Autenticación reforzada de clientes:

De requisito normativo a ventaja competitiva

checkout.com

Introducción

La autenticación reforzada de clientes (o SCA, de strong customer authentication) es una iniciativa concebida para reducir el fraude. Forma parte de la Directiva de servicios de pago 2 (PSD2) y tiene el objetivo de mejorar la seguridad de los pagos electrónicos. No obstante, cumplir este objetivo sin provocar un impacto negativo en la experiencia del consumidor ha supuesto todo un reto para los emisores y las empresas.

No cabe ninguna duda de que proteger al cliente, reducir el fraude e incrementar la seguridad de los pagos son iniciativas positivas desde el punto de vista teórico, pero, en la práctica, había una inquietud más que justificada por el impacto potencial de la normativa de SCA en el funcionamiento de los pagos. A los comercios en línea —y a la industria en general— les preocupaba que los pasos adicionales en el punto de venta digital exasperaran a los clientes y les hicieran abandonar la compra.

Sin embargo, los comercios electrónicos más avispados han hallado la solución en los últimos avances tecnológicos, con el aprovechamiento de los conocimientos extraídos de los datos y la creación de un plan estratégico que saca partido de las exenciones de los requisitos de la SCA.

Las empresas tienen la oportunidad de reducir el fraude, pero para conseguirlo también tienen que replantearse el recorrido del cliente, incrementar el número de autorizaciones aprobadas y ganarse la confianza de sus clientes al mismo tiempo que les garantizan la protección que ofrece la SCA. Aunque se trata de un compromiso improrrogable en Europa, las empresas de todo el mundo deberían considerar su adopción.

¿Cuáles son los aspectos clave que deben considerar los comercios electrónicos al elaborar una estrategia de autenticación reforzada de clientes? En este manual te ofrecemos una serie de ideas prácticas para sacar el máximo partido a tu proveedor de servicios de pago y para transformar el desafío de conformidad normativa que supone la SCA en una oportunidad para optimizar las conversiones.

Contenido

Cronograma de implantación de la autenticación reforzada en Europa

Desde la propuesta inicial de la normativa PSD2, se han concedido ampliaciones de plazos que han dado a las empresas europeas más tiempo para cumplirla. Por su parte, el Reino Unido marcó su propio plazo para las normativas, que también ha sido ampliado. En este breve cronograma se muestran las fechas más significativas de la aplicación del mandato.

13 DE ENERO DE 2016
Entra en vigor la PSD2

13 DE ENERO DE 2018
Fecha límite para la transposición de las normativas sobre la SCA en Europa

14 DE SEPTIEMBRE DE 2019
Fecha original de entrada en vigor del mandato SCA en Europa

31 DE DICIEMBRE DE 2020
Fecha revisada de entrada en vigor del mandato SCA en Europa

14 DE MARZO DE 2021
Fecha original de entrada en vigor del mandato SCA en el Reino Unido

14 DE SEPTIEMBRE DE 2021
Fecha inicial revisada de entrada en vigor del mandato SCA en el Reino Unido

NOVIEMBRE DE 2021
Los bancos británicos inician los planes para acelerar la implantación de la SCA

14 DE MARZO DE 2022
Fecha de entrada en vigor del mandato SCA en el R. U.

14 DE OCTUBRE DE 2022
Se desmantela el uso de 3DS1 para todos los sistemas de tarjetas

¿De qué sirve la autenticación reforzada de clientes?

La creciente amenaza del fraude en línea

Se mire por donde se mire, el fraude en línea es un problema; **un problema con un coste de 35.540 millones de dólares anuales.** Eso es lo que les costó a los comercios electrónicos de todo el mundo el fraude por pago remoto o sin presencia de tarjeta en 2020.[1]

El que en la práctica era ya un importe enorme que afectaba a todo tipo de marcas, se acentuó durante la pandemia y **hasta el 25 % de los comercios electrónicos experimentaron un repunte considerable de costosas devoluciones en los primeros 12 meses.[2]**

Tras estas estadísticas se esconde la amenaza del conocido como «fraude amistoso», que supone hasta un tercio de los pagos impugnados.[3] Consiste en que los clientes presentan una reclamación fraudulenta de devolución, ya sea porque se aprovechan del sistema para iniciar la devolución de bienes o servicios que han recibido correctamente o bien, porque solicitan la rectificación de operaciones que se ejecutaron de forma incorrecta o sin su consentimiento, por ejemplo por parte de un familiar.

