

Strong Customer Authentication (Autenticación Reforzada del Cliente):

Guía de comunicaciones de *marketing* para comercios



Aviso legal

Te facilitamos esta presentación únicamente en tu calidad de cliente de Visa y/o participante en el sistema de pagos de Visa.

Al aceptar esta presentación, reconoces que la información aquí presente (la «Información») es confidencial y está sujeta a las restricciones de confidencialidad contenidas en las Normas de Visa u otros acuerdos de confidencialidad, que limitan su uso de la Información.

Te comprometes a mantener la confidencialidad de la Información y a no utilizarla para ningún otro fin que no sea en tu calidad de cliente de Visa o participante en el sistema de pagos de Visa. La Información solo puede ser difundida dentro de tu organización en función de la necesidad de conocerla para permitir tu participación en el sistema de pagos de Visa. Ten en cuenta que esta Información puede constituir información confidencial según las leyes federales de EE. UU. sobre acciones y que la compra o venta de acciones de Visa, en como consecuencia de disponer de esta información confidencial, constituiría una violación de las leyes federales sobre acciones aplicables en EE. UU.

Los estudios de casos, las comparaciones, las estadísticas, la investigación y las recomendaciones se proporcionan «TAL CUAL» y tienen por objeto únicamente fines informativos y no deben utilizarse para asesoramiento operativo, de *marketing*, jurídico, técnico, fiscal, financiero o de otro tipo.

Los productos y servicios descritos en este documento pueden estar sujetos a un mayor desarrollo y las fechas de lanzamiento de las características específicas son meramente indicativas. Visa se reserva el derecho de revisar este documento en caso necesario.

Como nuevo marco regulador en un ecosistema en evolución, los requisitos para la SCA aún necesitan ser perfeccionados para algunos casos de uso.

Este documento representa la interpretación de Visa, pero no debe tomarse como una posición definitiva ni considerarse como asesoramiento jurídico y está sujeto a posibles cambios en base a las orientaciones y aclaraciones de las autoridades competentes. Visa se reserva el derecho a revisar este documento a la espera de nuevos avances normativos. Animamos a nuestros clientes a que se pongan en contacto con Visa en caso de existir dudas relacionadas con las orientaciones facilitadas por las entidades reguladoras locales. Cuando proceda, Visa contactará de forma proactiva con las entidades reguladoras para intentar resolver estos asuntos.

Esta guía tampoco pretende asegurar o garantizar el cumplimiento de los requisitos reglamentarios. Los proveedores de servicios de pago son responsables de su propio cumplimiento de los requisitos de la SCA y se les anima a buscar el asesoramiento de un profesional competente cuando sea necesario.

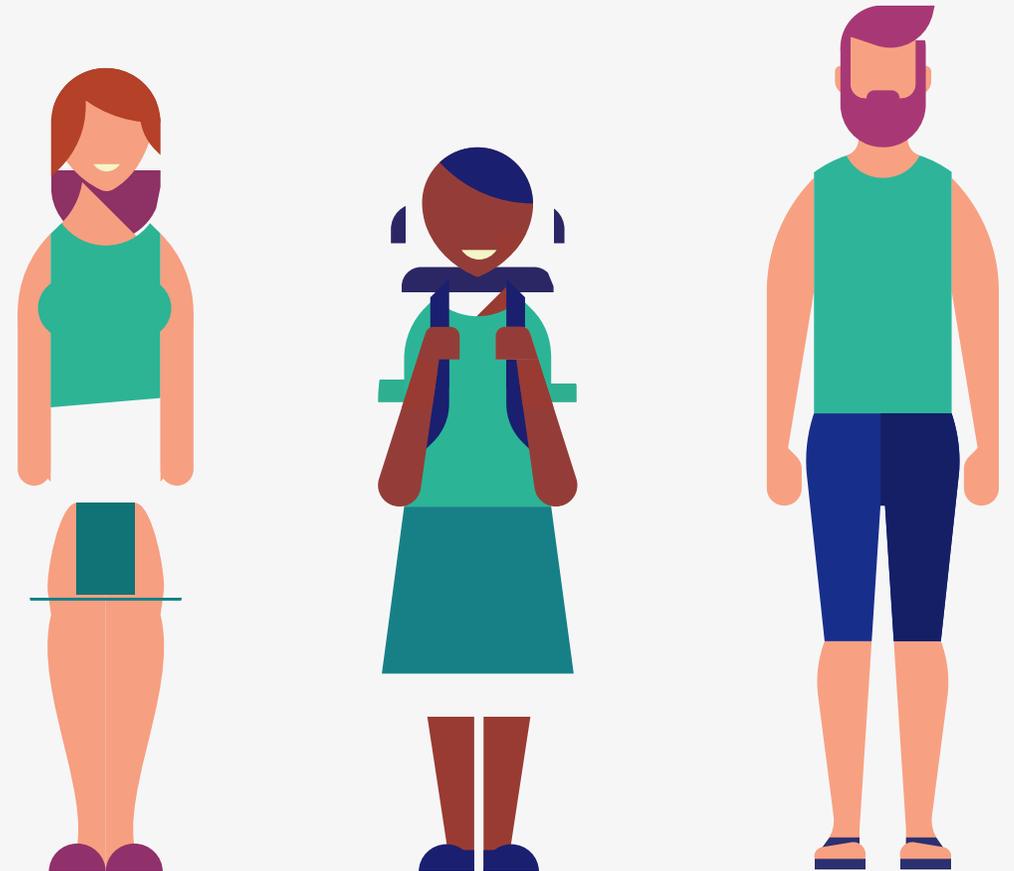
Te damos la bienvenida

Hemos creado esta guía para ayudarte a preparar tu negocio para el lanzamiento en toda Europa de la Strong Customer Authentication (SCA).

La SCA beneficiará a todos los que efectúen y acepten pagos con Visa. Esta nueva medida supondrá una reducción del riesgo de fraude y una mejora de la seguridad. Representará un adelanto tanto para las empresas (como la tuya) como para los clientes.

Esta guía incluye consejos y comunicaciones para ayudar a tu negocio y a tu personal a prepararse para los cambios y explica por qué es importante que te pongas en contacto con tu proveedor de servicios de pago (PSP).

También contiene materiales que te ayudarán a dar a conocer los cambios a los clientes en tu sitio web y en los puntos de venta.



Contenidos

Entender la SCA

- 1.1 La SCA en pocas palabras
- 1.2 Autenticación de dos factores
- 1.3 El impacto potencial de la SCA para tu negocio
- 1.4 Lo que debes tener en cuenta sobre la SCA

Experiencia del cliente tras SCA

- 2.1 Qué supondrá la SCA para tus clientes
- 2.2 Experiencia online del cliente
- 2.3 Experiencia del cliente en el punto de venta

Poner en marcha la SCA

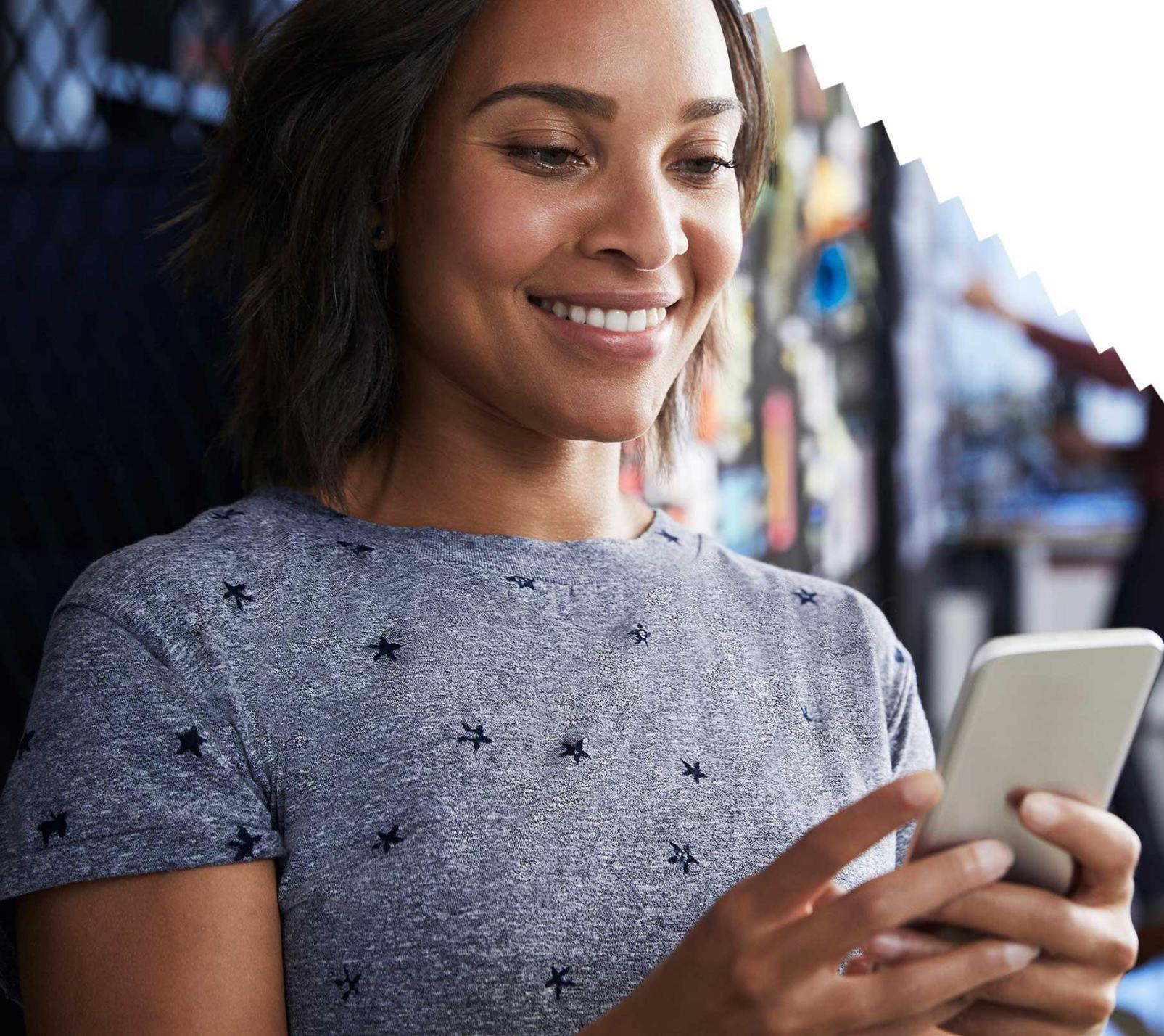
- 3.1 Habla con tu PSP
- 3.2 Aplicación para negocios online
- 3.3 Aplicación para negocios físicos
- 3.4 Aprovecha las exenciones
- 3.5 Transacciones no sujetas a la SCA (fuera del ámbito de aplicación)

