Cómo garantizar la seguridad de los cobros con tarjeta

Por: *Lidia Martínez – Alisys*

Fáciles, rápidos y sencillos. Estas tres características han situado a los pagos digitales entre los métodos predilectos por los consumidores europeos para abonar el coste de sus compras, pedidos y facturas. Pero es indispensable añadir una cuarta característica, seguros. La seguridad es un factor crítico que según estimaciones de Juniper Research pasará de los 17 mil millones de dólares en 2020 a los 25 millones de dólares en 2024 en pérdidas derivadas del fraude en los pagos digitales.

Sin embargo, las marcas no pueden renunciar a un método de pago que gana adeptos día tras día. Y es que, aunque los datos varían en función de la transacción y del país, la tendencia indica la predisposición de los usuarios por utilizar métodos de pago digitales como alternativa al dinero en efectivo.

25 millones de dólares en 2024 en pérdidas derivadas del fraude en los pagos digitales

Juniper Research

Así, mientras que el 94,5% de los pagos de facturas en Grecia se realizan en efectivo; en el lado opuesto del ranking, se sitúa Dinamarca con solo un 2,1% de las facturas pagadas en metálico. En España, los pagos en efectivo se sitúan en torno al 27%.

Por su parte, el pago a través de móvil alcanzó un tasa de penetración del 90% en Suecia en 2019 y, en España, más de 2,5 millones de españoles utilizaron sus teléfonos móviles como método de pago.

No obstante, como ya sucedió con la primera ola de la COVID-19, cuando las ventas online se triplicaron con el confinamiento y se multiplicaron las peticiones de comida a domicilio; en esta segunda oleada se prevé de nuevo un auge de los métodos de pago touch free.

Los métodos de pago digitales, por tanto, se posicionan como los grandes aliados de las marcas para satisfacer las demandas de un consumidor que manifiesta su preferencia por los pagos digitales. Según Capgemini, el 48% de los clientes eligen establecimiento y marcas que permiten el pago digital.

Pero, ¿cómo hacer frente al reto de seguridad de los pagos digitales?

La entrada en vigor 1 de enero de 2018 de la Directiva PSD2 (Payment Services Directive) de la Comisión Europea marcó un punto de inflexión en los pagos online. Redefinió y estableció un marco legal común para los pagos digitales de los 28 países de la Unión, más Islandia, Liechtenstein, Noruega, Mónaco, San Marino y Suiza con el propósito, principal, de reducir el fraude de los pagos online y aumentar la protección de los usuarios.

Aunque su aplicación ha sido aplazada, la moratoria expira el 31 de diciembre de 2020. Así, a partir del 1 de enero de 2021 los negocios que admitan pagos online deberán cumplir con los requisitos de autentificación de cliente. Con la SCA (Strong Customer Authentication) ya no basta con introducir los clientes los datos de la tarjeta de crédito, además deben cumplir, al menos, 2 de los 3 factores de validación que contempla la directiva:

- Algo que solo conoce el usuario: contraseña o pin.
- Algo que solo tiene el usuario: Smartphone o token.
- Algo que el usuario es: huelga digital o biometría.

No obstante, esta normativa no aplica a todas las transacciones ni a todos los productos. Así quedan exentos:

- Pagos recurrentes, como suscripciones, ya que solo será necesario la doble autentificación para la primera transacción. El SCA solo aplica a las transacciones iniciadas por el cliente.
- Transacciones cuyo banco emisor y receptor están ubicados fuera del Espacio Económico Europeo.
- Pagos inferiores a 30€. La SCA será aplicable cuando el cliente realice más de 5 pagos o más que sumen más de 100€.
- Pagos corporativos

Aunque los negocios están obligados a verificar que su proveedor de servicios de pago cumple con la normativa, su principal labor deberá centrarse en localizar entidades bancarias, proveedores de soluciones de pago y/o pasarelas de pago que cumplan con la normativa.

