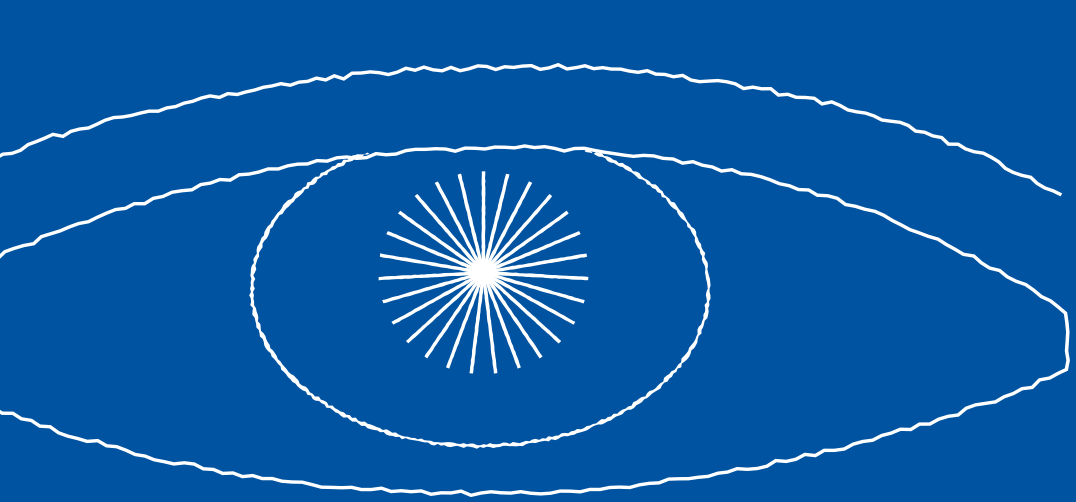
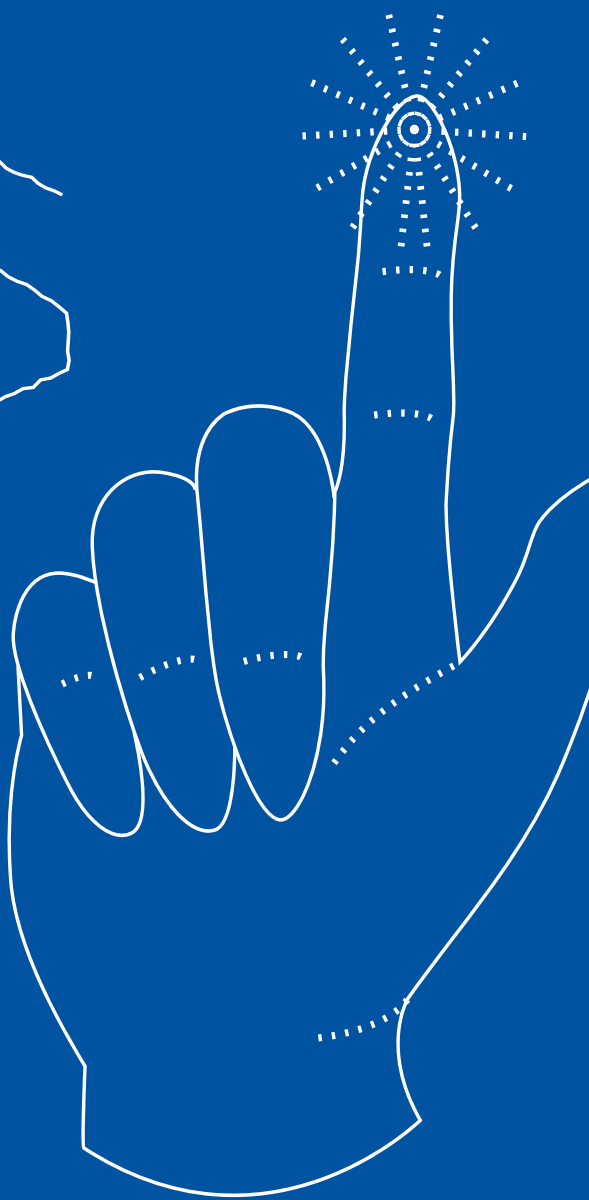
Guía completa sobre la Autenticación Reforzada de cliente (SCA)





GOCARDLESS

01.
Introducción a la Autenticación Reforzada de Cliente

Introducción a la PSD2

La PSD2 es la segunda Directiva sobre los servicios de pago europeos.

La directiva se basa en tres aspectos clave de la legislación introducidas por primera vez en la Directiva original de 2007. Dentro de los puntos importantes se incluye el aumento de los derechos de los consumidores a los pagos que permiten, mediante regulación, el acceso a la información de la cuenta de terceros y a una seguridad que está reforzada.

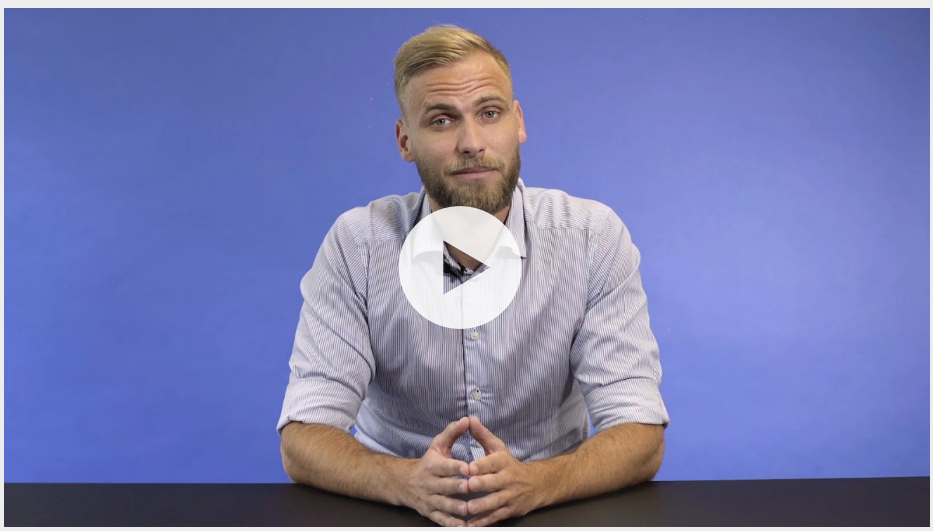
La seguridad reforzada se refiere al conjunto de requisitos denominados Autenticación Reforzada del Cliente (SCA) que implica en gran medida a cualquier empresa con presencia online.

Esta guía se adentra en la SCA, a quién y a qué afecta y cómo las empresas pueden prepararse para la entrada en vigor de los requisitos.

¿Qué es la SCA?

La Autenticación Reforzada de Cliente es un conjunto de requisitos reglamentarios, diseñados para hacer que el pago online sea más seguro y, en consecuencia, reducir el fraude en los pagos.

La SCA añade una capa adicional de seguridad cuando los clientes finales realizan un pago online. Hasta ahora, los compradores podían simplemente introducir sus datos de pago y completar su compra (aunque algunas empresas eligen voluntariamente solicitar una nueva autenticación).



¿Cómo funciona la SCA?