Cómo informar a los clientes

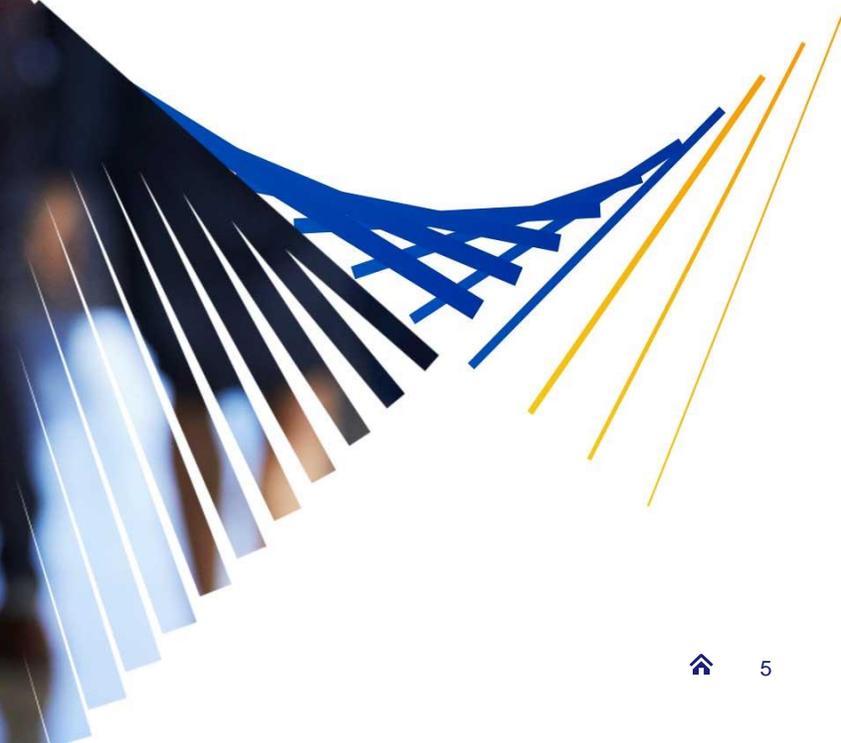
- 4.1 Cómo explicar la SCA a tus clientes
- 4.2 Guía de comunicaciones de *marketing* para negocios online
- 4.3 Guía de comunicaciones de *marketing* para negocios físicos

Apéndice:

Material de comunicación detallado



1. Entender la SCA



1.1 Introducción a la SCA

La Unión Europea está introduciendo nuevas medidas de seguridad denominadas SCA (Strong Customer Authentication), las cuales pueden cambiar la forma en que los clientes pagan online y en los puntos de venta al efectuar un pago Contactless con su tarjeta Visa.

Esta medida afectará a todas las empresas del Espacio Económico Europeo (EEE) que acepten pagos con tarjeta de crédito o de débito.

Las nuevas leyes introducen medidas de seguridad conocidas como autenticación de dos factores, las cuales ayudan a aumentar la seguridad de los clientes a la hora de efectuar transacciones de pago, incluidas las efectuadas en Internet y a través de la tecnología Contactless. Se trata de un cambio que afectará a toda la industria.

Asimismo, como parte de los cambios, los bancos contarán con más datos para tomar decisiones informadas sobre la necesidad de la autenticación de dos factores.

Las soluciones con respecto a SCA de Visa emplean la tecnología más avanzada para analizar el riesgo con mayor rapidez y facilitar una experiencia de pago perfecta.

El incremento de los niveles de seguridad y control beneficiará de forma directa a los clientes, ya que aumentará su confianza a la hora de efectuar sus compras online o en el punto de venta.

Visa está trabajando en colaboración con los emisores participantes y tu PSP para ayudar a proteger a los clientes contra el uso no autorizado de su tarjeta cuando compran online o en el punto de venta.

1.2 Autenticación de dos factores

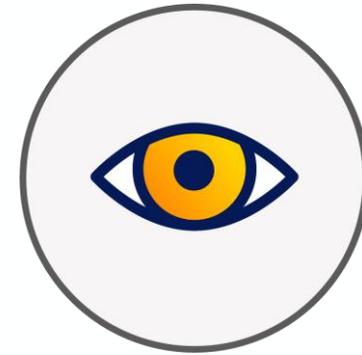
Tras la puesta en marcha de la SCA, es posible que tus clientes tengan que confirmar quiénes son mediante un paso de seguridad adicional al pagar con su Visa. Esto se conoce como **autenticación de dos factores**, por lo que es posible que tengan que proporcionar información de al menos dos de las tres categorías siguientes. La información que tendrán que proporcionar dependerá de los requisitos de su banco.



Algo que **saben**
como una contraseña o un PIN



Algo que **tienen**
como un teléfono móvil, un lector de
tarjetas u otro dispositivo



Algo que **son**
como un escáner del iris, un
reconocimiento facial o una huella dactilar

Tu PSP puede indicarte qué necesitas hacer para prepararte y cuáles son los plazos de aplicación. En la actualidad, diferentes organismos reguladores locales están estudiando estas cuestiones. Tu PSP también puede facilitarte información sobre los cambios en su sitio web.

1.3 El impacto potencial de la SCA para tu negocio

La SCA te ofrecerá una oportunidad a ti y a tus clientes para que los pagos sean aún más seguros y ofrezcan más protección contra el riesgo de fraude.

Si tu negocio está preparado para la SCA, puedes ofrecer a tus clientes una experiencia de pago rápida y sencilla con Visa, y de paso te beneficiarás de las próximas mejoras.

Qué supondrá la SCA para tu negocio:

La autenticación del cliente está en camino – Los bancos emisores de tarjetas prevén solicitar la autenticación del cliente en más transacciones.¹

Prepararse para la SCA – Un estudio de investigación reciente descubrió que solo el 15 % de las empresas se sienten «totalmente preparadas» para la SCA y solo el 40 % preveían estar preparadas para septiembre de 2019.²

Conseguir que la experiencia de tus clientes siga siendo perfecta para que vuelvan – El 52 % de los clientes que abandonan sus carritos sin completar la transacción compran en empresas alternativas con mejores experiencias y sistemas de pago.³

Ponte en contacto con tu PSP para comentar las mejoras que necesitas aplicar de cara a incorporar el nuevo proceso de autenticación en tu pasarela de pago de Visa. De esta forma, garantizarás el éxito continuado de tu negocio y te diferenciarás de tus competidores.

[1] Visa UK Authentication Steering Group; Feb 2019.

[2] The impact of SCA, 451 Investigación; Mayo 2019.

[3] The impact of SCA, 451 Investigación; Mayo 2019.

1.4 Lo que debes tener en cuenta sobre la SCA

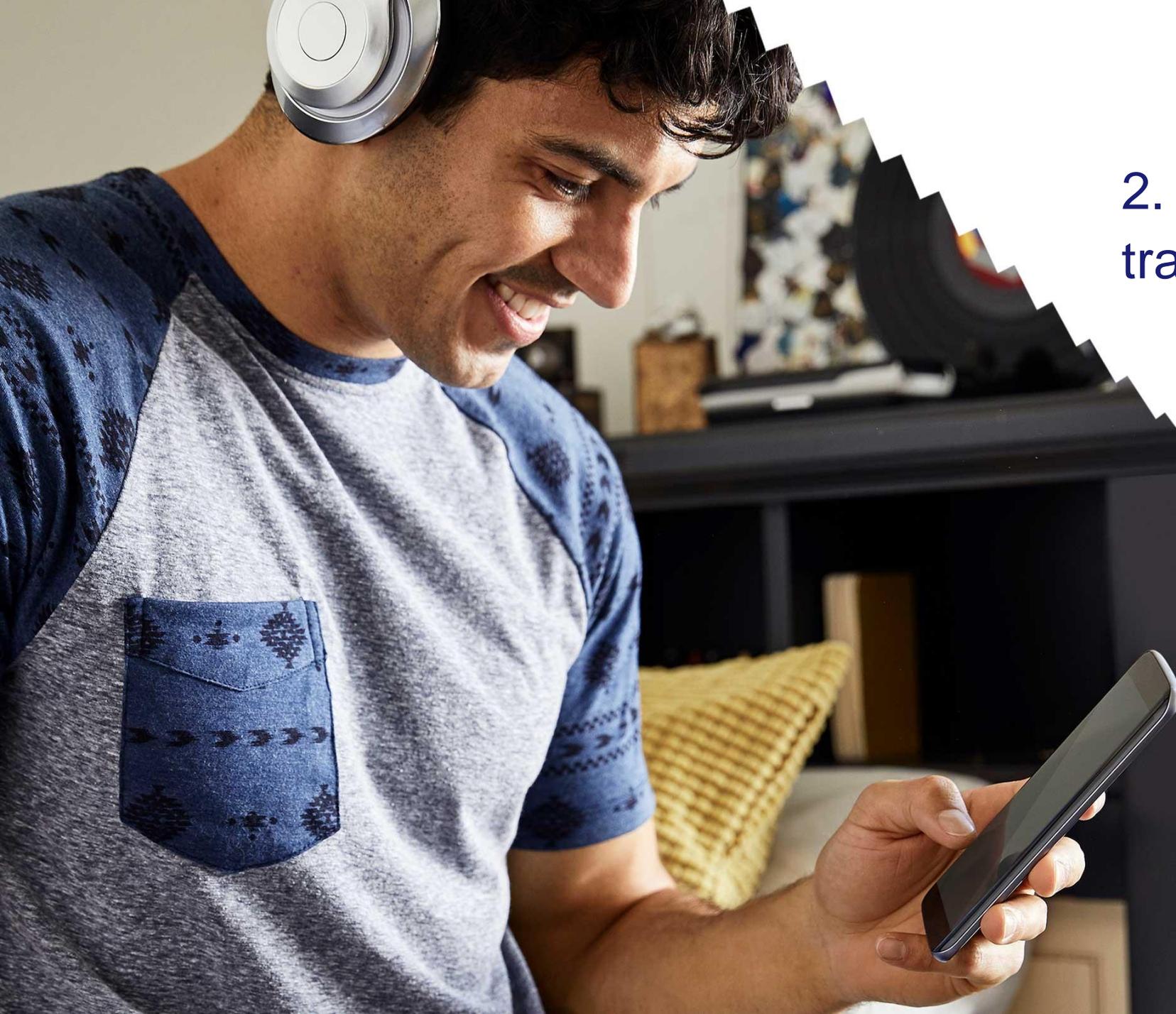
Mantén tu negocio en funcionamiento – Para continuar aceptando pagos con Visa en eCommerce y presencialmente gracias a la tecnología Contactless, de forma rápida y sencilla una vez se haya puesto en marcha la SCA.