[1] First Data, The Future of Fraud Report, 2021

[2] Checkout.com, The New State of Retail Report, 2021

[3] Javelin Research, The Chargeback Triangle, 2018

La autenticación reforzada como remedio al fraude

La autenticación reforzada de clientes tiene el potencial de reducir el fraude con tarjeta en las tiendas electrónicas del mismo modo que el uso de chips y PIN lo redujo en las transacciones físicas. SCA ofrece una capa de protección contra el uso fraudulento de las cuentas bancarias y, en la mayoría de los casos, traslada la responsabilidad de los comerciantes a los emisores de las tarjetas.

Ahora los bancos y los proveedores de servicios de pago garantizan el pago a los comercios para determinadas operaciones electrónicas autenticadas con 3DS2. Es más, 3DS2 supone una oportunidad para los comercios de compartir más datos con los emisores, lo que mejora la autenticación basada en el riesgo y también la experiencia de los clientes a la hora de realizar el pago.

Vista desde esta perspectiva, la autenticación reforzada de clientes es más que un simple requisito normativo.

Hay casi tantas maneras de aproximarse a la SCA como empresas hay en internet y la explicación es que una buena estrategia de SCA debe tener en cuenta el tipo de operación, el comercio, el cliente, los bienes o servicios que se venden, el emisor y el apetito por el riesgo, entre otros factores. Como es lógico, también debe reflejar la estrategia general del comerciante con respecto a los pagos y los fraudes. Dado que no hay una solución universal, en las páginas siguientes proponemos ideas y preguntas que te ayudarán a formular tu propia estrategia para la autenticación reforzada.

Explica

¿En qué consiste la autenticación reforzada de clientes?

La autenticación es el proceso de confirmar si alguien es quien dice ser. Hay distintas maneras de hacerlo, máxime cuando las partes no se encuentran cara a cara, como al hacer compras u operaciones bancarias en línea.

Normalmente, los elementos de autenticación se categorizan en:

Algo que solo conoce el cliente
(p. ej., un PIN o una contraseña)

Algo que solo posee el cliente
(p. ej., un token o un dispositivo)

Algo que es inherente al cliente
(p. ej., huella dactilar o reconocimiento de voz)

Para aumentar la seguridad de los pagos remotos, la Directiva de servicios de pago revisada de la UE (PSD2) requiere un mínimo de dos factores para conseguir la llamada autenticación «reforzada» de clientes o SCA, por sus siglas en inglés.

Aunque la PSD2 es obligatoria para los bancos y las entidades financieras, todos los proveedores de la cadena de pago han tenido que hacer cambios en su forma de procesar los pagos con tarjeta y de autenticar a los clientes.

Los comercios han tenido que desarrollar estrategias de autenticación adecuadas y compatibles con 3DS; las pasarelas de pago han tenido que adaptar su servicio a los nuevos estándares de EMV 3DS2; los adquirientes han tenido que gestionar las exenciones y los índices de fraude; las redes han tenido que actualizar sus reglas, sus servidores de directorios y prestar servicios de comunicaciones a todas las partes; y los emisores han tenido que autenticar a los titulares de tarjetas, aplicar las exenciones y mejorar sus controles del riesgo.[4]

[4] The Payments Association, The Long and Winding Road to SCA, 2021

Cinco preguntas para definir tu estrategia de SCA

Hay que tener en cuenta muchos aspectos para decidir cómo actuar frente a cada operación y a la vez garantizar el cumplimiento, reducir el fraude y minimizar las fricciones. Hemos desglosado estas cuestiones en cinco preguntas.