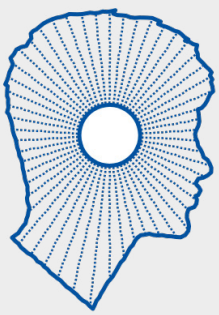
La SCA es una forma de autenticación de 2 factores diseñada para demostrar que los clientes finales son quienes dicen ser, con reglas específicas que constituyen la "Autenticación".

Es necesario dos formas de validación de las tres categorías disponibles.

¿Qué supone el método de Autenticación?

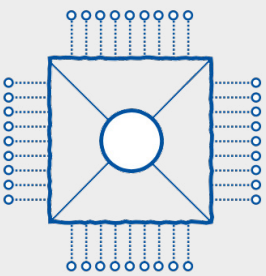
Existen tres categorías válidas para la autenticación disponibles como parte de la SCA. Dentro de cada categoría, hay una serie de métodos potenciales para satisfacer esa categoría.

Las tres categorías son:



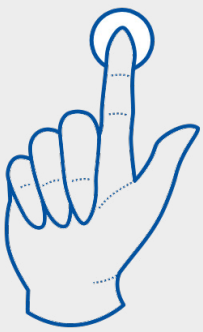
Conocimiento

(algo que solo el pagador sabe) - los ejemplos incluyen una contraseña, PIN, frase o información / respuesta secreta



Posesión

(algo que solo el pagador posee) - los ejemplos incluyen su teléfono móvil, reloj inteligente, tarjeta inteligente o token



Herencia

(algo que el pagador es): los ejemplos incluyen una huella digital, reconocimiento facial, patrones de voz, firma de ADN o su iris

Solo cuando el pagador haya proporcionado dos de estas formas de Autenticación, se les permitirá completar su pago.

El 21 de junio de 2019, la EBA (European Banking Authority) lanzó una nueva opinión sobre lo que puede constituir un elemento compatible de inherencia, posesión y conocimiento en cada una de las tres categorías. También estableció los requisitos adicionales sobre la conexión dinámica y la independencia de los elementos.

¿En qué transacciones se aplica la SCA?

La incorporación de la SCA se realiza para que la gestión del dinero y los pagos online sean más seguros y para reducir el fraude en estos procesos. En un nivel alto, se requerirá la SCA cuando un pagador transfiera fondos o acceda a la información de su cuenta.

En particular:

- Cada vez que un pagador accede a su cuenta de pago online
- Al iniciar una transacción de pago electrónico
- Al realizar cualquier acción a través de un canal remoto que pueda implicar un riesgo de fraude de pago u otro abuso

Es muy probable que el principal impacto sea sobre los pagos con tarjeta y las transferencias bancarias. La razón es que los pagos con tarjeta son instantáneos e iniciados por el cliente final,

y el pago o el consentimiento para acceder a los datos de la cuenta es instantáneo, lo que genera riesgos.

Existe una serie de exenciones donde ciertas acciones y transacciones no requerirán la SCA.

¿Se aplica la SCA a los pagos recurrentes?

Cuando los pagos son iniciados por el cliente final, la SCA solo se aplicará al primer pago en un conjunto de pagos recurrentes por la misma cantidad. Sin embargo, si éste cambia, entonces se aplicará la SCA.

Cuando los pagos son iniciados por el comerciante que recibe el dinero, la SCA generalmente (aunque no en el caso de las domiciliaciones bancarias estándar) se requerirá para el primer pago de una serie de pagos recurrentes. Mientras los pagos posteriores sean iniciados por el comerciante, no se requerirá la SCA adicional siempre que las cantidades que se cobren estén dentro de la expectativa razonable del cliente final.

Esto significa que las empresas de suscripción, las empresas de SaaS y las empresas de membresía deberán prepararse para la SCA.

Sin embargo, existen exenciones múltiples a la SCA, incluidas algunas que beneficiarán a las empresas con ingresos recurrentes.

Por qué se está implantando la SCA

La SCA es parte de la PSD2. Uno de los objetivos de la PSD2 es brindar protección a los consumidores.

Desde la implementación de la PSD original ha habido nuevos avances tecnológicos en el mercado de los pagos, que han visto un aumento de Terceros Proveedores (TPP). Estos TPP ofrecen formas nuevas e innovadoras de acceder a la información de la cuenta de los consumidores e iniciar pagos.

Sin embargo, abrir el acceso a las cuentas de los consumidores de esta manera supone un mayor riesgo de seguridad, y la compensación es una regulación estricta sobre cómo los TPP y los proveedores de servicios de pago obtienen acceso a estas cuentas.

En resumen, la SCA tiene como objetivo mejorar la seguridad de las transacciones online de los pagadores y reducir el fraude en los pagos.

El coste del fraude

La SCA está diseñada para reducir el fraude en las transacciones online, pero ¿cuál será su impacto?

La Europol ha estimado que el fraude con tarjeta no presente representó el 66% de los 144.000 millones de euros de transacciones fraudulentas con tarjeta en 2013. En 2016, el Banco Central Europeo (BCE) calculó que el coste total del fraude en pagos con tarjeta alcanzó los 18.000 millones de euros. Reino Unido, Francia y Dinamarca sufrieron las tasas más altas de fraude con tarjetas.

En España, el Banco de España señala que se registraron más de 590.000 operaciones fraudulentas con tarjetas bancarias por un importe de 40 millones de euros en 2017.

Cualquier reducción de la tasa de fraude podría suponer un ahorro significativo en toda Europa.

¿Dónde y cuándo entra en vigor la SCA?

La SCA (como parte de la PSD2) es un requisito a nivel europeo que se requerirá para cualquier transacción aplicable en la que tanto el proveedor de servicios de pago comercial como el proveedor de tarjeta o banco del pagador se encuentren dentro del Espacio Económica Europea (EEE). Si uno de éstos se encuentra fuera de Europa, el requisito es que el proveedor de servicios de pago en Europa realice sus "mejores esfuerzos" para aplicar la SCA.

Esto supone que si una empresa tiene su sede fuera del EEE; pero realizan pagos online a pagadores en el EEE, esas transacciones pueden estar sujetas a la SCA.

Es muy probable que la SCA continúe aplicándose en el Reino Unido, independientemente del resultado o el calendario de Brexit. La FCA ha dejado en claro sus planes: quiere que la SCA se siga aplicando. No ha habido ninguna sugerencia de lo contrario por parte de otros reguladores europeos.

El papel en la SCA de la Autoridad Bancaria Europea

La Autoridad Bancaria Europea (EBA) es una autoridad independiente de la UE que trabaja para garantizar una regulación y supervisión prudencial efectiva y coherente en todo el sector bancario europeo. Sus objetivos generales son mantener la estabilidad financiera en la UE y salvaguardar la integridad, la eficiencia y el funcionamiento ordenado del sector bancario.

La EBA ha publicado las Normas Técnicas de Reglamentación (RTS) que describen el mandato completo de la SCA para el EEE.

Sin embargo, las autoridades competentes de los países del EEE, como la FCA en el Reino Unido o BaFin en Alemania, serán responsables de hacer cumplir la SCA cuando entre en vigor.

¿Cuándo entra en vigor la SCA?