Podrás estudiar con tu PSP las mejoras que necesitas, como recurrir al sistema 3DS, aprovechar al máximo las exenciones o actualizar tu terminal de punto de venta. De este modo, podrás optimizar la experiencia de pago de tus clientes y aprovechar al máximo las oportunidades que ofrece la SCA.

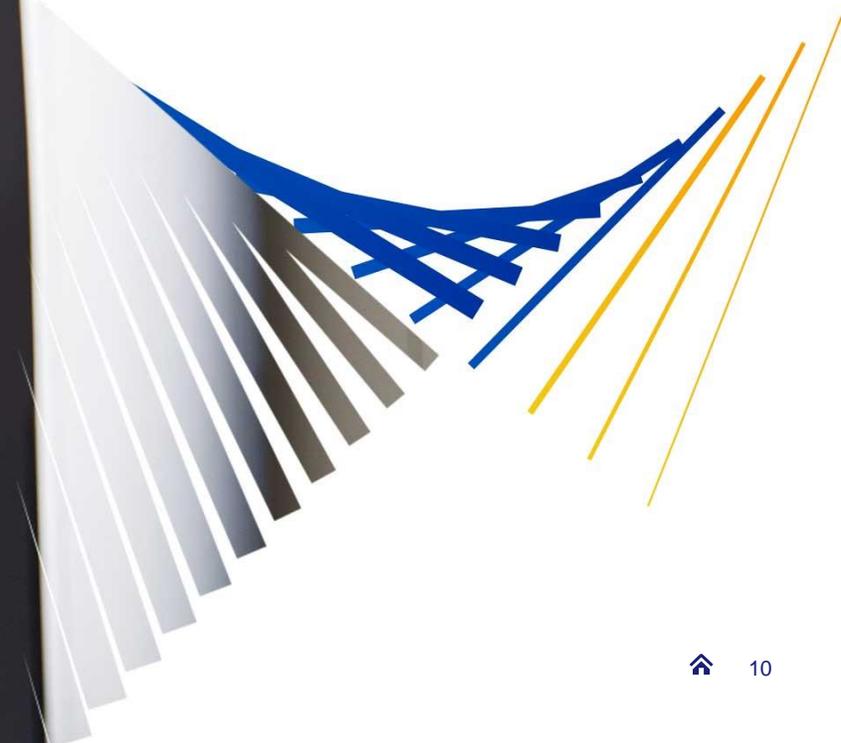
El compromiso de Visa por mejorar la información sobre la SCA
– Para ayudarte a comunicar a tu personal las próximas mejoras de la SCA y sus beneficios, hemos adjuntado una serie de comunicaciones a esta guía.

Una experiencia del cliente perfecta – Al comprender lo que significa la SCA, puedes garantizar una experiencia de pago sin complicaciones para tus clientes y asegurarte de que sigan contando contigo.

**Ponte en contacto con tu PSP hoy
y asegúrate de que tu negocio está preparado para la SCA.**



2. Experiencia del cliente tras la SCA



2.1 Qué supondrá la SCA para tus clientes

Una vez la SCA haya entrado en vigor, tu negocio y tus clientes se beneficiarán de unos mayores niveles de seguridad y de un menor riesgo de fraude.

La SCA tiene como objetivo ayudar a los comerciantes a mejorar la seguridad de las transacciones y optimizar la experiencia del cliente con un mayor número de ventas completadas. Para los clientes, se trata sobre todo de proporcionarles la tranquilidad que necesitan gracias a una mayor protección contra el fraude y a un sistema de pago más perfecto.



2.2 Experiencia del cliente en línea

Online, para pagos en Internet

A continuación, te mostramos cómo efectuarán los pagos con Visa tus clientes cuando se requiera la doble autenticación.

Es posible que los clientes tengan que confirmar su identidad al efectuar un pago a través del método de autenticación elegido por su banco. Para ello, proporcionarán información de al menos dos de las tres categorías que figuran a continuación (autenticación de dos factores):



Algo que saben – como una contraseña o un PIN



Algo que tienen – como un teléfono móvil, un lector de tarjetas u otro dispositivo



Algo que son – como un escáner del iris, un reconocimiento facial o una huella dactilar

2.2 Experiencia del cliente en línea

A continuación, te mostramos cómo efectuarán los pagos con Visa tus clientes cuando se ponga en marcha la SCA:

Paso 1

Un cliente desea efectuar una compra en Internet a través de su ordenador de sobremesa, portátil, teléfono móvil u otro dispositivo digital y se dirige a la página de pago del vendedor.

Consejo:

Si un cliente se pone en contacto contigo en relación con problemas de autenticación, remítele al emisor de su tarjeta para más información.

electronic
S T O R E

[Cart](#) > [Information](#) > [Shipping](#) > [Payment](#) > [Review order](#)

Review order

Contact	alexbmiller@example.com
Ship to	Alex Miller Unit 4, 22 Heather St Ashington Dublin 4 D07 E0322 Ireland
Method	Standard EU Delivery (2-3 days)
Payment	ending with 1234

Subtotal	€250.00
Shipping	€9.95
Total	€259.95

[Place order](#)

	(1) Smart Watch SW3	€259.95
Gift card or discount code		APPLY
Subtotal		€250.00
Shipping		€9.95
Total		€259.95

La tienda online es solo un ejemplo de comercio creado para mostrar el proceso de compra.

Este material no es un consejo legal u otro tipo de consejo profesional. Los proveedores de servicios de pago son responsables de su propio cumplimiento de los requisitos de PSD2 y de sus propias comunicaciones con los clientes. Este material debe leerse junto con la diapositiva 2. Esta guía ha sido publicada en septiembre de 2019.

2.2 Experiencia del cliente en línea

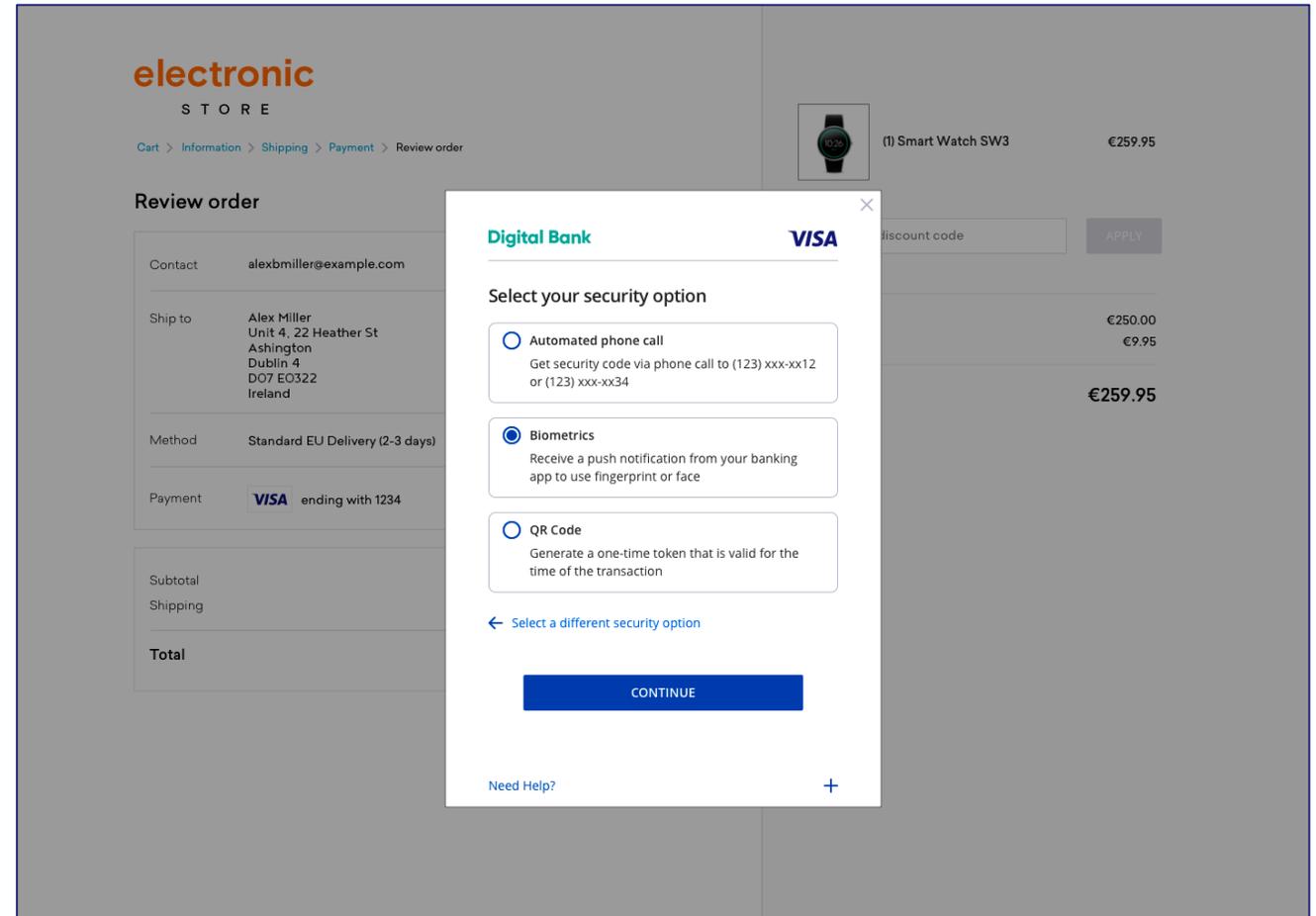
A continuación, te mostramos cómo efectuarán los pagos con Visa tus clientes cuando se ponga en marcha la SCA:

Paso 2

Para completar la transacción, pueden elegir su método de verificación o seguir el método elegido por el emisor.

Consejo:

Si un cliente se pone en contacto contigo en relación con problemas de autenticación, remítelo al emisor de su tarjeta para más información.



La tienda online es solo un ejemplo de comercio creado para mostrar el proceso de compra.

Este material no es un consejo legal u otro tipo de consejo profesional. Los proveedores de servicios de pago son responsables de su propio cumplimiento de los requisitos de PSD2 y de sus propias comunicaciones con los clientes. Este material debe leerse junto con la diapositiva 2. Esta guía ha sido publicada en septiembre de 2019.