1. ¿La operación se incluye en el ámbito de aplicación de la SCA?

↓

2. ¿Las operaciones posteriores del mismo tipo se incluyen en el ámbito de la SCA?

↓

3. ¿Puede mi empresa pedir la exención de la autenticación reforzada para esta operación?

↓

4. ¿Debe mi empresa pedir la exención para esta operación?

↓

5. ¿Quiere mi empresa gestionar el plan de SCA por su cuenta?

PREGUNTA 1

¿La operación se incluye en el ámbito de aplicación de la SCA?

Casi la mitad de las operaciones sin presencia de tarjeta podrían quedar fuera del ámbito de aplicación de los requisitos de la autenticación reforzada de clientes, según los cálculos de Visa. Eso significa que los emisores de tarjetas no solicitarán un segundo factor de autenticación (algo que el cliente conoce, posee o es) al hacer el pago electrónico.

Las cuatro principales operaciones excluidas de este ámbito son:

Las operaciones de compra telefónica o por correo (MOTO)

Las operaciones anónimas con tarjeta de prepago en las que los emisores no pueden llevar a cabo la autenticación

Las operaciones en las que el emisor de la tarjeta o el adquiriente están radicados fuera del Espacio Económico Europeo (EEE). En estas operaciones hay que hacer lo posible por aplicar la autenticación, pero, al quedar fuera del ámbito de aplicación de la normativa, los emisores no pueden rechazar las solicitudes de autorización de este tipo.

Las operaciones iniciadas por el comercio, que forman un gran grupo que incluye los pagos fraccionados, las operaciones frecuentes, los pagos aplazados, los cargos por no presentarse y los pagos con nueva autorización. En la página 11 encontrarás más información sobre las operaciones iniciadas por el comercio.

Algunas operaciones que no son de compra también están excluidas del ámbito de aplicación de la SCA. Por ejemplo, aquellas en las que se hace un abono en la cuenta o la tarjeta del cliente en vez de efectuar un cargo, como los reembolsos y las transferencias originales de crédito de las indemnizaciones de seguros o el pago de los premios en el sector del juego. También se excluyen las operaciones de verificación de cuenta, de valor cero, que se usan para comprobar el estado de una cuenta.

La identificación y la clasificación correctas de las operaciones que quedan fuera del ámbito son fundamentales para evitar que los emisores rechacen las operaciones. Colabora con tu proveedor de servicios de pago para entender el recorrido de tus clientes en el contexto de la autenticación reforzada y minimizar así las fricciones y el abandono de las compras en línea.

Sí, ve a la pregunta 2

No, ve a la pregunta 5

PREGUNTA 2

¿Las operaciones posteriores del mismo tipo se incluyen en el ámbito de la SCA?

Determinados tipos de operaciones iniciadas por el comerciante quedan fuera del ámbito de aplicación de la autenticación reforzada una vez que se lleva a cabo la primera operación y el cliente ha aceptado las condiciones de las operaciones posteriores o las ha configurado.

Si los comercios identifican y clasifican correctamente estas operaciones excluidas, los emisores podrán reconocerlas y evitar a los clientes fricciones innecesarias en el proceso de pago.

Las operaciones con beneficiarios de confianza tampoco requieren autenticación reforzada después de la primera operación de «configuración». Los clientes añaden a los comercios a una lista de «beneficiarios de confianza» que mantiene su emisor. Los comercios no tendrán un control directo sobre esta lista, pero pueden educar a sus clientes para que los añadan a la lista en el momento de la autenticación o con sus emisores y, de ese modo, ofrecer a sus clientes habituales una experiencia sin fricciones. En la página 13 encontrarás más información sobre las exenciones de la SCA.