Actualmente, está previsto que la SCA entre en vigor en el Espacio Económico Europeo el 14 de septiembre de 2019.

Sin embargo, el 21 de junio de 2019, tras la presión de organismos de la industria de toda la UE, la EBA confirmó que los reguladores de la UE (como el FCA) pueden "trabajar con los PSPs y los stakeholders, incluidos los consumidores y los comerciantes, para proporcionar un tiempo adicional y limitado para permitir a los emisores migrar a enfoques de la autenticación que sean compatibles con la SCA".

Esto significa que algunos PSPs se les puede permitir una entrada posterior, también conocido como un período de "preparación operativa", durante el cual la FCA y otros reguladores no pueden tomar medidas para su aplicación.

El plazo general para cualquier demora en la implementación aún se está definiendo, pero se ha sugerido que durará aproximadamente 18 meses a partir de septiembre de 2019, la fecha prevista inicialmente para la entrada en vigor de los nuevos requisitos.

02.

Prepara a tu empresa para la SCA

¿Están preparadas las empresas online para la SCA?

A pesar de que la PSD2 se adoptó por primera vez en 2015 (aunque las Normas Técnicas de Reglamentación sobre la SCA no finalizaron hasta noviembre de 2018), las investigaciones sugieren que muchas empresas no están preparadas para la próxima fecha límite de la SCA.

En 2018, Mastercard encuestó a más de 300 negocios online y descubrió que el 86% de ellos aún no cumplían los requisitos de la SCA, mientras que el 75% ni siquiera estaba al tanto de la próxima legislación.

Un estudio de mayo de 2019 realizado por 451 Research asegura que solo el 15% de las empresas se sienten "extremadamente preparadas". Muchas de las que admiten no estar preparadas son pequeñas empresas; aunque el problema de la falta de preparación es mayor. Según esta investigación, solo el 19% de las empresas con más de 5.000 empleados se sienten extremadamente preparados, y solo dos de cada cinco empresas anticipan cumplir con la SCA antes de septiembre de 2019.

Al menos, hay indicios de que las empresas online están comenzando a tomar nota: la SCA ha sido un tema importante de conversación en el sector fintech y en eventos relacionado con los pagos como el Merchant Risk Council London 2019 y Money 20/20.

El potencial impacto de la SCA en la empresa

Mientras más empresas están empezando a descubrir la inminente legislación de la SCA que entrará en vigor en septiembre, muchas todavía están pensando cuáles serán los posibles efectos de la SCA. Aquí hay cuatro potenciales impactos de la SCA.

1 Caída de la Tasa de conversión

Para transacciones que requieren Autenticación, la nueva legislación significa pasos adicionales durante el flujo de pago. La fricción durante el pago puede aumentar considerablemente la probabilidad de que un cliente final potencial no complete una compra. El 69% de las compras se abandonaron en 2019 y el 27% de quienes abandonaron una compra lo hicieron porque el proceso fue "demasiado largo o complicado".

Hay exenciones disponibles para ciertos tipos de transacciones y otras tácticas generales que las empresas pueden implementar para reducir la fricción en el pago. La SCA probablemente reduzca las tasas de conversión para los negocios que no pueden equilibrar las nuevas medidas de seguridad con una experiencia de pago conveniente para los clientes finales.

En la India, la aplicación de una legislación similar supuso una caída de la tasa de conversión "nocturna" del 25% en todas las empresas afectadas.

2 El impacto económico de la SCA

Se espera un menor número de clientes completen las compras debido a que el nuevo proceso de Autenticación tenga un efecto en cadena en la economía europea. Las empresas europeas podrían perder aproximadamente 57.000 millones de euros en el primer año tras la implementación de la SCA.

3 Reembolsos al cliente final

Según el Consejo Europeo de Pagos:
"la PSD2 prevé que el pagador pueda reclamar el reembolso completo de su PSP en caso de un pago no autorizado si no existiera una medida como la SCA y si el pagador no actuó de manera fraudulenta".

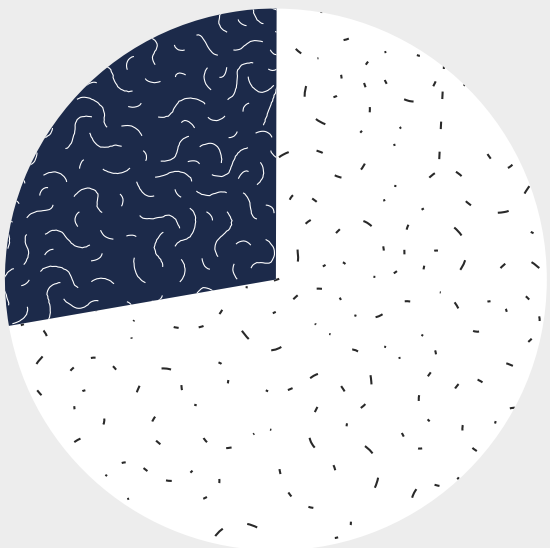
In En la práctica, esto significa que cuando el PSP de una empresa (por ejemplo, un adquirente de tarjeta) opta por depender de una exención (para no aplicar la SCA) o no implementa la SCA, serán responsables de cualquier fraude resultante. Cuando se aplica la SCA, esa responsabilidad puede transferirse a la parte que aplica la SCA, es decir, el PSP del pagador (por ejemplo, el emisor de la tarjeta). Cuando un comerciante obliga a su PSP (por ejemplo, un adquirente de tarjetas) a aplicar una exención específica, no hay nada que impida que el PSP y la empresa acuerden dónde

recae la responsabilidad, y esperamos que esa responsabilidad se transfiera a la empresa.

Redes de tarjetas como Visa han estado trabajando para actualizar sus reglas y reflejar estas disposiciones de responsabilidad.

4 Demanda de recursos

A corto plazo, cumplir con la SCA requerirá equipos de producto, legal, operaciones y finanzas en las empresas afectadas para ayudar a implementar los cambios. Si las empresas eligen comunicar las modificaciones a los clientes finales (encontrarás más sobre esto más adelante), también requerirá un esfuerzo por parte de marketing para que los mensajes calen de la mejor manera posible.



El 71% de las empresas creen que la carga para los recursos con el objetivo de implementar la SCA es "significativa".

Cómo implantar la SCA

En esta sección, analizaremos quién es responsable de la implementación de la SCA, y ofrecemos orientación sobre cómo las empresas afectadas pueden cumplir con los requisitos.

¿Quién es responsable de implementar la SCA?

Las empresas que realizan pagos online no son directamente responsables de cumplir con la SCA. Esa responsabilidad recae en los proveedores intermedios de servicios de pago (suponiendo que las transacciones online relevantes se encuentren bajo el mandato de ese proveedor) y en los bancos.

Para ser más precisos, el banco pagador es responsable de garantizar que las transacciones cumplan con la SCA (y denegar las transacciones que no cumplen con ello). Para hacer eso, debe recopilar la información de la Autenticación como se indica en el marco de la SCA.