2.2 Experiencia del cliente en línea

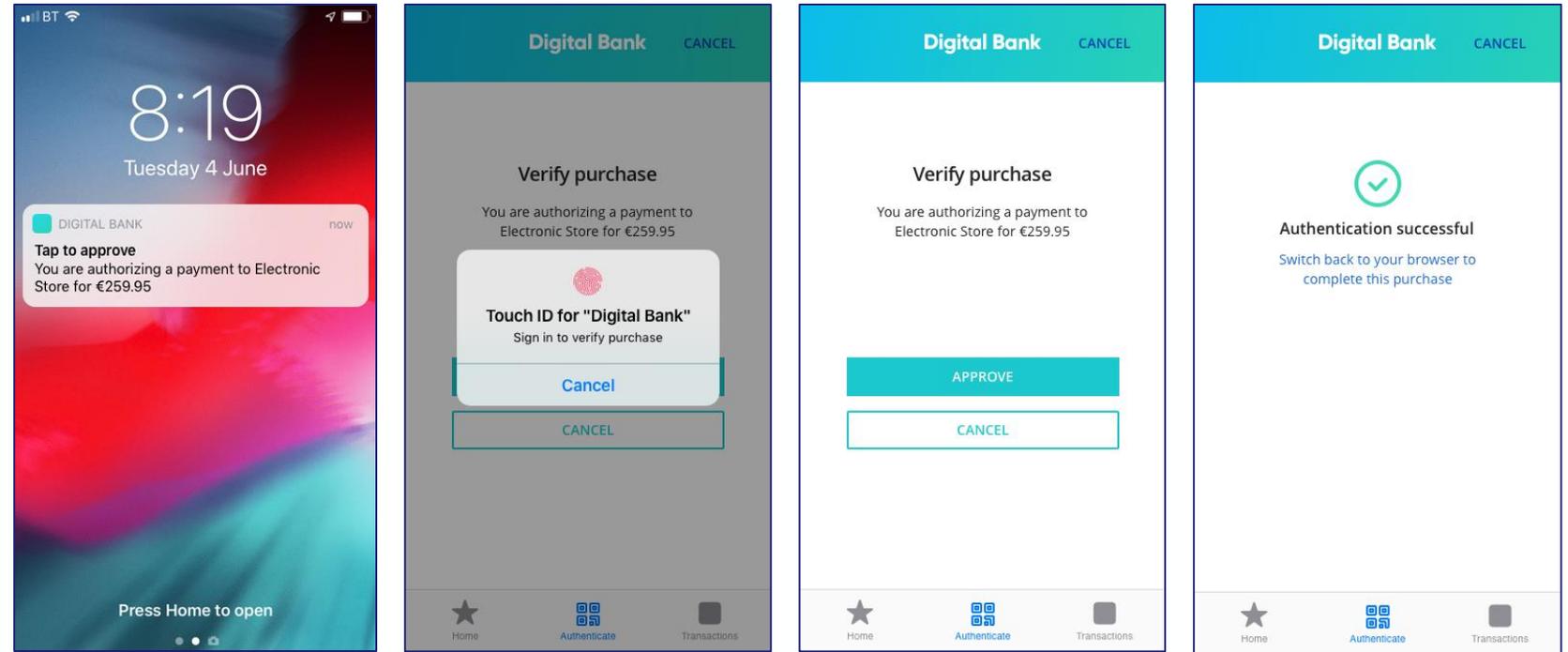
A continuación, te mostramos cómo efectuarán los pagos con Visa tus clientes cuando se ponga en marcha la SCA:

Paso 3

Basta con que sigan las instrucciones para completar su compra.

Consejo:

Si un cliente se pone en contacto contigo en relación con problemas de autenticación, remítelo al emisor de su tarjeta para más información.



La tienda online es solo un ejemplo de comercio creado para mostrar el proceso de compra.

Este material no es un consejo legal u otro tipo de consejo profesional. Los proveedores de servicios de pago son responsables de su propio cumplimiento de los requisitos de PSD2 y de sus propias comunicaciones con los clientes. Este material debe leerse junto con la diapositiva 2. Esta guía ha sido publicada en septiembre de 2019.

2.3 Experiencia del cliente en el punto de venta

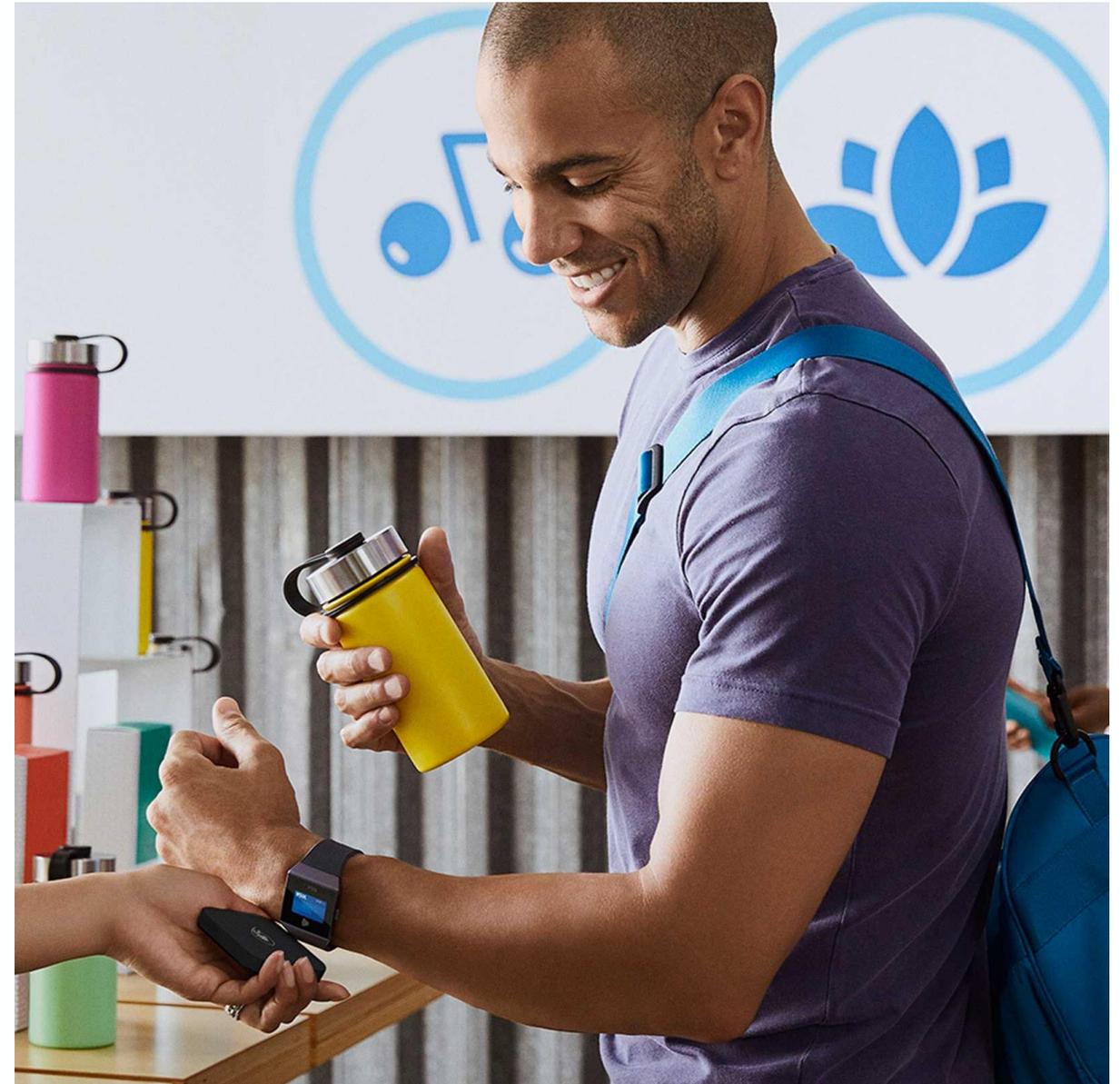
Es posible que los clientes tengan que introducir su PIN con más frecuencia en caso de pagos Contactless si:

- Los clientes hacen más de (5)** compras consecutivas mediante pago Contactless sin proporcionar autenticación.
- El valor acumulado de los pagos Contactless desde la última vez que se proporcionó la autenticación adicional supera los (150€)** en total.
- Un emisor desea verificar la identidad del cliente.

Consejo:

Si el cliente no puede completar la transacción Contactless después de introducir el PIN, pídele que introduzca su tarjeta y marque el PIN para efectuar el pago con el chip y el PIN.

Si el problema persiste, remítelo a su emisor, el cual podrá proporcionarle más información.



**Depende de la aplicación del emisor

3. Poner en marcha la SCA



3.1 Habla con tu PSP

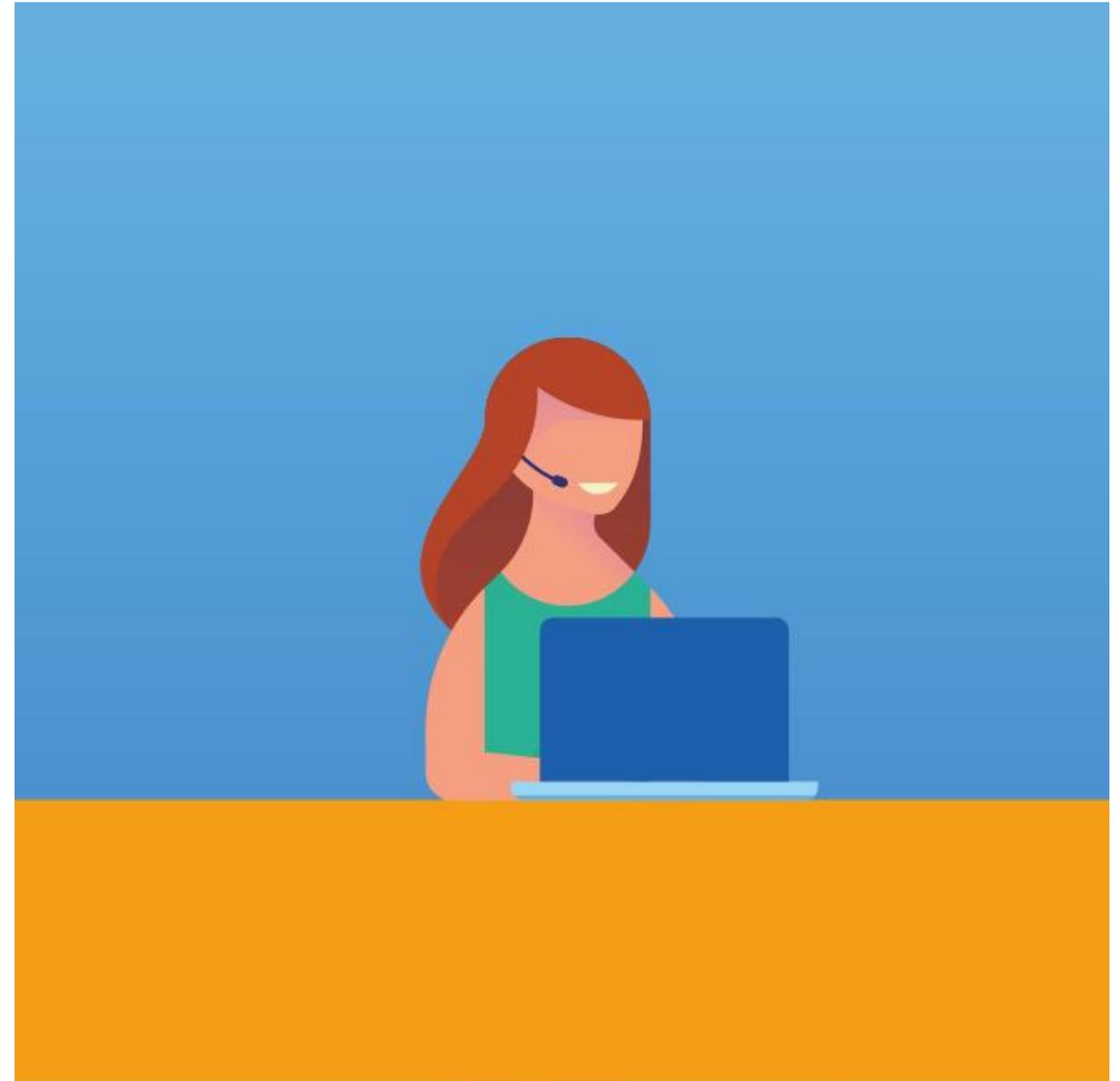
Los comerciantes como tú desempeñáis un papel fundamental en la reducción del fraude y en la mejora de la experiencia del cliente.

