Impacto en la aplicación de la autenticación reforzada sobre el pago con tarjeta en comercio electrónico

Introducción

De acuerdo con la normativa de pagos en vigor[1], a partir del 14 de septiembre cuando se inicie una operación de pago electrónico, deberá hacerse uso de autenticación reforzada del cliente ordenante, esto es, la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario).

A pesar de los esfuerzos que están realizando los proveedores de servicios de pago para cumplir con los requisitos derivados de la norma, el despliegue de la autenticación reforzada está encontrando numerosos obstáculos, tanto de tipo tecnológico como de adaptación de las partes implicadas.

Una aplicación exhaustiva de las exigencias de autenticación reforzada en el ámbito de las transacciones con tarjeta de comercio electrónico llevaría consigo un impacto negativo muy significativo para este tipo de transacciones, respecto al impacto en transacciones con tarjeta en comercio físico.

Impacto SCA en comercio electrónico

En este caso concreto hay dos factores determinantes a considerar:

- la indisponibilidad o retraso de soluciones tecnológicas que permitirán alcanzar el equilibrio adecuado entre el interés en una mayor seguridad (autenticación reforzada) en los pagos remotos y las necesidades de facilidad de uso y accesibilidad de los pagos (exenciones) en el ámbito del comercio electrónico,
- la limitada preparación por parte de muchos de los comercios, que han de adaptar sus plataformas a las nuevas exigencias.

El comercio electrónico se enfrenta a un riesgo de disrupción debido al elevado que el número de transacciones que, o bien se verían rechazadas por no incluir autenticación reforzada, o bien conllevarían cambios significativos

[1] Reglamento Delegado (UE) 2018/389 de la Comisión del 27 de noviembre de 2017 relativas a las normas técnicas de regulación para la autenticación reforzada del cliente y unos estándares de comunicación comunes y seguros

en la experiencia de usuario para incorporar la autenticación reforzada, sin poder ser objeto de una exención. Esta situación generaría un alto nivel de confusión entre los consumidores que experimentarían problemas para realizar las compras, creando sobre todo una falta de confianza en el proceso de digitalización actualmente en pleno auge. Conviene tener en cuenta que el crecimiento del comercio electrónico en el último año en España se sitúa próximo al 30% con un volumen que lo sitúa en el cuarto lugar del ranking de los países de la Unión.

Las operaciones en el entorno del comercio electrónico tienen una gran dependencia de proveedores externos, que facilitan los protocolos técnicos en los que se sustentan, y de desarrollos por parte de los comercios, no sólo por los PSPs o sus proveedores de servicios de distinta índole. 3D Secure es la solución global existente para la aplicación de autenticación reforzada de clientes en las operaciones de comercio electrónico, que en sus versiones v1 y v2.1 están en el mercado e implantadas en un 70-80% de comercios españoles (frente a otros países vecinos donde esta tasa no alcanza el 50%). Sin embargo, esta solución únicamente es utilizada en 23% de las transacciones dentro de la Unión, llegando hasta el 31% en el mercado nacional.

No obstante, los actuales protocolos técnicos de 3D Secure no incorporan la posibilidad de la gestión de la totalidad de las exenciones que prevén los estándares técnicos de autenticación reforzada. Esta situación conllevaría en la teoría a aplicar autenticación reforzada en casi todas las operaciones que se procesan. Aunque el protocolo técnico, V.2.1, de 3D Secure incorpora un primer nivel de gestión de exenciones a la autenticación reforzada, la versión que permitirá mejorar y ampliar, la posibilidad de la gestión de las exenciones a las entidades, es la v2.2, cuya previsión de previsión de implantación se sitúa, a partir del último trimestre del año. A esto hay que añadir un periodo razonable de puesta en el mercado (incluida la adopción por parte de los comercios).

La migración a comercio seguro es algo que se asumía como implícito en la directiva, al no permitir operaciones sin SCA o bajo la aplicación de una exención. Pero aún en el supuesto de la plena adopción del comercio electrónico seguro en el tiempo que queda hasta el 14 de septiembre, la práctica a la que están acostumbrados los usuarios se sustenta en el número de tarjeta junto con la fecha de caducidad y el código de seguridad CVV más un factor adicional (OTP), como factores suficientes para considerar que se aplica autenticación reforzada ya que se combinan los datos estáticos de la tarjeta con un factor dinámico.