Sin embargo, el banco necesita un lugar para recopilar esa información, y es donde entran los PSP. Deben capturar la información de forma segura, como parte del flujo de pago, y luego transmitirla de manera segura a los bancos utilizando mecanismos fiables para hacerlo. Así, los bancos tienen la última palabra sobre si esa transacción en particular cumple con la normativa.

Si bien es responsabilidad del PSP aplicar la SCA, puede haber dificultades prácticas dado

el grado de control que una PSP puede tener sobre las actividades o el cumplimiento de otro PSP. En última instancia, cada PSP debe garantizar su propio cumplimiento, lo que podría, en algunos casos, llevar a que los PSP de un pagador adopten un enfoque más severo que el que necesariamente ha sido en el pasado.

Sin embargo, el impacto de la SCA que ya hemos descrito, incluidas las posibles caídas de conversión, recae principalmente en las empresas.

Trabajar con un PSP preparado y proactivo sobre la SCA será fundamental.

Si quieres saber más sobre la SCA y las implicaciones que tendrá en tus pagos, estaremos encantados de atenderte.

No hay una forma obvia de que los PSP apliquen esto, aunque en el mundo de las tarjetas, el cumplimiento podría ser conducido a nivel de esquema al obligar a todos los comerciantes a usar 3D Secure 2.

Actualización del flujo de pago

El proceso de cumplir con la SCA significa un paso adicional durante el flujo de pago. Este será el cambio más obvio que verán tus clientes finales. Dependiendo del método de pago, este paso añadido puede ser muy obvio o casi imperceptible. Por ejemplo, los pagos móviles ya utilizan el escaneo de huellas dactilares o el reconocimiento facial para aprobar las compras, y éstas son aceptadas como "inherentes" medidas de Autenticación.

Como ya hemos mencionado, la SCA afectará principalmente a las transacciones de tarjetas de crédito y débito. Para actualizar tus flujos de pago en transacciones con tarjeta, 3D Secure 2 (3DS2) ha lanzado un método de Autenticación ampliamente compatible.

En un artículo reciente para Forbes, Jordan Mckee, Director de Investigación en 451 Research señaló que "las empresas que mejor integren la SCA en su flujo de pago y apliquen efectivamente las exenciones destacarán sobre el resto al minimizar el impacto en el cliente".

3D Secure 2

3D Secure (3DS) es un método de Autenticación implementado por primera vez por Visa, que se realiza de forma online en las compras con tarjeta de crédito y débito. Los clientes finales deben proporcionar una contraseña para completar la transacción de pago. Los negocios online normalmente obtienen acceso a 3D Secure a través de un PSP relevante.

3D Secure 2 (3DS2) es una nueva versión que cumplirá con las demandas de la SCA al:

- Introducir los requisitos de Autenticación, como, por ejemplo, exigir a los clientes finales que ingresen una contraseña, un código de acceso único o que proporcionen una autorización biométrica

- Permitir al emisor evaluar si aceptan o rechazan la transacción.

Sin embargo, es poco probable que las pruebas y la implantación de todas las partes finalicen completamente antes del 14 de septiembre.

El objetivo clave de 3DS2 es crear una "Autorización sin fricción" incluso ante las comprobaciones de seguridad adicionales requeridas por la SCA. Si la transacción se considera exenta, 3D Secure 2 debe omitir estas comprobaciones. Una mejora clave en comparación con el protocolo 3D Secure (3DS) original es la capacidad de realizar las comprobaciones necesarias sin redirigir desde la página de pago.

Problemas potenciales de 3D Secure 2
El 3D Secure (3DS) original estaba plagado de problemas para los comerciantes, incluida la temida caída de la conversión debido a los redireccionamientos mencionados anteriormente y la experiencia deficiente del usuario. Un estudio realizado por Ravelin aseguró que el 22% de todas las transacciones autenticadas con 3D Secure se perdían.

La nueva versión ha sido diseñada para minimizar los inconvenientes del original, incluida una mejor experiencia de usuario diseñada para usuarios de smartphones, requerirá una implantación más amplia para evaluar si ha tenido éxito.

Soporte 3DS2 y reconocimiento del consumidor
El éxito de 3D secure 2 gestionando las preocupaciones de conversión de la SCA dependerá de su adopción por parte de bancos y clientes finales. A pesar de la implementación inminente de la SCA, varios bancos aún tienen que comenzar a admitir el protocolo 3DS2.

En cuanto a los clientes finales, el uso del protocolo 3DS original se ha limitado en Europa. Según PYMNTS, a finales de 2017, solo el 50% de los clientes finales estaban inscritos y solo el 25% de las transacciones estaban verificadas.

Las Normas Técnicas de Reglamentación (RTS) de la SCA establecen que las especificaciones completas de lo que cubre exactamente la SCA y lo que se espera de los interesados. La versión final fue completada y distribuida por la Comisión de la UE en noviembre de 2018.

Gran parte de esta guía está dirigida a poner los aspectos clave de RTS en un lenguaje sencillo. Sin embargo, la versión original resulta de utilidad si quieres ver los detalles completos de la SCA.

La SCA y tus clientes

Si bien la SCA, sin duda, tendrá impacto en tu negocio, también será un cambio importante para los clientes finales que intentan realizar compras online. ¿Cómo se sienten sobre ello? ¿Les importa la seguridad añadida? ¿Conocen los cambios que vienen?

El conocimiento sobre el SCA del consumidor

Los bancos han comenzado a comunicar la SCA a las empresas (ejemplo 1, ejemplo 2), pero aún no han comunicado los cambios al consumidor final.

En España, menos de la mitad de los consumidores asegura tener un buen conocimiento de los próximos cambios como consecuencia de la SCA.

Equilibrio entre seguridad y conveniencia

Independientemente del conocimiento, ¿los clientes finales estarían dispuestos a perder parte de la conveniencia en las compras online permitiendo controles de seguridad más amplios con la aplicación de la SCA? Después de todo, el sistema de pedidos de 1 clic de Amazon es el proceso conveniente con el que se comparan el resto.

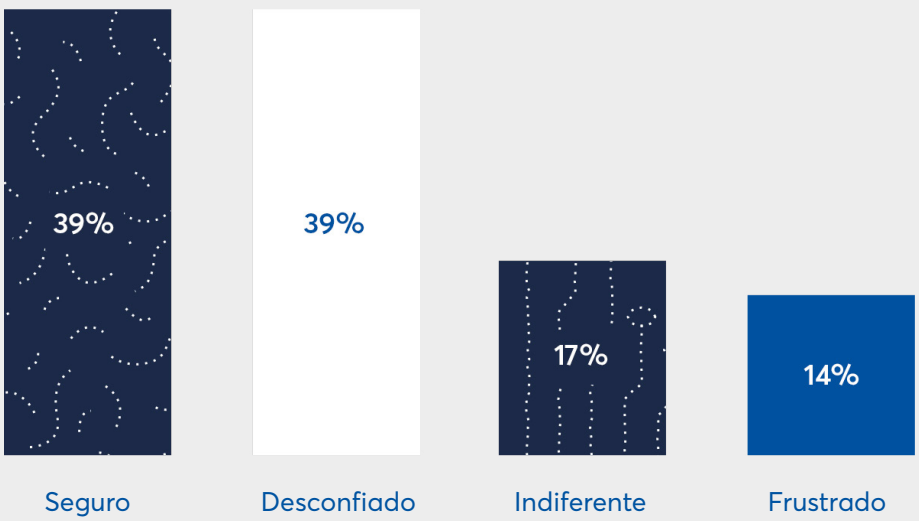
En un estudio realizado a 4.000 clientes de Reino Unido, Francia, Alemania y España se les preguntó acerca de sus actitudes respecto a la seguridad y la comodidad cuando compran online.