Por lo tanto, tu negocio debe estar preparado para que, en la medida de lo posible, la SCA evite que los bancos emisores rechacen transacciones.

Infórmate con tus PSPs sobre:

- qué tienes que hacer
- qué supondrá la SCA para tu negocio
- cómo proporcionar a tus clientes una experiencia de pago perfecta.

Las siguientes secciones explican qué aspectos debes comentar con ellos si tu negocio opera en Internet, en el punto de venta o en ambos y si deseas beneficiarte de las exenciones de la SCA.



3.2 Aplicación para negocios online

Debes hablar con tus PSPs para que te guíen a través de los cambios tecnológicos necesarios para procesar los pagos online.

Ponte en contacto con tus PSP:

Cuando hayas puesto en marcha el sistema 3DS a través de tu PSP, éste te proporcionará el distintivo «Visa Secure» (logotipo) para tu negocio en Internet.

Para ofrecer una experiencia de pago en línea excelente a tus clientes:

- Asegúrate de haberte inscrito para autenticarte mediante **3-D Secure (3DS)** – Visa ofrece este servicio a través de Visa Secure. Si no dispones de Visa Secure, es posible que tus clientes no puedan efectuar transacciones online.
- Comprueba que dispones de la versión más reciente de 3DS (la última versión es 3DS 2.2) para ofrecer la mejor experiencia al cliente, sobre todo en compras realizadas a través de teléfonos móviles y *smartphones*. Esto puede aportar grandes ventajas a tu negocio. Si no dispones de esta última versión de 3DS, te recomendamos que la actualices.

3.3 Aplicación para negocios físicos

Los pagos con chip y PIN en el punto de venta no sufrirán cambios. Para pagos Contactless es posible que se solicite a los clientes que introduzcan su PIN con más frecuencia.

Códigos de respuesta

En la actualidad, cuando tus PSPs procesan una transacción, envían a tu negocio un código de respuesta de dos dígitos del banco emisor para notificarte el estado del pago. De esta manera te indicará si el pago ha sido aprobado, rechazado o qué medidas debes tomar. Estos códigos de respuesta cambiarán tras la introducción de la SCA.

¿Cómo cambiarán los códigos de respuesta?

Durante el proceso de transacción, se activarán dos nuevos códigos de respuesta en las siguientes situaciones:

- Los clientes hacen más de (5)** compras consecutivas mediante pago Contactless sin proporcionar autenticación.
- El valor acumulado de los pagos Contactless desde la última vez que se proporcionó la autenticación adicional supera los (150€)** en total.
- Un emisor desea verificar la identidad del cliente.

Los PSPs controlan los nuevos códigos de respuesta. Si un emisor de cualquier país del EEE utiliza los nuevos códigos de respuesta, los PSPs y los comerciantes tendrán que estar preparados para garantizar que sus terminales son compatibles con estos nuevos códigos:

Código 70

1. **Código de respuesta 70** – se aplica a las transacciones online con PIN y solicita el PIN al cliente.

Código 1A

2. **Código de respuesta 1A** – se aplica a las transacciones con PIN en el punto de venta y se comunica con el terminal para cambiar la interfaz con el fin de insertar la tarjeta e introducir un PIN.

Ponte en contacto con tus PSPs

Te ayudarán a comprender mejor estos cambios.

**Depende de la aplicación del emisor

3.4 Aprovecha las exenciones

Ponte en contacto con tus PSPs

Descubre cómo tu negocio puede aprovechar las exenciones de la SCA y las transacciones que quedan fuera del ámbito de aplicación para ofrecer una experiencia de pago perfecta a tus clientes.

A continuación, presentamos algunos ejemplos de casos en los que los clientes no tendrán que utilizar la autenticación de dos factores para efectuar pagos.

- **Para pagos Contactless inferiores a (XX €)*** (No obstante, después de cinco transacciones consecutivas, o si el valor acumulado de los pagos Contactless desde la última vez que se proporcionó la autenticación adicional supera los (150€)*, es posible que tengan que introducir su PIN).
- **Pagos online de riesgo reducido.** Como parte de las nuevas medidas de seguridad, los bancos podrán tomar decisiones de análisis de riesgo de forma más eficaz y rápida, ya que dispondrán de datos más exhaustivos. La SCA no será necesaria si se determina que un pago online es de bajo riesgo mediante un análisis de transacciones en tiempo real.
- **Comercios de confianza.** Los titulares de tarjetas pueden añadir tiendas de confianza a una lista, de modo que no necesitarán utilizar la SCA cuando compren en esa tienda.**
- **Pagos corporativos.** Algunos pagos corporativos efectuados mediante procesos específicos podrían estar exentos si el organismo regulador local considera que son lo bastante seguros (por ejemplo, las tarjetas virtuales).

*Depende del límite de la tarjeta Contactless en el mercado local. (CVM - «Customer Verification Method» o Método de verificación del cliente).

**Pronto disponible en tu mercado. Infórmate con tu PSP.

3.4 Aprovecha las exenciones

Ponte en contacto con tus PSPs

Descubre cómo tu negocio puede aprovechar las exenciones de la SCA y las transacciones que quedan fuera del ámbito de aplicación para ofrecer una experiencia de pago perfecta a tus clientes.

(Continuación)

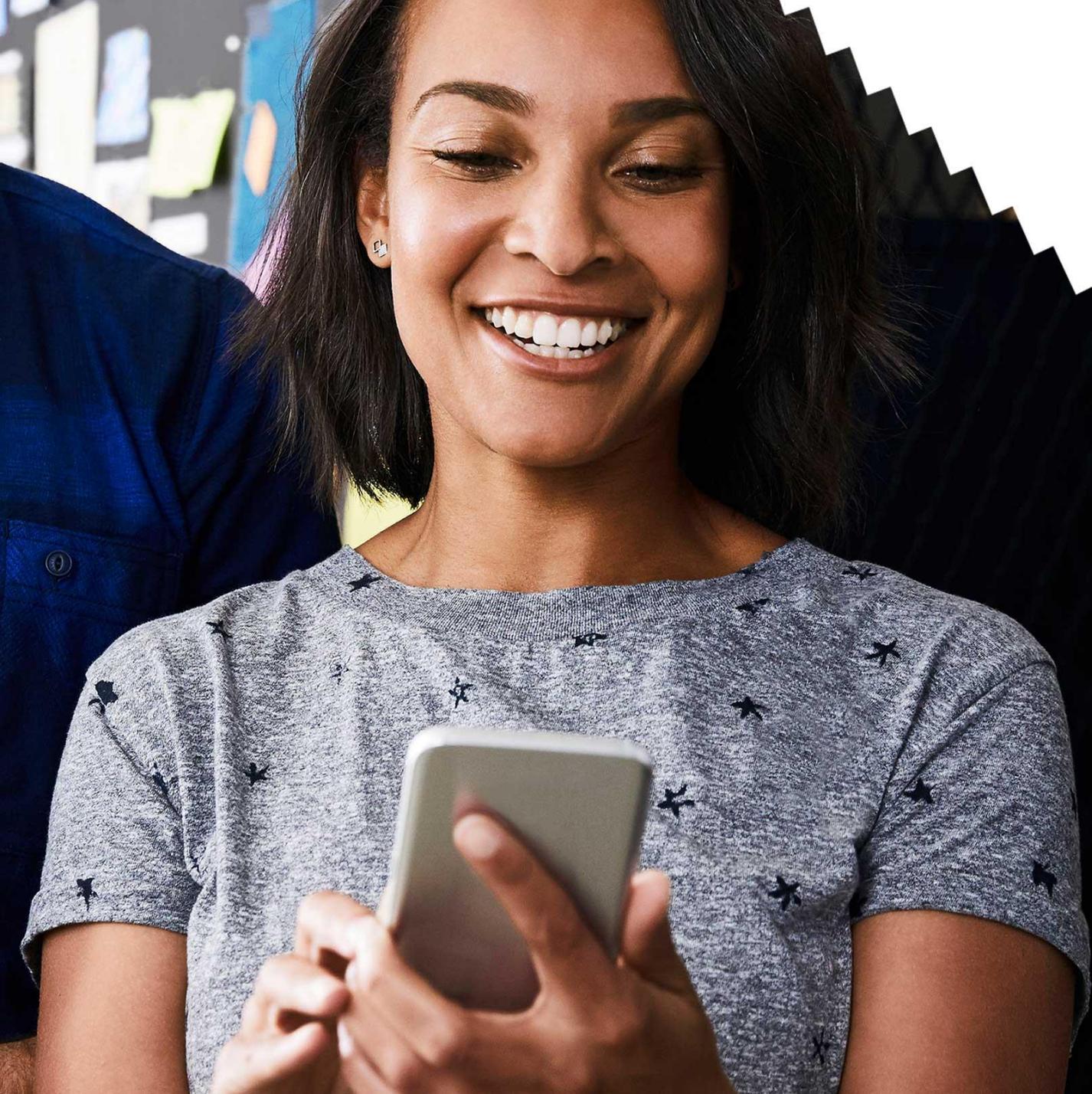
- **Pagos online de valor reducido.** Al igual que ocurre con los pagos Contactless, los pagos inferiores a (XX €) están exentos de la SCA. (No obstante, si se ha recurrido a la exención en cinco ocasiones desde la última autenticación satisfactoria del cliente, o si los pagos superan los (XX €), su banco podrá solicitar la autenticación).
- **Terminales de transporte y aparcamiento sin supervisión.** Los pagos de tarifas de transporte o aparcamiento en terminales sin supervisión (por ejemplo, en un aeropuerto o estación de tren) no requerirán la SCA**.

