciante cree que uno de sus clientes está cometiendo fraude, debe comunicárselo a su entidad adquirente.

Si un comerciante desea informar a la policía sobre un defraudador, no necesita el número de la tarjeta de crédito. La información útil para la policía es la dirección IP que el cliente utilizó en el momento de la transacción junto con la fecha, la hora y el huso horario. Si el comerciante puede incluir las direcciones de entrega con esta información, la policía tendrá más posibilidades de seguir el rastro del defraudador. Tenga en cuenta, no obstante, que la dirección IP puede suplantarse y la dirección de entrega puede ser la de un intermediario que tiene que reenviar los bienes a un país extranjero. Esto complica el trabajo de la policía a la hora de seguir el rastro del defraudador.

12 Apéndice: Configuración de grupos y uso compartido de listas negras

Los comerciantes con una cuenta de grupo, que reúne varias cuentas individuales (PSPID) bajo una cuenta principal, pueden beneficiarse de las posibilidades de gestión del fraude entre PSPID.

Estas posibilidades permiten al comerciante:

- Compartir listas negras, grises y blancas entre los diversos PSPID que pertenecen a la cuenta de grupo del comerciante.
- Compartir la configuración de FDMA (criterios, reglas, límites, etc.) y las listas (grupos de países, códigos postales de riesgo, etc.).

Activación

- Si utiliza "Group Manager" (Administrador de grupos) y está interesado en habilitar "Group fraud configuration and sharing" (Uso compartido y configuración de datos de fraude para grupos), póngase en contacto con our Customer Care
- Si todavía no utiliza "Group Manager" (Administrador de grupos), pero tiene varios PSPID que desea unir en una cuenta de grupo, para utilizar "Group fraud configuration and sharing" (Uso compartido y configuración de datos de fraude para grupos), póngase en contacto con our Sales Team para obtener más información.

13 Apéndice: Mecanismo de anulación

La tabla siguiente contiene todos los criterios que se pueden anular:

Criterio	Se puede anular mediante 3-D Secure / lista blanca de CUI / Lista blanca de correo electrónico	Se puede anular mediante lista blanca de direcciones IP
La dirección es un apartado de correos	✓	
Importe - superior al intervalo	✓	
Importe - inferior al intervalo	✓	
BIN en lista negra	✓	
BIN en lista gris	✓	
País de tarjeta - Riesgo elevado	✓	
País de tarjeta - Riesgo medio	✓	
Tarjeta en lista gris	✓	
Submarca de tarjeta - Riesgo elevado	✓	
Submarca de tarjeta - Riesgo medio	✓	
Nombre del titular de la tarjeta en lista negra - Coincidencia parcial	✓	
Nombre del titular de la tarjeta en lista negra - Coincidencia total	✓	
Nombre del titular de la tarjeta en lista gris- Coincidencia parcial	✓	
Nombre del titular de la tarjeta en lista gris- Coincidencia total	✓	
Datos en lista negra genérica	✓	
Datos en lista gris genérica	✓	
Huella de dispositivo no recibida	✓	
Huella de dispositivo no solicitada - por defecto	✓	
Huella de dispositivo no solicitada - transac. Nivel	✓	
Categoría de perfil de huella de dispositivo - Riesgo elevado	✓	
Categoría de perfil de huella de dispositivo - Sospechoso	✓	
Correo electrónico en lista negra - Coincidencia parcial	✓	
Correo electrónico en lista negra - Coincidencia total	✓	
Correo electrónico en lista gris- Coincidencia parcial	✓	

Criterio	Se puede anular mediante 3-D Secure / lista blanca de CUI / Lista blanca de correo electrónico	Se puede anular mediante lista blanca de direcciones IP
Correo electrónico en lista gris- Coincidencia total	✓	
Puntuación de Expert no disponible	✓	
El primer aeropuerto de salida no es un aeropuerto de confianza	✓	
Correo electrónico gratuito	✓	
La dirección de facturación es diferente de la dirección de entrega	✓	
Dirección IP en lista negra	✓	✓
Dirección IP en lista gris	✓	✓
País de IP - Proxy anónimo	✓	✓
País de IP - Riesgo elevado	✓	✓
País de IP - Riesgo medio	✓	✓
El país de IP es diferente del país de tarjeta	✓	✓
Número de emisor - Riesgo elevado	✓	
Número de emisor - Riesgo medio	✓	
Cantidad máxima/tarjeta - Umbral elevado	✓	
Cantidad máxima/tarjeta - Umbral medio	✓	
Utilización máxima del correo electrónico - Umbral elevado	✓	
Utilización máxima del correo electrónico - Umbral medio	✓	
Utilización máxima de IP en todos los estados - Umbral elevado	✓	✓
Utilización máxima de IP en todos los estados - Umbral medio	✓	✓
Utilización máxima/tarjeta - Umbral elevado	✓	
Utilización máxima/tarjeta - Umbral medio	✓	
Utilización máxima/IP - Umbral elevado	✓	✓
Utilización máxima/IP - Umbral medio	✓	✓
Cantidad de países diferentes	✓	
Billete de ida	✓	
Nombre del pasajero distinto al nombre del titular de la tarjeta	✓	
Nombre del pasajero en lista negra de nombres - Coincidencia parcial	✓	

Criterio	Se puede anular mediante 3-D Secure / lista blanca de CUI / Lista blanca de correo electrónico	Se puede anular mediante lista blanca de direcciones IP
Nombre del pasajero en lista negra de nombres - Coincidencia total	✓	
Nombre del pasajero en lista gris de nombres - Coincidencia parcial	✓	
Nombre del pasajero en lista gris de nombres - Coincidencia total	✓	
Teléfono en lista negra - Coincidencia parcial	✓	
Teléfono en lista gris - Coincidencia parcial	✓	
Código postal y dirección - Riesgo elevado	✓	
Código postal y dirección - Riesgo medio	✓	
Categoría de producto - Riesgo elevado	✓	
Categoría de producto - Riesgo medio	✓	
Itinerario de riesgo (grupos de aeropuertos) - aeropuerto de riesgo elevado	✓	
Itinerario de riesgo (grupos de aeropuertos) - aeropuerto de riesgo medio	✓	
Método de envío - Riesgo elevado	✓	
Método de envío - Riesgo medio	✓	
Detalles de método de envío - Riesgo elevado	✓	
Detalles de método de envío - Riesgo medio	✓	
Hora de pedido - Período de riesgo elevado	✓	
Hora de pedido - Período de riesgo medio	✓	
Plazo de entrega - Estrictamente inferior a X horas	✓	
Plazo de entrega - Estrictamente inferior a Y horas	✓	
Plazo de entrega - Estrictamente inferior a Y horas	✓	
Plazo hasta la salida - Estrictamente inferior a X días	✓	
Plazo hasta la salida - Estrictamente inferior a Y días	✓	
Plazo hasta la salida - Estrictamente inferior a Z días	✓	
Combinación de país de tarjeta y de IP no autorizada - Riesgo elevado	✓	✓
Combinación de país de tarjeta y de IP no autorizada - Riesgo medio	✓	✓
País de IP no autorizado para el itinerario	✓	✓

Observaciones:

- El criterio "Tarjeta en lista negra" no se puede anular y no se anulará nunca.
- Las reglas de post-adquirente (AVS/CVC) no se anularán.
- La categoría de puntuación (Bloqueo o Revisión) se puede anular mediante los criterios 3-D Secure/lista blanca de CUI/lista blanca de correo electrónico.
- Se añaden tres puntos a la puntuación incluso si se anula una regla de revisión.