

Desafíos a los que se enfrentan los participantes del ecosistema de pagos

"Los bancos que entiendan la tecnología sobrevivirán. Los que no, desaparecerán."

Paráfrasis de las ideas de Chris Skinner (autor, conferencista y consultor británico, reconocido como uno de los principales expertos mundiales en transformación digital de servicios financieros, banca, tecnología financiera (fintech) y el futuro del dinero), en su libro Digital Bank (2014).

El ecosistema de pagos está experimentando una transformación significativa, impulsada por la digitalización, la evolución tecnológica y los cambios en las demandas de los consumidores. Esta transformación presenta desafíos importantes para las entidades financieras y no financieras. En este contexto, resulta crucial que las organizaciones comprendan y se adapten a estos cambios para mantenerse competitivas y aprovechar las nuevas oportunidades de negocio.

La escala importa

En el ámbito de los pagos, la escala constituye un factor crucial, aunque no es el único determinante para lograr el éxito financiero. La capacidad de gestionar un gran volumen de transacciones resulta esencial para cualquier entidad que desee competir de manera eficiente.

Sin embargo, el negocio de los pagos no se sostiene exclusivamente mediante las comisiones generadas por transacción, dado que estas tienden a disminuir progresivamente y, en algunos modelos, no son suficientes para garantizar la rentabilidad a largo plazo ni para financiar las inversiones tecnológicas necesarias. La verdadera importancia de la escala radica en su capacidad para actuar como facilitador de servicios complementarios más lucrativos. Una amplia base de clientes y un alto volumen de transacciones permiten recopilar una cantidad significativa de datos, que pueden ser aprovechados para ofrecer productos financieros adicionales, como créditos, seguros, inversiones y servicios personalizados.

Además, la escala posibilita negociar mejores tarifas con proveedores y reducir los costes operativos mediante economías de escala. Esto no solo mejora la eficiencia, sino que también permite ofrecer precios más competitivos, captando así más clientes y reforzando aún más el crecimiento. Este fenómeno ha sido una de las claves del éxito de compañías como Alipay, cuyo modelo de negocio se basa en optimizar el procesamiento masivo de transacciones para mejorar el margen global del grupo matriz.

Por otra parte, contar con una gran escala facilita la innovación dado que permite probar y lanzar nuevos productos con mayor rapidez y menor riesgo, como soluciones de pago en tiempo real, pagos integrados o invisibles, mejorando así la experiencia y la fidelización de los clientes.

En suma, aunque el procesamiento de pagos, incluso siendo a gran escala, por sí solo no garantiza una rentabilidad elevada, su ausencia puede representar una desventaja competitiva. Por ello, los actores que intervienen en el ecosistema buscan ser líderes en el procesamiento de pagos, buscando que actúe como catalizador para fortalecer la vinculación del cliente y aumentar los ingresos a través de servicios complementarios.

El uso intensivo de la tecnología no es una opción

En el ámbito de los pagos, el uso intensivo de la tecnología ha dejado de ser una opción estratégica para convertirse en una condición indispensable para la competitividad y la sostenibilidad de los actores del ecosistema.

La tecnología no solo habilita mejoras operativas, sino que también define la capacidad de las instituciones para integrarse a redes de interoperabilidad, adoptar estándares de seguridad avanzados y desarrollar modelos de negocio adaptables a un entorno de innovación constante. Ignorar esta realidad implica quedar rezagado en un mercado cada vez más dinámico, donde la eficiencia, la confiabilidad y la conveniencia tecnológica determinan las reglas de competencia.

Pese a que las inversiones tecnológicas iniciales sean elevadas y su rentabilización pueda tardar en materializarse, resulta obligatorio que las organizaciones que quieran alcanzar o mantener una posición de relevancia en el ecosistema de pagos deban poner foco en una innovación constante (a través, por ejemplo, de la creación de *hubs* de innovación), enfrentándose a la alta incertidumbre inherente a este tipo de emprendimientos (más habitual en las *fintechs* que en la banca tradicional).

Para los actores tradicionales, este desafío tecnológico es doble: no solo tienen que ser capaces de innovar sino, también de conseguir escalabilidad a la vez que conviven con infraestructuras *legacy* heredadas que les dificultan la transformación.

A los hechos comentados se une que la evolución tecnológica del sector de pagos es vertiginosa, y las soluciones innovadoras tienden a estandarizarse rápidamente, lo que requiere una cultura organizacional de cambio profundamente arraigada, capaz de pivotar en función de las nuevas tendencias y de adaptarse de forma ágil. A diferencia de las *fintechs* y las *bigtechs*, las entidades financieras tradicionales suelen carecer de esta cultura de transformación rápida, lo que les supone una desventaja competitiva.

Nuevas formas de delitos financieros

La aparición de nuevos métodos de pago y modelos de negocio genera también nuevos riesgos inherentes, particularmente en lo referente al fraude financiero y al blanqueo de capitales. Este nuevo entorno obliga a actualizar las estrategias de mitigación de riesgos.

El reflejo de la evolución de los servicios de pago en el fraude financiero

La implementación de sistemas de pago más ágiles provoca nuevas formas de fraude financiero entre los que cabe destacar el denominado fraude de Pagos Push Autorizados (APP), donde los delincuentes manipulan a las víctimas mediante técnicas de ingeniería social para que realicen transferencias a cuentas fraudulentas.