**Si un emisor pone en marcha una «Card-Based Solution», es posible que la SCA se active en algunos casos, para los que el titular de la tarjeta no podrá completar determinados requisitos de la SCA, como, por ejemplo, introducir su PIN.

3.5 Transacciones no sujetas a la SCA (fuera del ámbito de aplicación)

Existen transacciones en las que no se aplica la SCA. La lista que aparece a la derecha no incluye todos los casos. Consulta la página 2.

- **Transacciones iniciadas por el comerciante (MIT).** Entre ellas se incluyen las suscripciones y cuotas acordadas de antemano con el titular de la tarjeta e iniciadas por el comerciante. Cuando se configura una nueva suscripción o membresía, es posible que se solicite a los clientes una autenticación.
- **Pagos por correo/teléfono.** Los pagos efectuados por teléfono o por correo no requerirán una autenticación.
- **Una transacción en la que el banco o el PSP se encuentren fuera del EEE.** Tu banco tendrá que hacer todo lo que esté en su mano para aplicar la SCA en la medida de lo posible.
- **Transacciones anónimas.** Es posible que no se requiera la SCA si los clientes efectúan una compra con una tarjeta de prepago anónima, ya que, en estos casos, no es necesario que conozcas al titular de la tarjeta.



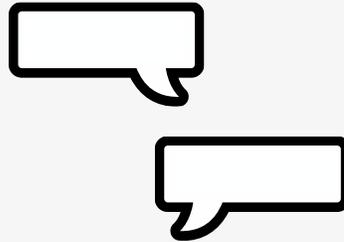
4. Cómo informar a los clientes



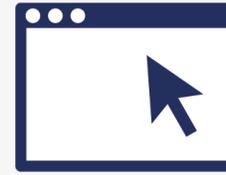
4.1 Cómo explicar la SCA a tus clientes

Para que la aplicación de la SCA se desarrolle con éxito, es fundamental que tanto tu personal como tus clientes conozcan las mejoras que se avecinan.

Hemos creado los siguientes recursos para ayudarte a explicar las mejoras a tu personal:



Una guía de conversación



Mensajería para el sitio web



Un manual para el personal con preguntas frecuentes

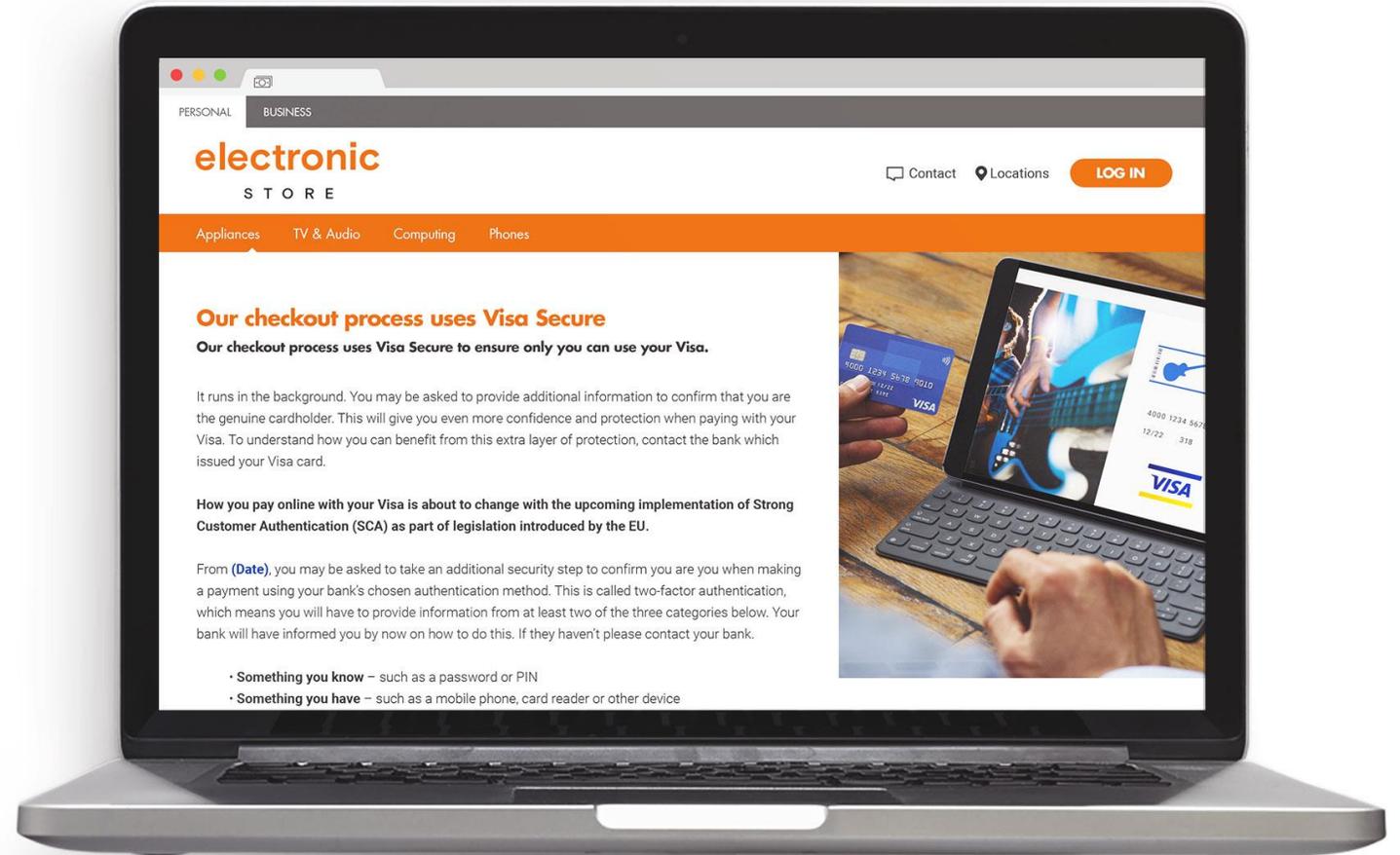
Estas herramientas contribuirán a que tu personal se sienta seguro y confiado con respecto a los próximos cambios de la SCA.

El banco emisor del cliente será el más indicado para proporcionar información detallada sobre la SCA, como, por ejemplo, acerca de las medidas antifraude y la seguridad de los pagos. Si tu cliente tiene consultas específicas con respecto a la SCA, asegúrate de que tus empleados están preparados para remitir al cliente a su emisor.

4.2 Guía de comunicaciones de *marketing* para negocios online

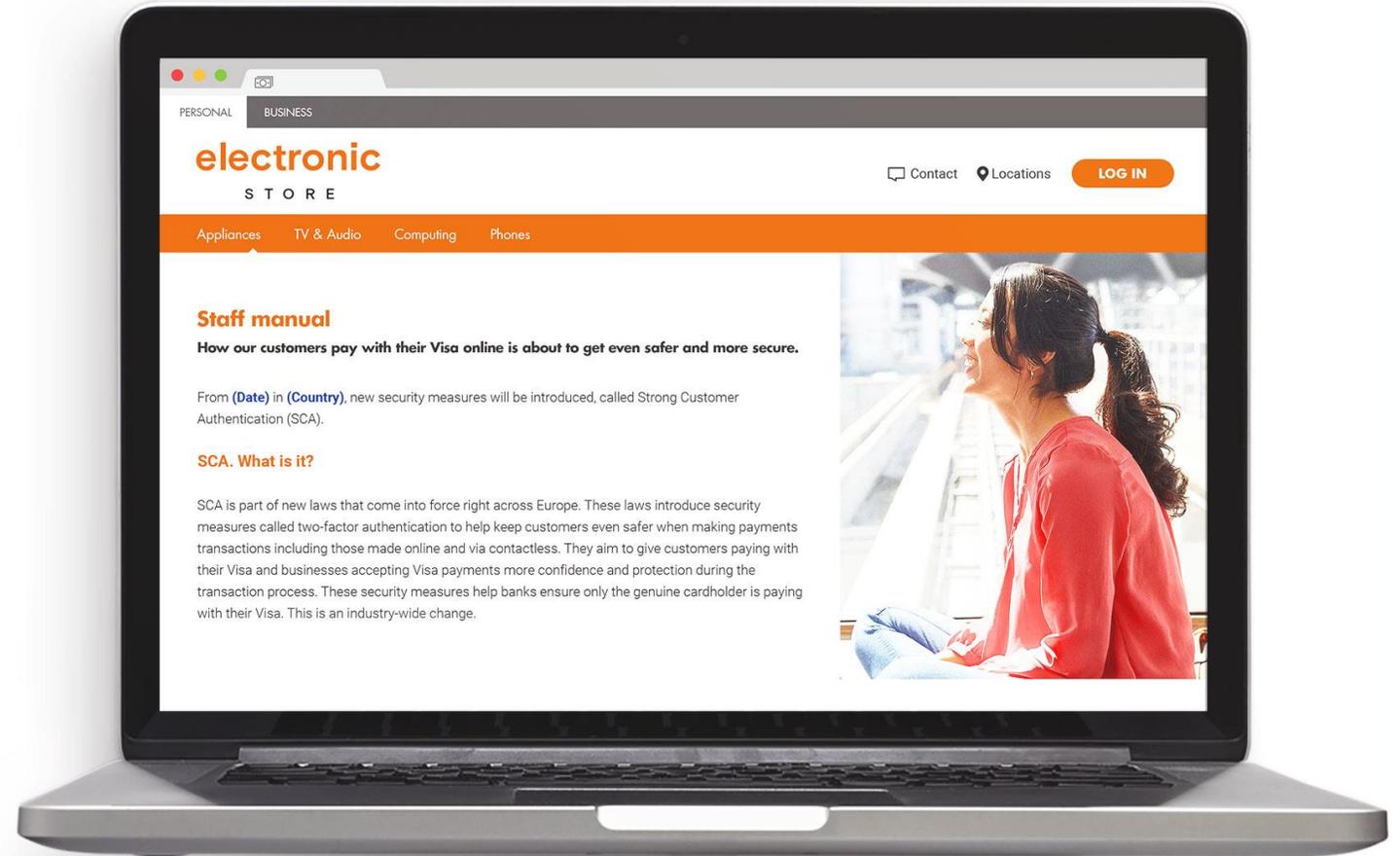
4.2.1 Información en su web

A continuación, presentamos un ejemplo de cómo recomendamos que se publique la SCA en tu web (por ejemplo, en la página de preguntas frecuentes, en la página de ayuda o durante el proceso de pago).