Pero el PSD2 no es la única normativa que deben tener en cuenta los negocios para garantizar la seguridad de los cobros digitales. El PCI-DSS (Payment Card Industry – Data Security Standard) es el estándar de seguridad de datos de la industria de tarjetas de pago. Tiene como finalizar garantizar que todas las organización que recopilan, transmiten, almacenan o procesan datos de tarjetas de pago disponen de entornos seguros. Es por tanto, de obligado cumplimiento, para todos los negocios que acepten pagos con tarjeta de crédito con independencia del canal de pago.

PCI-DSS es de obligado cumplimiento para todos los negocios que acepten pagos con tarjeta.

Así el estándar PCI-DSS establece 12 requerimientos para los comerciales:

1. Instalar y mantener una configuración de firewall para proteger los datos
2. No utilice valores predeterminados por los proveedores para contraseñas de sistema y otros parámetros de seguridad
3. Proteger los datos del titular de la tarjeta
4. Proteger los datos del titular de la tarjeta que fueron almacenados

5. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
6. Mantener un programa de administración de vulnerabilidad
7. Utilizar y actualizar con regularidad los programas o software antivirus
8. Desarrolle y mantenga sistemas y aplicaciones seguras
9. Implementar medidas sólidas de control de acceso
10. Restrinja el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa
11. Restringir el acceso físico a los datos del titular de la tarjeta
12. Mantener una política de seguridad de información
13. Mantener una política que aborde la seguridad de la información para todo el personal

La normativa, por ende, prohíbe grabar y almacenar datos de la tarjeta en entornos webs, tiendas online o logs de sistemas. Dejando atrás prácticas obsoletas como apuntar los datos de la tarjeta en papel o Excel para introducirlos posteriormente en el sistema o proporcionar los datos a un agente, en el caso de los pagos por teléfono; o enviar a través de SMS dicha información para que el vendedor acepte el pedido.

Para no incurrir en los grandes costes que implica adaptar la propia infraestructura a la normativa, los negocios que venden online y/o aceptan cobros con tarjeta deberán contratar los servicios de un proveedor de soluciones de pago avalado por el certificado PCI y que incluya pasarelas de pago PS2D2.

No obstante, el PCI-DSS establece 4 niveles de seguridad en función del número de operaciones con tarjetas que una empresa efectúa al año:

- Nivel 1: negocios con más de 6.000.000 de transacciones anuales
- Nivel 2: negocios con 1.000.000 y 6.000.000 de transacciones anuales
- Nivel 3: negocios con 20.000 y 1.000.000 de transacciones online anuales o que procesan menos de 1.000.000 de transacciones anuales en total

- Nivel 4: negocios con menos de 20.000 transacciones online anuales o que procesan hasta 1.000.000 de transacciones anuales en total

¿Qué sucede si se incumplen los estándares de seguridad?

En el caso de la normativa PSD2, la normativa contempla sanciones aplicables a los "proveedores de servicios de pago" que serán comunicadas por el Banco de España. Dichas sanciones, pueden superar la inhabilitación para los cargos directivos o administradores de las plataformas.

Por su parte, las sanciones del PCI-DSS dependerán del volumen de transacciones del negocio, la cantidad de requisitos de PCI-DSS afectados y de la política de multas de la marca de tarjeta. No obstante, aunque las sanciones recaen sobre los procesadores de pago, éstas a su vez pueden aplicar correctivos a los negocios. Las marcas de tarjetas de crédito, por tanto, pueden aplicar sanciones, multas, reclamaciones o cancelar la actividad comercial con el negocio.

Apostar por un proveedor de soluciones de pago con certificación PCI-DSS es la fórmula más eficiente para que los negocios que aceptan pagos con tarjeta de crédito puedan garantizar a sus clientes la seguridad de los cobros con tarjeta.

Fuentes

- Cadena Ser, El uso del efectivo en Europa: ¿Qué países están más cerca de eliminarlo?
- Capgemini, El consumidor y el COVID-19. Investigación global sobre el sentimiento de los consumidores y el sector minorista
- Juniper Researc, Ecommerce losses to online payment fraud to exceed $25 billion annually by 2024
- Expansión, El futuro de los pagos: Pagar por la cara, ni tarjetas de crédito ni tampoco efectivo
- PCI Security Standards, Industria de las Tarjetas de Pago (PCI) Norma de Seguridad de Datos
- BOE, Real Decreto 736/2019, de 20 de diciembre