La encuesta también se interesó sobre cómo se sienten acerca de ciertos elementos específicos de los nuevos requisitos de la SCA, y cómo una mayor seguridad en el pago afectaría a su comportamiento de compra.

Los resultados revelaron una ligera preferencia por la seguridad sobre la conversión, con el 58% de los compradores priorizando la seguridad.

Sin embargo, cuando se les preguntó cómo se sentirían si se enfrentaran a procedimientos de seguridad complejos cuando solo compraban, la mayoría (54%) reconoció que sentirían desconfianza o frustración. Sólo el 39% aseguró que se sentirían más seguros.

¿Cómo te harían sentir procedimientos de seguridad complejos?

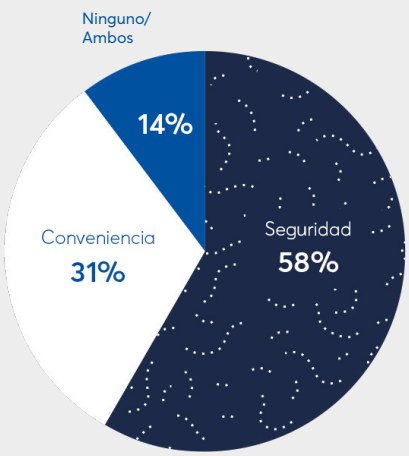


Encuesta a 4.000 compradores en línea en el Reino Unido, Francia, Alemania y España

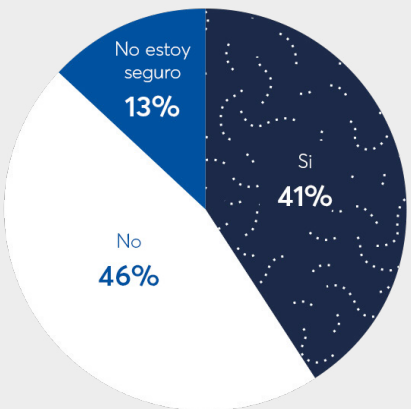
La encuesta también mostró que las actitudes hacia la seguridad y el comportamiento de compra real pueden ser muy diferentes. El 41% de los encuestados había abandonado previamente una compra online que era demasiado compleja, y casi una cuarta parte (24%) compraría menos en su marca favorita si la adquisición implicara medidas de seguridad adicionales.

Esta disonancia en las actitudes indica que el pensamiento de los clientes finales y cómo actúan son cosas diferentes. Pueden reaccionar positivamente a la idea de seguridad adicional, pero su comportamiento real, cuando se enfrentan con la SCA, podría ser muy diferente.

¿Qué es lo más importante cuando pagas de manera online?



¿Alguna vez has abandonado una compra debido a complejos procesos de seguridad?



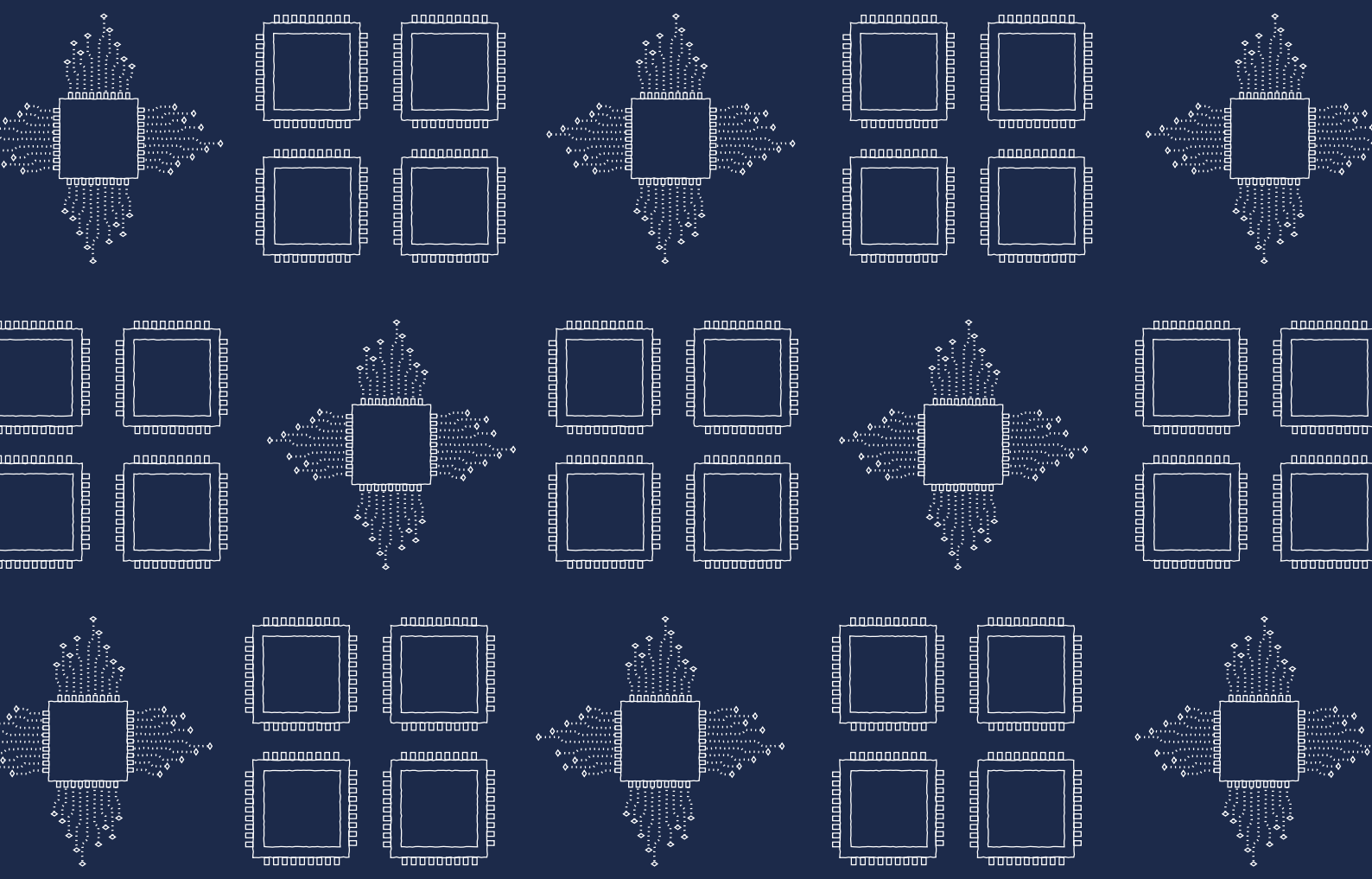
Encuesta a 4.000 compradores en línea en el Reino Unido, Francia, Alemania y España

Comunicando la SCA a tus clientes finales

A raíz de la legislación GDPR de 2018, muchos clientes finales recibieron una avalancha de correos electrónicos de empresas que les informaban sobre cambios en sus políticas de privacidad. El efecto combinado fue mal recibido por los clientes finales y muchos de los correos electrónicos eran incluso ilegales según la normativa GDPR.