Cabe indicar que la ratio de fraude para las operaciones de comercio electrónico seguro es de 0,022% en España, frente a 0,069% en el caso de operaciones que no reúnen las condiciones de comercio electrónico seguro. Estos valores ascienden a 0,034% y 0,225% respectivamente cuando se computa el tráfico transfronterizo dentro de la Unión.

Sin embargo, el problema se acrecienta cuando, incluso en un escenario de total adopción del comercio electrónico seguro, se tiene en consideración la opinión de la Autoridad Bancaria Europea (EBA) sobre la implementación de los estándares técnicos de autenticación reforzada[2], expresada en el párrafo 35, de donde se desprende que la combinación de número de tarjeta junto con el CCV y la fecha de caducidad de la tarjeta no pueden considerarse como un elemento de conocimiento. Tampoco como elemento de posesión puesto que para que un dispositivo se pueda considerar como posesión es preciso confirmar la posesión mediante medios fiables que permitan la generación o recepción de un elemento de validación dinámico en el dispositivo.

En la actualidad estas transacciones incumplirían las exigencias de autenticación reforzada, y deberían de incorporar algún factor adicional para cumplir con los requisitos lo que implica una fricción añadida, con reflejo directo en la tasa de abandono de las transacciones. Esta tasa se sitúa en el 9,30% en las transacciones de comercio seguro y se estima que cada punto porcentual de incremento en la misma comprometería 188 millones de € en el volumen de ventas en comercio electrónico en España. La alternativa sería un incremento del número de transacciones rechazadas con las consecuencias indeseables tanto económicas como de pérdida de confianza en las transacciones de pago electrónicas y en el entorno digital que se persigue potenciar, no solo en el ámbito nacional sino transfronterizo dentro de la Unión.

Conclusión

El sector financiero español lleva tiempo trabajando intensamente en la implementación de la segunda Directiva de Servicios de Pago (PSD2) y está plenamente comprometido con los objetivos que fija la norma, incluida la necesidad de reforzar la seguridad de las transacciones y la lucha contra el fraude.

El escenario que se presenta no es tanto un problema de cumplimiento de la norma, como de preparación del mercado. En la actual situación, el cumplimiento implicaría el rechazo de numerosas transacciones o la incorporación de factores de autenticación adicionales. Cualquiera de las opciones generaría altas tasas de abandono, todo ello con consecuencias devastadoras para el comercio electrónico que se encuentra en pleno auge y para el conjunto de la economía.

[2] Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC https://eba.europa.eu/documents/10180/2137845/Opinion+on+the+implementation+of+the+RTS+on+SCA+and+CSC+%28EBA-2018-Op-04%29.pdf

No hay que perder de vista que el objetivo que persiguen las normas técnicas de regulación para la autenticación reforzada de clientes es limitar el fraude, pero también debe permitir la innovación.

Las entidades financieras son partidarias de dar continuidad a estos pagos, en un entorno de comercio electrónico seguro, donde el nivel de seguridad, como demuestran los niveles de fraude, es muy elevado. Esto implica, asumir la responsabilidad derivada del artículo 46.2 del RDL de servicios de pago.

Por parte de los proveedores de servicios de pago y [del comercio minorista] se propone un plan de acción para la plena adopción de los factores la autenticación reforzada en un plazo razonable de meses, como medida para minimizar el potencial impacto de esta situación.

Este plan permite la introducción de los cambios de forma paulatina y permitirá que tanto los consumidores como las empresas puedan beneficiarse de una máxima seguridad en los pagos, sin que ello conlleve un detrimento en la experiencia de usuario con el consecuente perjuicio económico y una merma de confianza en el comercio electrónico.

Entre tanto, mientras se implanta plenamente el 3D Secure v2.2 y un segundo factor, que permitan una buena experiencia de usuario en las transacciones de comercio electrónico seguro y a la espera de mayor claridad normativa para asegurar una interpretación consistente, se trabaja con la presunción de que un factor dinámico (OTP) adicional al número de tarjeta+CVV+fecha de caducidad es compatible con la autenticación reforzada (SCA) hasta el fin del periodo transitorio que se fije en el plan de acción. Cabe recordar que además de manera habitual, se toman en consideración suficientes medidas de evaluación de riesgo en las transacciones, incluidas características comportamentales, que permiten mitigar las actuaciones fraudulentas.

De esta forma los comercios trabajarán para la adopción del comercio electrónico seguro en su versión más avanzada, 3D Secure v2.2, si tener que hacer actualizaciones intermedias, que en su caso implicarían una regresión en la experiencia de usuario para poder a posteriori mejorarla, lo que sin duda conllevaría las consecuencias indeseables que se pretende evitar.

Junio 2019