Las operaciones iniciadas por el comercio no se limitan a las operaciones frecuentes ni a las suscripciones. También incluyen los envíos aplazados o con entregas parciales que son habituales en el comercio electrónico. Un buen proveedor de servicios de pago procurará estudiar el funcionamiento de tu empresa y personalizar su asesoramiento en cuanto a las operaciones que se excluyen del ámbito de aplicación y cómo clasificar y codificar adecuadamente las operaciones iniciadas por el comercio.

Explica

Los siguientes son ejemplos de operaciones iniciadas por el comercio:

- **Operaciones frecuentes** en las que los comercios facturan a intervalos regulares por bienes o servicios que prestan durante un tiempo prolongado tras la firma de un contrato con el cliente
- **Pagos fraccionados** en los que los comercios realizan varias operaciones para facturar por bienes o servicios tras la firma de un contrato con el cliente
- **Pagos anticipados en los que los comercios facturan por adelantado** en una o varias operaciones tras la firma de un contrato con el cliente
- **Pagos con credenciales almacenadas**, en los que el cliente permite al comercio iniciar una operación o varias en el futuro usando los datos de acceso almacenados. Las ventas pueden corresponder tanto a cantidades e intervalos fijos como variables
- **Pagos con nueva autorización** en los que el pago se realiza después de la compra original; por ejemplo en los envíos con entregas parciales o aplazados
- **Los cobros aplazados** en que los comercios facturan al cliente después de ofrecerle el servicio original, como pueden ser los servicios adicionales o el cobro de desperfectos en el sector hotelero
- **Los cargos por no presentarse** en que los comercios facturan a clientes que no utilizan los servicios que han contratado, bastante habituales en los sectores hotelero, de cruceros o de alquiler de vehículos

Sí, ve a la pregunta 3

No, ve a la pregunta 5

Explica

La evolución de 3DS 1.0 a EMV 3DS 2.x

El protocolo EMV 3DS actualizado se ha optimizado para los pagos por teléfono móvil y en las aplicaciones. De ese modo aborda la experiencia multicanal actual que abarca los teléfonos móviles, los ordenadores y hasta los televisores digitales, pero además se anticipa para aceptar los canales y los factores del futuro.

Además, EMV 3DS 2.x favorece un mayor intercambio de datos entre el comercio y el emisor para mejorar las aprobaciones, El protocolo actualizado permite a los emisores pedir autenticación cuando se producen operaciones de riesgo y, a los comercios, incluir esas respuestas en el contexto de la operación para mejorar los índices de aprobación y la experiencia del usuario.

	3DS1.0	EMV 3DS2.x
Experiencia del usuario mejorada		
Capacidad de integración en el proceso del comercio	✓	✓
Reducción del número de mensajes necesarios		✓
Capacidad de procesar las solicitudes de autenticación reforzadas		✓
Más datos para la autenticación		
Datos relacionados con el pago	✓	✓
Datos no relacionados con el pago		✓
Compatibilidad con los nuevos métodos de autenticación y los que haya en el futuro		✓
Omnicanal y compatibilidad con diversos dispositivos		
Compatibilidad con la autenticación en el navegador	✓	✓
Compatibilidad con la autenticación mediante el teléfono/las aplicaciones		✓
Compatibilidad con el monedero electrónico y la autenticación no basada en el pago		✓
Compatibilidad con los canales y factores del futuro (p. ej., MOTO, videoconsolas, televisores inteligentes, IoT)		✓

PREGUNTA 3

¿Puede mi empresa pedir la exención de la autenticación reforzada para esta operación?

Las principales exenciones en el comercio electrónico:

- **Operaciones que han superado un análisis del riesgo** en casos en que los índices de fraude no superan unos parámetros sujetos a un control estricto
- **Operaciones de escasa cuantía**, clasificadas como pagos a distancia inferiores a 30 € hasta un máximo de cinco operaciones o un límite acumulativo de 100 €
- **Beneficiarios de confianza**, cuando los clientes añaden a los comercios a una lista de beneficiarios de confianza que mantiene su emisor
- **Pagos corporativos seguros** iniciados mediante procesos y protocolos corporativos seguros, como los sistemas de gestión de viajes centralizados, las tarjetas de viaje corporativas o las tarjetas virtuales

Una de las mejores formas de crear una experiencia sin fricciones consiste en saber en qué casos no aplicar la autenticación reforzada de clientes.