Comunicar cualquier cambio importante a tus clientes finales está lleno de sus propios problemas. Si no comunicas estos cambios, ¿se confundirán cuando éstos surtan efecto? Si se comunica la SCA, ¿esto creará una preocupación innecesaria? También es muy difícil comunicar la naturaleza exacta de cualquier cambio cuando aún se encuentra en proceso de implementar nuevos flujos de pago y procesos de autorización.

03.
Exenciones claves de la SCA y transacciones fuera del ámbito de aplicación



Transacciones fuera del ámbito de aplicación

Transacciones fuera del ámbito de aplicación

Las transacciones fuera del ámbito de aplicación son aquellas que nunca fueron parte del mandato de la SCA en primer lugar y, por lo tanto, no requieren exención. Simplemente no necesitarán una Autenticación Reforzada de Cliente.

Un tipo de transacción clave que está fuera del ámbito de aplicación, especialmente para las empresas de suscripción y aquellas con ingresos recurrentes, son las transacciones iniciadas por la empresa:

Transacciones iniciadas por la empresa
Una transacción iniciada por una empresa es un pago que se realiza en una fecha acordada con el consentimiento del pagador y, como su nombre indica, es iniciado por la empresa que cobra el pago.

Si la transacción es iniciada por una empresa, los pagos fijos y variables estarán exentos de la SCA.

A diferencia de la mayoría de las transacciones iniciadas por los clientes finales, los flujos de pago de las transacciones iniciadas por la empresa a menudo no son instantáneos. Los datos del cliente final se recopilan en un momento determinado y se envían al banco del cliente final en otro momento.

La comunicación entre el cliente final, el banco y el proveedor de pagos no se produce en tiempo real. En el lenguaje de la SCA, esto se conoce como una transacción asíncrona. Sería poco práctico, y en algunos casos, imposible que la SCA se aplique a estas transacciones.

Sin embargo, ten en cuenta que algunas transacciones iniciadas por la empresa, como las transacciones recurrentes con tarjeta, la SCA aún tendrá que aplicarse al primer pago si se hace con la participación del PSP del pagador (por ejemplo, el emisor de la tarjeta).

Mandatos electrónicos de domiciliación bancaria "de forma digitalizada"

Un tipo de transacciones iniciadas por la empresa son las domiciliaciones bancarias electrónicas "de forma digitalizada " que no requerirán la SCA, incluso para el primer pago (siempre que cumpla con los criterios que se comentan a continuación). Esto es lo que GoCardless utiliza para configurar y cobrar los pagos.

Para cobrar los pagos recibidos mediante domiciliación bancaria, el cliente final del que se cobrarán los pagos debe facilitar un "mandato" de la empresa / PSP que recolecta dichos pagos.

Ha habido mucha confusión acerca de si el pagador requiere la SCA en el momento de la configuración del mandato, concretamente si la acción de establecer el mandato es una "acción a través de un canal remoto que puede implicar un riesgo de fraude de pago u otros abusos".

El 7 de junio de 2019, la EBA confirmó a través de su herramienta de Preguntas y Respuestas que no se requiere una Autenticación Reforzada de Cliente (SCA) para el establecimiento de mandatos electrónicos de Domiciliación Bancaria "de forma digitalizada" provistos a favor de las empresas beneficiarias, siempre que el PSP del cliente final (por ejemplo, un emisor de la tarjeta) no esté directamente involucrado en esa configuración.

En concreto, la EBA confirmó:

"Los mandatos otorgados por el pagador al beneficiario establecido sin la participación directa del PSP del pagador no están sujetos a la SCA."

Exenciones

Las exenciones de la SCA solo se aplican a los proveedores de servicios de pago. Ellos se relacionan con la cantidad de la transacción de pago, el riesgo del pago, la recurrencia de la transacción de pago y el canal de pago utilizado para la ejecución del pago. Incluyen:

Transacciones y suscripciones periódicas fijas

Cuando se utiliza un método de pago iniciado por el pagador, como las órdenes permanentes, solo el primer pago de una suscripción fija requerirá la SCA. Mientras la cantidad pagada permanezca igual, las transacciones adicionales no requerirán la SCA.

Sin embargo, si la cantidad cambia, como lo hacen muchas suscripciones basadas en el uso, se requerirá la SCA nuevamente para cada cambio.

Pagos Contactless

Los pagos contactless que cumplan con cualquiera de las siguientes condiciones estarán exentos de la aplicación de la SCA:

- Pagos individuales sin contacto por debajo de 50 €
- Cinco o más pagos por debajo de 50 €

Cuando se hayan realizado pagos acumulados por un total de 150€ desde la última aplicación de la SCA, se requerirá de nuevo.

La exención es específica para cada tarjeta utilizada, por lo que, para las cuentas conjuntas, la exención se aplica para cada tarjeta asociada a la cuenta.

Transacciones online por debajo de 30 €

Al igual que los pagos contactless (pero con un valor inferior), los pagos inferiores a 30 € también estarán exentos de la Autenticación Reforzada de Cliente.

Sin embargo, se requerirá la SCA si un cliente final hace:

- Cinco o más pagos por debajo de 30 €
- Si una combinación de pagos múltiples de bajo valor totaliza más de 100 €

Estos umbrales no son específicos de la empresa, es decir, esas cinco transacciones que suman hasta 100 € o más podrían ser pagos a diferentes compañías.

Beneficiarios de confianza (lista blanca)

Los clientes tendrán la opción de asignar empresas conocidas a una lista de 'Beneficiarios de confianza'.

Esta lista será actualizada y mantenida por el ASPSP (Proveedor de servicios de pago de servicio de cuentas), que también tiene autoridad para eliminar beneficiarios del fideicomiso. El PSP de una empresa puede crear mecanismos para "sugerir" beneficiarios de confianza al ASPSP en nombre del cliente final. Por ejemplo, Mastercard sugiere que, como cliente, pasa por un flujo de pago online, en la configuración del punto de pago, en el que puede haber una casilla de verificación que solicite que el cliente final agregue a la empresa a la lista de beneficiarios confiables de su ASPSP. Esta solicitud se pasará al ASPSP, que posteriormente requerirá que el cliente final pase por la SCA para aprobar la lista de beneficiarios de confianza. El cliente final también podrá administrar su lista de beneficiarios de confianza directamente con su ASPSP.

Es importante tener en cuenta que los ASPSP no necesariamente tienen que proporcionar la lista de beneficiarios de confianza, ya que pueden externalizar esto y, como resultado, empresas como Visa están desarrollando productos.

Si una empresa está en la "lista blanca" de un cliente final, la SCA no será necesaria, independientemente de la cantidad, la frecuencia o la variación de cualquier compra.

