Opinión

MEDIOS DE PAGO: A QUIÉN AFECTA LA PRÓRROGA DE LA EBA

Paula De Biase

Responsable de la Práctica de Servicios Financieros Pérez-Llorca

ISTOCK

Uno de los hitos de implementación más importantes derivados de la segunda directiva de servicios de pago, conocida como PSD2, fue la entrada en vigor del Reglamento Delegado 2018/389, de 27 de noviembre de 2017 sobre autenticación reforzada y estándares de comunicación (el "Reglamento") el pasado 14 de septiembre de 2019.

Entre las principales novedades previstas en el Reglamento se encuentra la exigencia de que los proveedores de servicios de pago (lo que incluye en particular entidades de crédito) apliquen una autenticación reforzada a sus clientes cuando estos últimos accedan a su cuenta de pago en línea, inicien una operación de pago electrónico y/o realicen por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude, todo ello, salvo que las entidades apliquen alguna de las excepciones previstas en el Reglamento (como por ejemplo, la de operaciones de bajo importe contactless o la lista de beneficiarios de confianza).

La PSD2 y el Reglamento ya han entrado formalmente en vigor, aunque, en la práctica, la implementación de la autenticación reforzada para el comercio electrónico ha sufrido una prórroga y todavía existe mucho desconocimiento de entidades no reguladas (comercios y/o prestadores de servicios) sobre cómo les afectarán estas medidas y su sobre cuál es rol en su puesta en marcha.

Porque, al final, ¿qué cambia en materia de autenticación? La aplicación de la autenticación reforzada pasa a exigir que la comprobación de la identidad del usuario de un servicio de pago o la validez de la utilización de un determinado instrumento de pago (ejemplo: tarjetas) tenga que realizarse obligatoriamente aplicando dos o más de los siguientes elementos: conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), los cuales, a su vez, son independientes, es decir, que la vulneración de uno de ellos no puede comprometer la fiabilidad de los demás.

> Existe un gran desconocimiento en el comercio sobre cómo impacta la reciente normativa

Aunque como usuarios podríamos tener la sensación de utilizar una autenticación de doble factor desde hace mucho tiempo en comercio electrónico o en ciertas transacciones de banca electrónica, dicha operativa era normalmente algo voluntario como medida de comercio seguro y no seguía los mismos parámetros exigidos para la autenticación reforzada. En particular, debemos destacar que la operativa más habitual en comercio electrónico de incluir el número de la tarjeta y CCV y añadir posteriormente un código recibido al móvil no es suficiente para cumplir los nuevos requisitos de autenticación reforzada, pues el número de tarjeta no puede calificarse como algo que solo posee el usuario.

Esto implica que los distintos proveedores de servicios de pago tienen que implementar nuevas soluciones tecnológicas cumplidoras de los parámetros de autenticación reforzada y a su vez, migrar sus distintos clientes (ya sean personas físicas o comercios, según el caso) para dichas nuevas soluciones. Además, con aras a permitir una experiencia de usuario de un solo clic (extremadamente deseable por muchos comercios online), es necesario que dichas soluciones puedan permitir gestionar la aplicación de las distintas excepciones a la autenticación reforzada. Para poder aplicar dichas excepciones, los proveedores de servicios de pago son obligados a realizar un análisis de los riesgos de fraude que ello pueda entrañar y para esto, es fundamental que los sistemas tecnológicos utilizados permitan viajar distintos datos asociados a la transacción.

Conocedora de los desafíos asociados a dichos cambios, la Autoridad Bancaria Europea (EBA) otorgó cierta flexibilidad a las autoridades nacionales (en el caso español, el Banco de España) para coordinar con los proveedores de servicios de pago bajo su supervisión un tiempo adicional limitado para adaptarse a los procedimientos de la autenticación reforzada, pero únicamente en lo que se refiere a las operaciones de comercio electrónico (la autenticación para acceder a cuentas *online* por ejemplo, ya entró en vigor desde el 14 de septiembre). El pasado 16 de octubre de 2019, la EBA ha aclarado que la nueva fecha límite para la implantación de dichas normas es el próximo 31 de diciembre de 2020. Para ello, los proveedores de servicios de pago afectados tienen hasta el 31 de diciembre 2019 para presentar sus planes de migración al Banco de España.

Es importante subrayar que la obligación de aplicar la autenticación reforzada recae directamente sobre los proveedores de servicios de pago regulados. No obstante, cualquier empresa que tenga un comercio electrónico debe informarse sobre dichas medidas, no solo para realizar los pasos mínimos que le requiera su proveedor de servicios de pago para la migración pero también a los efectos de valorar la mejor estrategia comercial y de comunicación a sus clientes (lo que podría incluir actualización de términos y condiciones de usuarios u otros cambios que pudieran facilitar la aplicación de alguna de las excepciones a la autenticación reforzada).