4.2.2 Manual para el personal

A continuación, presentamos un ejemplo de un manual para el personal que muestra cómo te recomendamos que expliques la SCA a tu personal. Proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes.



4.2.3 Aviso en el sitio web

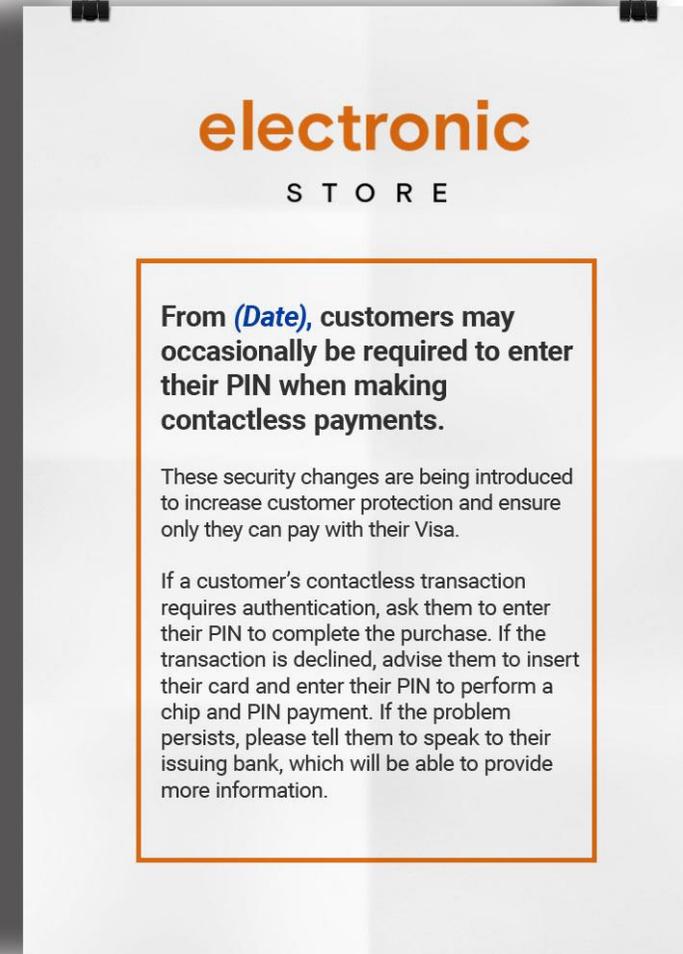
Puedes utilizar el distintivo de Visa Secure en tu web. Cuando tus clientes vean el distintivo «Visa Secure», sabrán que su transacción está protegida por múltiples niveles de seguridad. Ponte en contacto con tu PSP para obtener el distintivo.



4.3 Guía de comunicaciones de *marketing* para negocios físicos

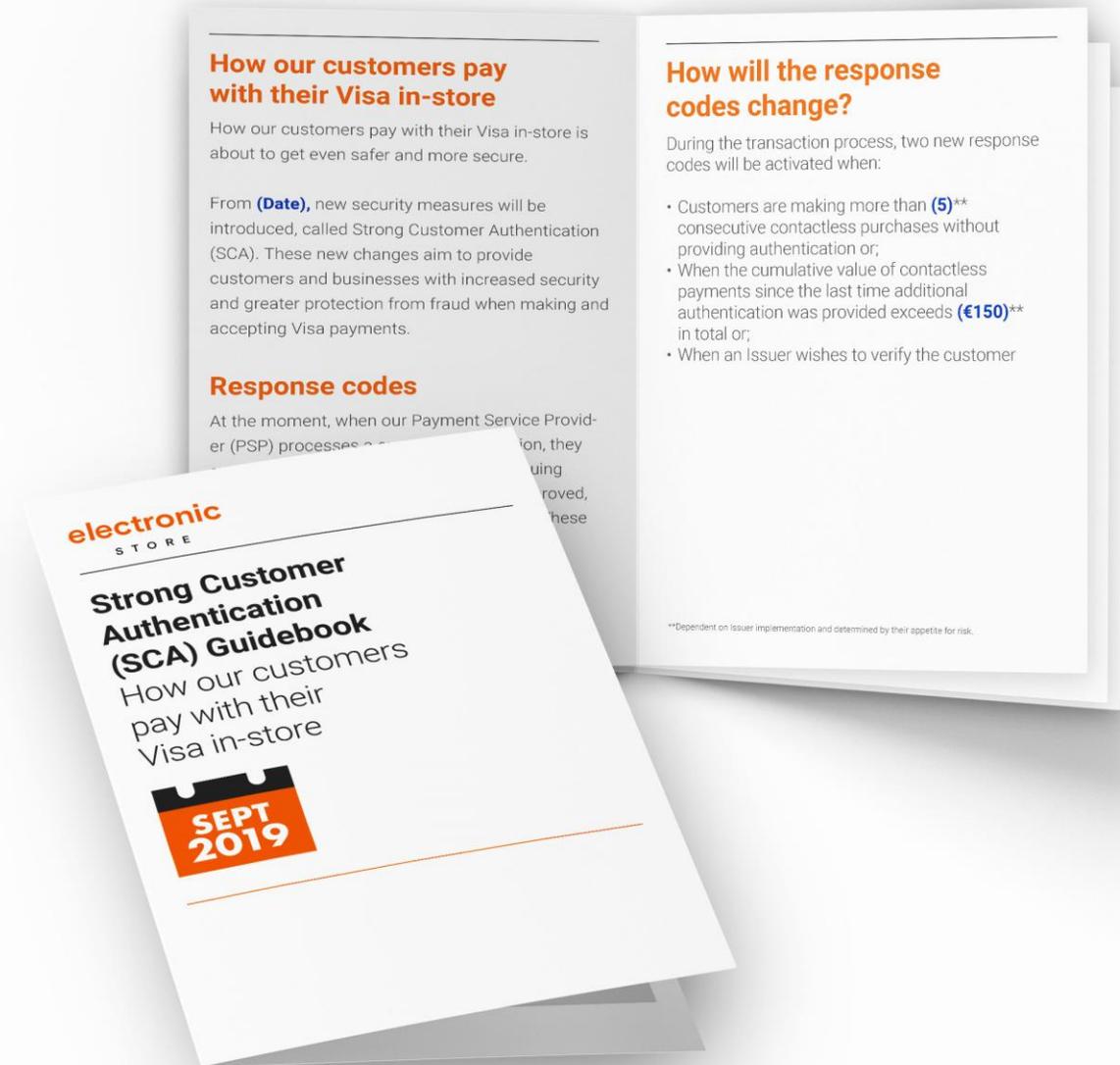
4.3.1 Guía de conversación

A continuación, presentamos un ejemplo de una versión más concisa del manual del personal. En ella se destaca la forma en que recomendaríamos que explicarás la SCA a tu personal. Puedes guardarla en la(s) caja(s) en el punto de venta para ayudar a los empleados a que estén siempre informados.



4.3.2 Manual para el personal

A continuación, presentamos un ejemplo que muestra cómo te recomendamos que expliques la SCA a tu personal. Proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes.



Apéndice: Material de comunicación detallado

Aquí encontrarás algunas indicaciones recomendadas para los titulares de tarjetas. Se trata de los documentos orientativos que puedes utilizar a la hora de comunicar tus mensajes.

Apéndice 4.2.1 [< TRÁS](#)

Párrafo del sitio web

A continuación, presentamos un ejemplo de cómo recomendamos que se publique la SCA en la web de tu negocio (por ejemplo, en la página de preguntas frecuentes, en la página de ayuda o durante el proceso de pago).

Nuestro proceso de pago emplea Visa Secure

Nuestro proceso de pago emplea Visa Secure para garantizar que solo tú puedes utilizar tu tarjeta Visa. Visa Secure se ejecuta en segundo plano para aportar mayor seguridad.

Es posible que se te solicite información adicional para confirmar que eres el titular de la tarjeta. De esta forma, podrás pagar con tu Visa con más tranquilidad y seguridad. Para saber cómo puedes beneficiarte de este nivel adicional de protección, ponte en contacto con el banco emisor de tu tarjeta Visa.

El modo de pago online con tu tarjeta Visa está a punto de cambiar con la inminente aplicación de la Strong Customer Authentication (Autenticación Reforzada del Cliente o SCA) en el marco de la legislación introducida por la UE.

A partir del **(Fecha)***, es posible que se te solicite añadir un paso de seguridad adicional para confirmar tu identidad al efectuar un pago mediante el método de autenticación elegido por tu banco. Esto se conoce como autenticación de dos factores, por lo que tendrás que proporcionar información de al menos dos de las tres categorías siguientes. A estas alturas, tu banco seguramente ya te habrá informado sobre cómo hacerlo. Si no lo ha hecho, ponte en contacto con tu banco.

- **Algo que sabes** – como una contraseña o un PIN
- **Algo que tienes** – como un teléfono móvil, un lector de tarjetas u otro dispositivo
- **Algo que eres** – como un escáner del iris, un reconocimiento facial o una huella dactilar

Incluye esta sección si tu negocio ofrece suscripciones o pagos periódicos.

Es posible que tengas que confirmar tu identidad al configurar una nueva suscripción o un pago periódico. Los pagos posteriores y las suscripciones existentes no requerirán la autenticación de dos factores, aunque es posible que se solicite una autenticación si se realizan cambios en la suscripción.

*Introducir la fecha

Apéndice 4.2.2 [← ATRÁS](#)

Manual para el personal

A continuación, presentamos un ejemplo de un manual para el personal que muestra cómo te recomendamos que expliques la SCA a tu personal. Les proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes y evitar que se produzcan problemas en tu negocio.

El modo de pago online con Visa de nuestros clientes está a punto de mejorar su nivel de seguridad y protección.

Se van a implantar nuevas medidas de seguridad, denominadas SCA (Strong Customer Authentication).

SCA. ¿Qué es?

La SCA, o Strong Customer Authentication, es parte de las nuevas leyes que entran en vigor en toda Europa. Las nuevas leyes introducen medidas de seguridad conocidas como autenticación de dos factores, las cuales ayudan a aumentar la seguridad de los clientes a la hora de efectuar transacciones de pago, incluidas las efectuadas tanto online como a través de la tecnología Contactless. Su objetivo es ofrecer a los clientes que pagan con Visa y a los negocios que aceptan pagos con Visa una mayor confianza y protección durante la transacción. Estas medidas de seguridad permiten a los bancos garantizar que el titular de la tarjeta es quien efectúa el pago con la Visa. Se trata de un cambio que afectará a toda la industria.