La forma de navegar

La forma de navegar por la SCA es atractiva; pero la aceptación del proceso por parte de los bancos ha sido hasta ahora irregular, y aún existen muchas preguntas sobre cómo funcionará exactamente en la práctica. Se sospecha que la inclusión en listas blancas no se convertirá en una táctica viable hasta mucho después de septiembre de 2019.

Sin embargo, es importante tener en cuenta que cada vez que se añada un beneficiario de confianza a una lista de exenciones, deberá aplicarse la SCA si se realizan cambios o un pago a un beneficiario de confianza; o si el PSP de una empresa solicita la eliminación de una lista.

Pagos Corporativos

Los pagos realizados directamente entre dos empresas estarán exentos de la SCA, pero solo si el método de pago utilizado es un método B2B como, por ejemplo, el acceso controlado a los servicios de gestión de viajes corporativos o sistema de compras corporativo.

De acuerdo con UK Finance: "No se requiere la SCA para los pagos iniciados con respecto a las personas jurídicas que utilizan procesos o protocolos de pago dedicados que están limitados a clientes finales que no son consumidores (por ejemplo, de host a host, algunos servicios SWIFT y algunos productos de tarjetas corporativas)"

Las RTS también se amplían exactamente en lo que se incluirá o no en esta exención:

- Espera que "el uso de redes corporativas restringidas de host a host (máquina a máquina) patentadas, tarjetas corporativas introducidas o virtuales, como las que se utilizan dentro de la gestión de viajes corporativos con control de acceso o el sistema de compras corporativas, posiblemente esté dentro del alcance de esta exención".

- El uso de tarjetas corporativas físicas emitidas a los empleados para gastos en circunstancias donde no se utiliza un proceso de pago y protocolo seguro (por ejemplo, donde las compras online se realizan a través de un sitio web público) no estaría dentro del alcance de esta exención

Exenciones en transacciones de bajo riesgo

Suponiendo que la SCA normalmente se aplicaría a una transacción, los proveedores de pagos tendrán la autoridad de evaluar las transacciones y elegirán no aplicar los protocolos de la SCA a aquellos que consideran con "bajo riesgo" de fraude.

Los proveedores de servicios de pago estarán sujetos a umbrales estrictos otorgándoles la capacidad de evaluar las tasas de riesgo de las transacciones en tiempo real. Las tasas de fraude del proveedor de pagos (en general, no solo para un comerciante específico) deben ser inferiores a los siguientes umbrales para el tipo de pago específico que se está utilizando y el valor de la transacción que se procesa:

Valor de umbral de exención (es decir, valor del pago que se está procesando)	Sistema de pago con tarjeta*	Transferencias de crédito*
500€	0.01%	0.005%
250€	0.06%	0.01%
100€	0.13%	0.015%

*La tasa de fraude no debe ser superior a estas cantidades para que se aplique la exención.

Tanto el PSP del beneficiario como el PSP del cliente final (por ejemplo, un emisor de tarjeta) pueden aplicar esta exención (según sus propias tasas de fraude generales para ese tipo de pago). Sin embargo, el ASPSP puede decidir si acepta o no la aplicación de esa exención. Así, por ejemplo, un adquirente de la tarjeta (el PSP de la empresa) puede aplicar la exención, pero el emisor de la tarjeta puede anular esa exención.

En la práctica, esperamos que la solicitud del PSP de la empresa sea válida, ya que la responsabilidad por cualquier pago fraudulento recaerá en el PSP que aplicó la exención.

Transporte y parking de terminales sin vigilancia

El pago de las tarifas de transporte o de estacionamiento en una terminal sin vigilancia no requiere la SCA.

Información de la cuenta de pago

Cuando un cliente final utiliza un TPP que proporciona servicios de información de cuenta para acceder a los datos de sus cuentas de pago, la SCA debe aplicarse al:

- Acceder al saldo de una cuenta de pago por primera vez
- Acceder a información más confidencial, como datos de todas las transacciones procesadas en una cuenta por primera vez

Sin embargo, la SCA no es necesaria aplicarla:

- Si se accede nuevamente al saldo de la cuenta
- Si se accede a los datos de transacciones históricos en los 90 días posteriores a la última aplicación de la SCA

Transferencia de Crédito

Para las transferencias realizadas entre, por ejemplo, una cuenta corriente a una cuenta de ahorros, donde ambas cuentas se mantienen en el mismo banco, por la misma persona, no es necesario aplicar la SCA.

Implantación de las exenciones de la SCA

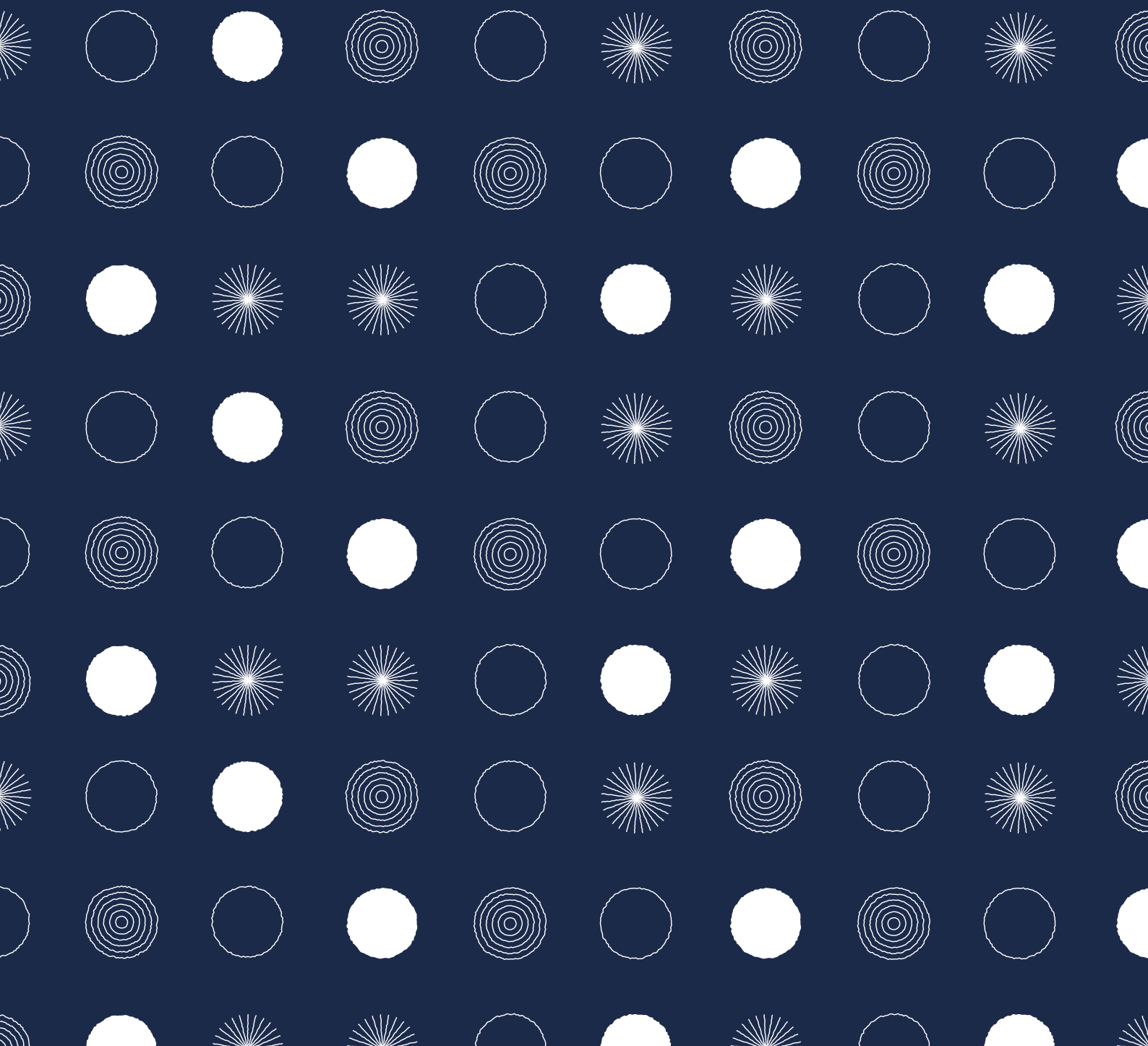
Estas exenciones de la SCA serán importantes para minimizar, o incluso eliminar, la fricción causada por el proceso de autorización adicional. Pero ¿cómo puedes asegurarte de que estas exenciones se activen cuando un cliente realiza una compra?