Para crear una estrategia de exenciones eficaz hay que utilizar la última versión del protocolo 3-D Secure (3DS), que permite la autenticación doble. Esta permite que, si los emisores declinan parcialmente (soft decline) una solicitud de autorización, el rechazo se pueda convertir en una aprobación si se completa correctamente la autenticación. La versión 1.0 de 3DS no es compatible con este proceso de rectificación. Los comercios que no se actualicen podrían enfrentarse a rechazos parciales y a una pérdida considerable de ingresos.

3DS 2 también permite un mayor intercambio de datos para aumentar las aprobaciones. Los comercios y los emisores solían intercambiar una media de ocho datos en las autenticaciones con 3DS 1, mientras que con la versión actualizada pueden intercambiar un número hasta diez veces mayor de datos para permitir a los emisores evaluar mejor el riesgo de cada operación.

Los proveedores de servicios de pago han desarrollado motores de SCA para determinar si las operaciones están excluidas del ámbito de aplicación o exentas de la autenticación reforzada y cómo categorizarlas y redirigirlas para obtener los mejores resultados. Es recomendable que los comercios colaboren estrechamente con sus proveedores de servicios de pago en el uso de esta tecnología y en el desarrollo de estrategias para las exenciones de la SCA que se adapten a su negocio. En la página 15 encontrarás más información sobre las estrategias de exención.

Sí, ve a la pregunta 4

No, ve a la pregunta 5

Explica

Rechazos parciales frente a rechazos firmes

Los rechazos firmes (hard declines) se producen cuando el emisor de la tarjeta rechaza el pago. Por ejemplo, cuando se intenta usar una tarjeta caducada o cuya pérdida o sustracción se han denunciado. Los rechazos firmes son permanentes y no admiten nuevos intentos de pago.

La gran mayoría de los rechazos son rechazos parciales (soft declines). Estos ocurren por una gran variedad de motivos, como la necesidad de autenticar mejor al titular de la tarjeta porque se trata de una compra atípica, o por problemas técnicos o de infraestructura al procesar el pago. Los rechazos parciales son temporales, ya que permiten a los comercios procesar de nuevo la operación siempre que se subsanen los errores que llevaron al rechazo inicial.

PREGUNTA 4

¿Debe mi empresa pedir la exención para esta operación?

El hecho de que una operación pueda estar exenta no obliga a tu empresa a pedir la exención. Además, las exenciones no están garantizadas. La solicitud de exención se envía al emisor y en última instancia es este quien decide si acepta la exención o rechaza la operación.

Una buena estrategia de exenciones es aquella que se adapta a las características propias de la operación y también considera, entre otros aspectos, la naturaleza de los bienes o servicios vendidos, la cartera de clientes, los países en los que opera el comercio y el apetito por el riesgo de la empresa.

Los comercios pueden solicitar al emisor la autenticación para las operaciones de alto riesgo o incluso para todas ellas y aprovechar así la inversión de responsabilidad de 3DS en caso de fraude. También podrían elegir esa opción porque venden productos muy caros, el valor de sus operaciones es superior a la media o quieren entrenar a sus motores de fraude para documentar las políticas de exenciones del futuro, entre otros motivos.

Si un pago se autentica mediante los protocolos de 3D Secure —y el emisor autoriza la operación— el comercio se beneficiará de la inversión de la responsabilidad prevista en la normativa de PSD2, lo que puede reducir en gran medida el número de solicitudes de devolución que reciben los comercios.

Sin embargo, hay que encontrar un equilibrio entre la seguridad y comodidad del cliente y el apetito por el riesgo y la responsabilidad de la empresa, por lo que el punto óptimo de cada una será único y deberá revisarse continuamente.