¿Cómo funcionará cuando hagas una compra con nosotros?

Cuando un cliente paga con una Visa, es posible que se le solicite que adopte una medida de seguridad adicional para confirmar su identidad mediante el método de autenticación elegido por su banco. Esto se conoce como autenticación de dos factores, por lo que tendrán que proporcionar información de al menos dos de las tres categorías siguientes:

- **Algo que saben** – como una contraseña o un PIN
- **Algo que tienen** – como un teléfono móvil, un lector de tarjetas u otro dispositivo
- **Algo que son** – como un escáner del iris, un reconocimiento facial o una huella dactilar

Apéndice 4.2.2 ATRÁS

Manual para el personal

A continuación, presentamos un ejemplo de un manual para el personal que muestra cómo te recomendamos que expliques la SCA a tu personal. Les proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes y evitar que se produzcan problemas en tu negocio.

Incluye esta sección si tu negocio ofrece suscripciones o pagos periódicos.

¿Cómo configurarán los clientes una nueva suscripción o un pago periódico?

Cuando los clientes configuren una nueva suscripción, es posible que se les solicite que confirmen su identidad mediante el método de autenticación de dos factores elegido por su banco. Los pagos posteriores y las suscripciones existentes no requerirán la autenticación de dos factores, aunque es posible que se solicite una autenticación si se realizan cambios en la suscripción.

¿Qué significará la SCA para nuestros clientes?

A partir de esta fecha, es posible que se modifique la forma de pago online de nuestros clientes debido a la autenticación de dos factores.

El incremento de los niveles de seguridad representará una ventaja para ellos, ya que aumentará su confianza a la hora de efectuar sus compras en Internet. Así podrán seguir efectuando sus pagos a través de todo tipo de dispositivos, como *smartphones*, tabletas y ordenadores portátiles.

Entre otros cambios, los bancos recibirán más datos que les permitirán tomar decisiones mejor informadas y evaluar si una transacción es de bajo riesgo (exenta) o está fuera del ámbito de aplicación de la SCA. Esto contribuirá a crear una experiencia de pago perfecta, ya que reducirá el riesgo de fraude y el número de veces que los titulares de tarjetas deberán autenticar su pago con Visa.

¿Qué debemos hacer?

Debemos estar informados de los cambios que implicará la SCA para poder informar y ayudar a nuestros clientes. No obstante, si tienen alguna pregunta que no puedas responder, remítelos a su banco emisor. Éste les proporcionará más información.

Apéndice 4.2.2 ATRÁS

Manual para el personal

A continuación, presentamos un ejemplo de un manual para el personal que muestra cómo te recomendamos que expliques la SCA a tu personal. Les proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes y evitar que se produzcan problemas en tu negocio.

Preguntas frecuentes

1. ¿Qué es la SCA?

SCA es la abreviatura de «Strong Customer Authentication» o Autenticación Reforzada del Cliente. Desde el **(Fecha)**, los bancos introducirán nuevas medidas de seguridad como parte de las nuevas leyes que entran en vigor en toda Europa para pagos con tarjeta. Estas medidas harán que el pago con Visa sea aún más seguro gracias a la autenticación de dos factores, la cual añade un nuevo nivel de seguridad a los pagos en línea y Contactless. Esto permitirá a los bancos garantizar que el titular de la tarjeta es quien efectúa el pago con la Visa.

2. ¿Cómo pagarán en línea nuestros clientes cuando la SCA entre en vigor?

Es posible que se les solicite que adopten una medida de seguridad adicional para confirmar su identidad mediante el método de autenticación elegido por su banco. Para ello, proporcionarán información de al menos dos de las tres categorías que figuran a continuación:

- **Algo que saben** – como una contraseña o un PIN
- **Algo que tienen** – como un teléfono móvil, un lector de tarjetas u otro dispositivo
- **Algo que son** – como un escáner del iris, un reconocimiento facial o una huella dactilar

Apéndice 4.2.2 Manual para el personal

A continuación, presentamos un ejemplo de un manual para el personal que muestra cómo te recomendamos que expliques la SCA a tu personal. Les proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes y evitar que se produzcan problemas en tu negocio.

Preguntas frecuentes (continuación)

3. ¿Qué pasará cuando nuestros clientes configuren una nueva suscripción o un pago periódico?

Es posible que se solicite a nuestros clientes que verifiquen su identidad en el momento de configurar una nueva suscripción o un nuevo pago periódico a través del método elegido por su banco. Los pagos posteriores y las suscripciones existentes no requerirán la autenticación de dos factores, aunque es posible que se solicite una autenticación si se realizan cambios en la suscripción

4. ¿Qué deben hacer nuestros clientes si se rechaza su transacción o si no saben cómo autenticarse?

Remíteles a su banco. Éste podrá proporcionarles más información.

5. ¿Qué es Visa Secure?

Visa Secure es la tecnología de Visa que los bancos utilizan para que los pagos de nuestros clientes sean más seguros. Cuando nuestros clientes vean el distintivo «Visa Secure», sabrán que su transacción está protegida por múltiples niveles de seguridad. Y estarán protegidos gracias a la política de Cero responsabilidad ante cualquier compra fraudulenta que cualquiera pueda haber realizado con su tarjeta Visa.

6. ¿Esta seguridad adicional es gratis?

Sí. Visa no cobra ningún coste adicional a los comerciantes por este nuevo nivel de protección.

Apéndice 4.3.1

Guía de conversación

A continuación, presentamos una versión más concisa del manual para el personal que destaca cómo te recomendamos que expliques la SCA a tu personal. Puedes guardarla en la(s) caja(s) en el punto de venta para que sus empleados estén siempre bien informados.

Desde el **(Fecha)***, es posible que se solicite de forma ocasional a los clientes que introduzcan su PIN cuando realicen pagos Contactless.

Se están introduciendo estos cambios de seguridad para mejorar la protección de los clientes y garantizar que solo ellos puedan pagar con su Visa.

Si la transacción Contactless de un cliente requiere autenticación, solicítale que introduzca su PIN para completar la compra. Si se rechaza la transacción, pídele que introduzca su tarjeta y marque el PIN para efectuar el pago con el chip y el PIN. Si el problema persiste, aconséjale que se dirija a su banco emisor, el cual podrá proporcionarle más información.

*Introducir la fecha

Apéndice 4.3.2 ← ATRÁS

Manual para el personal

A continuación, presentamos un ejemplo que muestra cómo te recomendamos que expliques la SCA a tu personal. Proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes.

Cómo pagarán nuestros clientes con su Visa en el punto de venta

El modo de pago en el punto de venta con Visa de nuestros clientes está a punto de mejorar su nivel de seguridad y protección.

Desde el **(Fecha)***, se van a implantar nuevas medidas de seguridad, denominadas SCA (Strong Customer Authentication). Estos nuevos cambios tienen como objetivo proporcionar a los clientes y a las empresas una mayor seguridad y protección contra el fraude a la hora de efectuar y aceptar pagos con Visa.

Códigos de respuesta

Actualmente, cuando nuestro Proveedor de Servicios de Pago (PSP) procesa la transacción de un cliente, nos envía un código de respuesta de dos dígitos desde el banco emisor para notificarnos si el pago ha sido aprobado, rechazado o qué medidas debemos tomar al respecto. Estos códigos de respuesta cambiarán tras la introducción de la SCA.

¿Cómo cambiarán los códigos de respuesta?

Durante el proceso de transacción, se activarán dos nuevos códigos de respuesta cuando:

- Los clientes hacen más de (5)** compras consecutivas mediante pago Contactless sin proporcionar autenticación.
- Cuando el valor acumulado de los pagos Contactless desde la última vez que se proporcionó la autenticación adicional supera los (150€)** en total.
- Cuando un emisor desea verificar la identidad del cliente

*Introducir la fecha

**Depende de la aplicación del emisor

Apéndice 4.3.2 < TRÁS

Manual para el personal

A continuación, presentamos un ejemplo que muestra cómo te recomendamos que expliques la SCA a tu personal. Proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes.

Incluye este detalle en las preguntas frecuentes si resulta relevante para tu personal

Los bancos manejan los nuevos códigos de respuesta. Para que nuestro negocio esté listo antes del **(Fecha)***, tendremos que asegurarnos de que todos nuestros terminales admitan estos dos nuevos códigos:

1. **Código de respuesta 70** – se aplica a las transacciones online con PIN y solicita el PIN al cliente.
2. **Código de respuesta 1A** – se aplica a las transacciones con PIN en el punto de venta y se comunica con el terminal para cambiar la interfaz con el fin de insertar la tarjeta e introducir un PIN.

Preguntas frecuentes

1. ¿Qué es la SCA?

SCA es la abreviatura de «Strong Customer Authentication» o Autenticación Reforzada del Cliente. Los bancos introducirán nuevas medidas de seguridad como parte de las nuevas leyes que entrarán en vigor en toda Europa. Estas medidas harán que el pago con Visa sea aún más seguro gracias a la autenticación de dos factores, la cual añade un nuevo nivel de seguridad a los pagos Contactless. Esto permitirá a los bancos garantizar que el titular de la tarjeta es quien efectúa el pago con la Visa.

2. ¿Qué ocurrirá cuando los clientes compren en el punto de venta mediante un pago Contactless?

Para pagos en el punto de venta, es posible que se les pida que introduzcan su PIN con más frecuencia.

3. ¿Qué deben hacer los clientes si su transacción Contactless aparece rechazada?

Pide al cliente que introduzca su tarjeta y marque el PIN para efectuar el pago con el chip y el PIN. Si la transacción falla o aparece rechazada, remite al cliente a su banco emisor. Este podrá proporcionarle más información.

*Introducir la fecha

Apéndice 4.3.2 [◀ ATRÁS](#)

Manual para el personal

A continuación, presentamos un ejemplo que muestra cómo te recomendamos que expliques la SCA a tu personal. Proporciona la información de referencia necesaria para responder a algunas de las preguntas más comunes de los clientes.

4. ¿Qué es Visa Secure?

Visa Secure es la tecnología de Visa que los bancos utilizan para que los pagos de los clientes sean más seguros. Cuando vean el distintivo «Visa Secure», sabrán que su transacción está protegida por múltiples niveles de seguridad.

5. ¿Cómo protege Visa a los clientes?

Estarán protegidos gracias a la política de Cero responsabilidad ante cualquier compra fraudulenta que cualquiera pueda haber realizado con su tarjeta Visa.

6. ¿Esta seguridad adicional es gratis?

Sí. Visa no cobra ningún coste adicional a los comerciantes por este nuevo nivel de protección.

Si eres un Comercio con tienda online y tienda física, combina estos materiales para adaptarlos a tus necesidades.

Gracias



VISA everywhere
you want to be