Para empezar, ¿se requerirá que los PSP y los ASPSP trabajen juntos y utilicen estándares comunes, por ejemplo, 3DS2?

¿Qué ocurre si la exención falla?

Si bien la lista de exenciones ahora es bastante clara, el banco del cliente final decidirá en última instancia si una exención es válida. Si no se concede una exención, el pago activará un código de rechazo. El pago deberá volver a enviarse y autorizarse mediante protocolos de Autenticación Reforzada de Cliente.

04.
GoCardless y la SCA



Esta sección proporcionará más información sobre cómo GoCardless se ha preparado para la legislación de la SCA y cómo estamos mejorando aún más la gestión de los pagos recurrentes en paralelo a esto.

¿GoCardless es compatible con la SCA?

GoCardless es totalmente compatible con la SCA. Nuestros clientes no necesitarán implementar ningún método de autorización adicional para los pagos que se realicen mediante GoCardless como resultado de la SCA.

GoCardless utiliza mandatos de domiciliación bancaria "de forma digitalizada", que están fuera del ámbito de aplicación de la SCA.

La EBA también ha confirmado que los mandatos de domiciliación bancaria "de forma digitalizada" no requerirán la SCA en ningún cobro de pagos, incluido el pago inicial.

En concreto, la EBA afirmó que:

"Los mandatos otorgados por el pagador al beneficiario establecido sin la participación directa del PSP del cliente final no están sujetos a la SCA."

La domiciliación bancaria digital no implica directamente al PSP del cliente final en la configuración.

Es importante tener en cuenta la confirmación anterior. Otros tipos de transacciones iniciadas por el comerciante (de las cuales la domiciliación bancaria digital es una de las formas), incluidas las transacciones recurrentes con tarjeta y los "mandatos electrónicos" también se consideran fuera del ámbito de aplicación de la SCA. Sin embargo, requerirán la SCA para cualquier pago inicial si hay una participación directa del PSP del cliente final en el momento de la configuración.

Protección adicional con la garantía de la domiciliación bancaria

Aunque no está directamente relacionado con la SCA, es importante tener en cuenta que las protecciones de garantía de domiciliación bancaria y reclamaciones de indemnización ofrecidas por los esquemas de pago de domiciliación bancaria de Bacs y SEPA (y protecciones similares que normalmente se ofrecen para los esquemas de domiciliación bancaria) reducen en gran medida el riesgo de fraude de pagos u otros abusos que impactan en al cliente final.

Cada uno ofrece protección a los clientes, en el sentido de que los clientes tienen derecho a revertir un pago realizado de manera fraudulenta o por error, después de que se haya cargado en su cuenta bancaria.

¿Qué deben hacer los clientes de GoCardless para prepararse para la SCA?

Para los pagos cobrados mediante GoCardless no se necesita realizar ninguna acción antes o después de la fecha límite del 14 de septiembre de 2019, porque, como ya se ha indicado, los mandatos de domiciliación bancaria "de forma digital" no están sujetos a la SCA. Sin embargo, si GoCardless es solo una parte de su combinación de pagos, debe consultar a sus otros PSP para ver qué cambios serán necesarios para preparar el resto de sus métodos de pago para los requisitos de la SCA.

Utilizar GoCardless para conseguir una ventaja competitiva de la SCA

Existen varias tácticas que las empresas pueden utilizar para minimizar el impacto de la SCA y proteger sus tasas de conversión e ingresos. Esto incluye aprovechar las exenciones e invertir en un producto como 3DS2 que minimice la fricción de la autenticación de dos factores, aunque esto no elimina completamente el riesgo de la caída de la conversión.

Dado que GoCardless es totalmente compatible con la SCA, utilizar GoCardless para cobrar tus facturas significa que no sufrirás el posible impacto de conversión que se avecina con la implementación de la SCA.

Utilizando el pago inteligente de GoCardless para detectar el fraude

La domiciliación bancaria es un método de pago de bajo riesgo con tasas de devolución mucho más bajas que las tarjetas. Estamos trabajando continuamente para mejorar aún más la seguridad; por ejemplo, estamos desarrollando un producto que ayudará a nuestros clientes a detectar (y contrarrestar) los intentos de fraude más fácilmente, mediante la aplicación de la información de pagos obtenida de millones de transacciones en nuestra red de más de 40.000 clientes.

Esto puede compararse con lo que se denomina Análisis de Riesgo de Transacciones en el mundo de la SCA, donde una empresa puede renunciar a los requisitos de la SCA si la tasa de fraude de su proveedor de pago está por debajo de cierto umbral.

Con esta nueva funcionalidad, GoCardless analizará cada transacción y ayudará a los comerciantes a detectar y detener los intentos de fraude, sin afectar la conversión.

La preferencia del cliente por la domiciliación bancaria

Además de ser siempre compatible con la SCA, GoCardless es el método de pago preferido para numerosos tipos de pagos recurrentes en toda Europa.

En una encuesta llevada a cabo recientemente por YouGov a alrededor de 12.000 clientes, se concluyó que la domiciliación bancaria era el método de pago más popular en cuatro tipos de compra (suscripciones online y tradicionales, cuotas, y facturas domésticas) en los seis mercados europeos encuestados (Reino Unido, Francia, España, Alemania, Dinamarca y Suecia), además de en otros mercados internacionales.

Además, en una encuesta de GoCardless a 4.000 consumidores en el Reino Unido, Francia, España y Alemania, el 52% aseguró que era probable o muy probable que pagara una suscripción mediante domiciliación bancaria si eso significaba que sería más sencillo.

¿Qué es GoCardless?

GoCardless ofrece una forma inteligente y escalable de realizar pagos, ayudando a las empresas a realizar automáticamente los cobros recurrentes de tus clientes en todo el mundo.

Ya estamos ayudando a que más de 40.000 empresas reciban sus pagos a tiempo.