NOTAS OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA

FUNCAS – 28 de julio de 2022 **ODF – Funcas 57 / 2022**

El reto del fraude en los pagos digitales

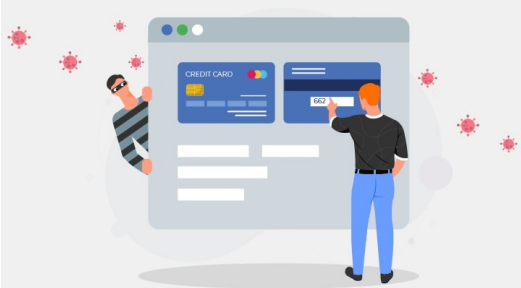
A medida que los consumidores optan con mayor frecuencia por pagar con medios distintos al efectivo, crecen los intentos de fraude. El auge de los pagos digitales también está suponiendo un incremento significativo en los mecanismos delictivos. Para que el crecimiento de los pagos digitales se mantenga es clave que estos sean cada vez menos vulnerables a los intentos de fraude.

Se estima que en 2021 se pagaron cerca de 6,6 billones de dólares a través de canales digitales, lo que supuso un aumento del 40% respecto a 2020. Se espera que este crecimiento continúe en el futuro, con el valor del mercado de pagos digitales alcanzando los 10.5 billones de dólares en 2025.[1] Esta evolución coincide con la creciente amenaza de fraude. Las innovaciones tecnológicas también se producen en esa dimensión delictiva. En Estados Unidos, cerca de 18 millones de personas fueron estafadas en transacciones con billeteras digitales y aplicaciones de pagos en 2020.[2]

Entre los tipos de fraude destacan formas más tradicionales como el "phishing", el robo de identidad, pero también surgen nuevas variedades como el "pagejacking". Este último consiste en redirigir el tráfico *online* de un sitio de comercio electrónico, hacia otro sitio web diferente para extraer información y suplantar la identidad. Se trata de un sistema sofisticado que crece a medida que los consumidores compran más a través del comercio electrónico.

[1] AI and Transaction Notifications Help FIs Stop Payments Fraud Before Customers Get Scammed. PYMNTS. 30 septiembre 2021. https://www.pymnts.com/authentication/2021/report-ai-and-transaction-notifications-help-fis-stop-payments-fraud-before-customers-gets-scammed/

[2] Retail payments fraud: How consumers and banks can fight back. FICO. 29 abril 2022. https://www.fico.com/blogs/retail-payments-fraud-how-consumers-and-banks-can-fight-back



Abordar el crimen financiero es una prioridad en la agenda corporativa de la mayoría de las empresas y de los proveedores de pagos. Además del coste económico para las entidades, puede haber un daño enorme a la marca y la reputación. Muchos bancos, proveedores de pagos, comerciantes y otros actores en el espacio de transacciones digitales están implementando tecnologías de ciberseguridad avanzadas como biometría, inteligencia artificial y *machine learning*. Todo ello, además de implementar métodos de autenticación multifactoriales, tal y como exige la PSD2 a través del protocolo de autentificación reforzada del cliente (SCA, por sus siglas en inglés).

El próximo paso debe ser impulsar la colaboración en el segmento de los pagos para avanzar hacia un ecosistema donde los actores implicados puedan compartir información sobre transacciones sospechosas e intentos de fraude. Por ejemplo, en el Reino Unido, el sistema de intercambio de inteligencia sobre fraudes permite a la industria bancaria compartir información sobre todos los delitos confirmados, intentados o sospechosos en una base de datos central compartida.[3]

[3] Arresting Payment Fraud: Why The Industry Must Collaborate To Outsmart A Global Enemy. Forbes. 28 junio 2022. https://www.forbes.com/sites/boblegters/2022/06/28/arresting-payments-fraud-why-the-industry-must-collaborate-to-outsmart-a-global-enemy/?sh=6abf471a4389