Una estrategia no puede ser buena si no lleva aparejada una buena implantación, que debería ser localizada y tener en cuenta la adopción de la SCA por parte de los emisores, los casos prácticos relevantes y la experiencia. Tu proveedor de servicios de pago debe estar al corriente de los avances en el sector y de la implantación de SCA en los mercados clave y objetivo. También debe ayudarte a adaptar tu estrategia de SCA para optimizarla, no para limitarse a cumplir la normativa.

La buena noticia es que no hay una única forma correcta de diseñar una estrategia de exenciones. Cada empresa puede personalizar y modificar su método con el tiempo para lograr una ventaja competitiva dependiendo del equilibrio que alcance entre la optimización de la experiencia del cliente, el aumento de los ingresos y la minimización de las pérdidas provocadas por el fraude.

Sí, ve a la pregunta 5

No, ve a la pregunta 5

Explica

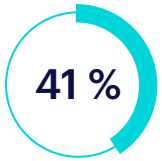
De las percepciones sobre la implantación de la SCA a la realidad

A mediados de 2021, Checkout.com preguntó a las empresas cómo les había afectado la autenticación reforzada de clientes.

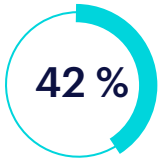
Cerca del 80 % de las empresas minoristas respondieron que SCA había tenido un impacto positivo en sus devoluciones y en la confianza de los consumidores o bien se reservaron su opinión porque consideraban que era demasiado pronto para conocer el efecto, ya fuera positivo o negativo, en los índices de aceptación. Solo el 12 % de los comercios electrónicos indicaron que sus índices de aceptación se habían visto afectados de forma negativa.[5]

Resulta alentador que los mercados europeos no se hayan hundido tras la aplicación de la SCA el 30 de diciembre de 2020. La inquietud por estar asomándose «al borde de un precipicio» que iba a llevar a un abandono masivo de los pagos por parte de los consumidores y a rechazos generalizados al procesarlos no se materializó. Según informa Visa, el 92 % de los 10 000 comercios electrónicos de mayor calado en Europa han usado alguna versión de 3DS y el 86 % de ellos han usado la versión EMV 3DS 2.x.[6]

Impacto que los comercios electrónicos consideran que ha tenido SCA en su empresa



Consideran que SCA tendrá un impacto positivo en las devoluciones y la confianza de los clientes



Consideran que es muy pronto para saber el impacto que tendrá SCA en el índice de aceptación

Consideran que sus índices de aceptación se han visto afectados de forma negativa por la SCA

Un análisis de la ABE puso de manifiesto que a finales de abril de 2021 el 94 % de los pagos con tarjeta de la UE tenían habilitada la autenticación reforzada de clientes (un incremento del 7 % desde finales de 2020) y que el 99 % de los comercios de la UE podrían admitir SCA, con una media del 96 %. Sus datos también indicaron que el 87 % de las operaciones iniciadas por los comerciantes y el 92 % de las solicitudes de autenticación se ajustaban a los requisitos de la SCA.[7]

[5] Checkout.com, The New State of Retail Report, 2021

[6] The Payments Association, The Long and Winding Road to SCA, 2021

[7] ibid.

PREGUNTA 5

¿Quiere mi empresa gestionar el plan de SCA por su cuenta?

RESPUESTA

No

No todas las empresas cuentan con el presupuesto ni los recursos internos necesarios para hacerse cargo de su estrategia de SCA. Por eso, elegir un socio de pagos que se anticipe a cualquier cambio en su nombre es una buena medida para las empresas de este tipo.

Los proveedores de servicios de pago ofrecen varias soluciones preexistentes de SCA que se basan en parámetros establecidos de antemano, como pueda ser la integración para las páginas alojadas y las herramientas de gestión automática de las exenciones. Estas soluciones son ideales para los comercios electrónicos que buscan minimizar el trabajo de desarrollo y los plazos de ejecución.

RESPUESTA

Sí

Las empresas que tienen la capacidad de asumir la tarea pueden desarrollar integraciones técnicas más complejas para la SCA, sobre todo las organizaciones empresariales. Estas aprovechan la última versión del protocolo EMV 3DS para conseguir un mayor control y visibilidad de la experiencia de autenticación del cliente. Eso permite, a su vez, reducir las fricciones en los pagos y el abandono de las compras en línea.

Las empresas pueden establecer sus propios parámetros para activar las solicitudes de exención de la SCA e irlos gestionando con el tiempo, o bien realizar estas tareas con ayuda de su proveedor de servicios de pago.

El desarrollo de tu estrategia de SCA en colaboración con un socio de pagos con amplios conocimientos del mercado local te permitirá acceder a gran cantidad de datos, tanto los propios como los del sector en general. Estos te ofrecerán una perspectiva mucho más clara para localizar realmente tu estrategia y optimizarla en función de tu propio perfil de riesgo.

Obtén una ventaja competitiva

Aumenta tu ventaja competitiva con una estrategia personalizada de SCA

Los pagos son la esencia de la economía digital y continúan siendo un componente clave para obtener ingresos y promover la innovación. La evolución de las tecnologías en este ámbito está facilitando la lucha contra el fraude y permitiendo ofrecer a los clientes la mejor experiencia posible.

La legislación contra el fraude lleva vigente el tiempo suficiente para permitirnos ver que está haciendo lo que prometía. Sin embargo, su impacto en las empresas no es homogéneo.

Además, las empresas deben mantener el ritmo de los cambios legislativos. Por ejemplo, la Comisión Europea está llevando a cabo una revisión de la legislación PSD2 en 2022, en la que se incluye la autenticación reforzada de clientes. Esta revisión se producirá a lo largo del año y podría resultar en propuestas de cambios del marco jurídico que regula la autenticación reforzada de clientes.

La cuestión para las empresas es encontrar el modo de implementar las normativas con el menor impacto posible en su proceso de pago y un efecto positivo en sus ingresos netos.

La respuesta pasa en parte por la tecnología, con el aprovechamiento de la última versión de EMV 3DS y los beneficios que esta ofrece, y en parte por los datos, por contar con la información suficiente acerca de sus clientes y las operaciones para minimizar los índices de fraude y las devoluciones. Finalmente, también depende de la toma de decisiones estratégica y basada en los datos para saber cuándo es mejor renunciar a la autenticación reforzada para evitar fricciones innecesarias en el recorrido del cliente.

Hay distintas maneras de afrontar la autenticación reforzada de clientes y tu proveedor de servicios de pago ideal debería ser capaz de colaborar con eficacia con tu empresa con independencia de la estrategia que hayas elegido. El trayecto para convertir un requisito normativo en una ventaja competitiva pasa por crear una estrategia a medida de las características de tu empresa.

Averigua si tu empresa está preparada con estas listas de comprobación

LISTA DE COMPROBACIÓN

Cómo prepararse para la SCA

Ahora que ya conoces los distintos aspectos que pueden influir en una estrategia para la autenticación reforzada de clientes, ¿qué debes hacer para conseguir una ventaja competitiva?

Estudia a fondo el protocolo 3DS

3DS seguirá evolucionando, por lo que te conviene dominarlo lo antes posible. Entre las versiones 3DS1 y 3DS 2.x se han producido avances considerables y aplicar la versión más reciente debería mejorar la experiencia de tus clientes. Un proveedor de servicios de pago de confianza debe ser capaz de informarte con tiempo de estos cambios y del efecto que tendrán en tu empresa.

Consigue los datos necesarios en el momento preciso

Averigua dónde se encuentran tus clientes y el dinero que gastan: necesitas saber si están radicados fuera del EEE o si se trata de operaciones exentas por haber superado un análisis del riesgo. Cuanta más información tengas sobre tus pagos, más fácil te resultará personalizar tu estrategia. El análisis en profundidad de los datos de tus pagos te servirá de guía para avanzar.

Desarrolla una estrategia de exenciones adaptada a tu empresa

Si a tu empresa le preocupan las fricciones en el proceso de pago, como a la mayoría, deberías aplicar exenciones. Puedes aplicarlas en los casos que recomienden los datos y adaptarlas al país, el tipo de clientes, el sector y el perfil de riesgo de tu empresa.

Decide cuál es el apetito por el riesgo de tu empresa

Las empresas que hayan detectado un incremento de las devoluciones pueden usar 3DS 2 para reducir las reclamaciones relacionadas con el fraude. Sin embargo, para saber hasta qué punto tu empresa debe recurrir a 3DS 2 con este fin tendrás que determinar tu perfil de riesgo para poder aplicarlo en el momento preciso y en las regiones adecuadas.

Colabora con tu proveedor de servicios de pago para mejorar constantemente el proceso de pago

Si cuentas con la información y el apoyo necesarios, tu empresa podrá desarrollar una estrategia que minimice el fraude y aumente al máximo las conversiones, que te permita ganarte la confianza de tus clientes y optimizar tu proceso de pago.

Hay diversas maneras de implementar la autenticación reforzada de clientes conforme a la normativa pero con un efecto positivo en el negocio. Tu socio de pagos ideal dará con la estrategia más adecuada para las necesidades propias de tu empresa.

LISTA DE COMPROBACIÓN

Qué debes hacer si tu empresa está radicada fuera de Europa

Aunque los países europeos hayan sido los primeros en exigir algún tipo de autenticación reforzada de clientes, está claro que no serán los últimos. Otros países van por el mismo camino: por ejemplo, Brasil requiere la autenticación de factor doble en todas las operaciones electrónicas efectuadas con tarjetas emitidas en el país y Australia requiere la autenticación reforzada de clientes en los comercios con un índice de fraude que supere un umbral determinado.

Además, vivimos en un mundo globalizado en el que el comercio transfronterizo se está convirtiendo en la norma general. **En este contexto, ¿qué deben saber las empresas que radican fuera de Europa?**

Estate al tanto de los últimos cambios en 3DS y la autenticación de clientes

Colabora con expertos que estén a la vanguardia de los cambios que se producen en todo el mundo en materia de autenticación. Estos podrán ofrecerte sus conocimientos para que tengas la seguridad de que no se te escapa nada.

Contar con un socio con entidades locales en los lugares en los que haces negocios te permitirá anticiparte a cualquier cambio en las normativas locales.

Desarrolla una estrategia antifraude rigurosa

Visto el éxito que han tenido las empresas europeas en la reducción de las devoluciones con el uso de 3DS, puedes aplicar esta estrategia cuando el perfil de riesgo lo recomiende. Convertir 3DS en un componente de tu estrategia antifraude puede ayudarte a reducir las reclamaciones y a mejorar tus resultados.

Puedes utilizar 3DS para cotejar las operaciones de alto riesgo determinadas por los índices de fraude. Eso te permitirá prevenir determinadas devoluciones fraudulentas.

Localiza tu estrategia

Debes contar con una estrategia que aplique los métodos de autenticación de clientes cuando sea necesario, ya sea por motivos de cumplimiento o de riesgo.

Es importante utilizar un método de autenticación de clientes localizado para que tu estrategia se ajuste a los matices de cada método de pago, los índices de fraude de los distintos mercados y líneas de productos, y la actitud de los clientes. Las empresas de todo el mundo pueden recurrir a las licencias locales de su socio de servicios de pago en las distintas jurisdicciones para aplicar la autenticación reforzada de clientes en las regiones en las que es obligatoria.

La solución para tu empresa debería considerar las expectativas generales de los clientes y sus diferencias según el mercado. De ese modo, tu socio podrá adaptar con agilidad la estrategia para adaptarse a ellas.

Para obtener asesoramiento sobre la mejor estrategia de SCA para tu empresa, ponte en contacto con nuestro equipo de expertos en pagos.

checkout.com