Según el informe “Real-time Payments and APP Fraud Emerging Globally” publicado en mayo de 2023 por Aite-Novarica Group⁴⁰ y que se centra en las tendencias de fraude en pagos en tiempo real (RTP) y fraudes de pagos autorizados (APP) (basado en encuestas realizadas a ejecutivos de fraude en instituciones financieras de Brasil, Canadá, India, Reino Unido y EE. UU.):

- El 71% de las instituciones financieras reportaron un aumento en la toma de control de cuentas (ATO) utilizando canales RTP entre 2021 y 2022.
- El 62% observó un incremento en fraudes APP en el mismo período.
- El 57% indicó un aumento en la actividad de cuentas mula sobre canales RTP.

Pero la “innovación” en fraude financiero, no se produce solo en canales RTP. En los últimos tiempos, los defraudadores han puesto también el foco en los monederos digitales y en las criptomonedas. De acuerdo con el informe de Sift⁴¹, los intentos de fraude en transacciones profesionales aumentaron un 66 % y los fraudes con monederos digitales, un 33 % en 2020. Asimismo, el fraude en transacciones de criptomonedas creció un 4,6 %.



Según la European Association for Secure Transactions⁴² (EAST), los fraudes más frecuentes corresponden a transacciones sin presencia física de tarjeta (CNP), seguidas de fraudes con tarjetas físicas y fraudes móviles (véase figura 16).

El Banco de España ha reportado que las reclamaciones por fraude pasaron de 911 en 2019 a 10.361 en 2022, multiplicándose por 11 en cuatro años⁴³ (véase figura 16).

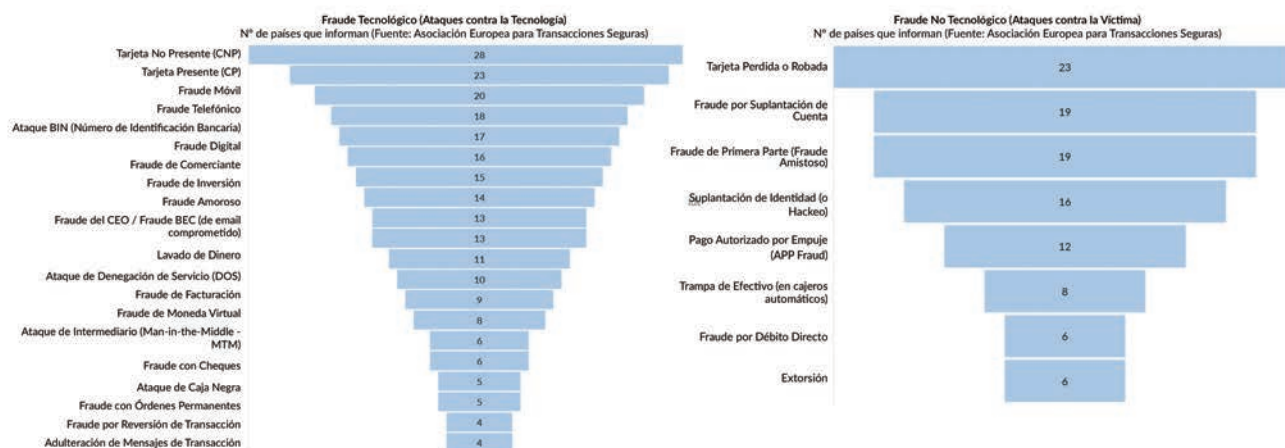
⁴⁰ Aite-Novarica: Faster Payments, Faster Fraud - Outseer™.

⁴¹ Fraud picks up as the economy goes digital during the pandemic, studies find | Payments Dive.

⁴² EAST publishes Fraud Update (association-secure-transactions.eu).

⁴³ Banco de España: memoria de reclamaciones 2022 (Memoria de Reclamaciones 2022).

Figura 16. Tipos de fraude manifestado por las entidades participantes en el estudio.



Hasta la fecha, en 2023, el Grupo de Expertos de EAST sobre el Fraude en Todos los Terminales (EGAF) ha publicado cinco Alertas de Fraude relacionadas con este tema.

Fuente: European Association for Secure Transaction.

Hasta la fecha, en 2023, el Grupo de Expertos en Fraude en los Pagos y las Transacciones (EPTF) de EAST ha publicado una Alerta de Pago relacionada con este tema.



Evolución en los métodos de prevención del fraude

En el ámbito de evolución de los métodos de prevención del fraude destaca la implementación de la autenticación reforzada de clientes (SCA)⁴⁴. En esta línea, el Banco Central Europeo (BCE) y la Autoridad Bancaria Europea (EBA) publicaron un informe conjunto en agosto de 2024⁴⁵ que analiza los datos de fraude en pagos dentro de la UE. El informe destaca que:

- ▶ El valor total de fraudes en 2022 fue de 4.300 millones de euros, reduciéndose a 2.000 millones en la primera mitad de 2023 gracias a la implantación efectiva de la SCA, bajo la PSD2 e indica que las transacciones autenticadas con SCA mostraron tasas de fraude significativamente más bajas, especialmente en pagos con tarjeta.
- ▶ La mayoría del fraude con tarjetas (71% del valor total en la primera mitad de 2023) involucró transacciones transfronterizas, donde la aplicación de SCA no es obligatoria.

Blanqueo de capitales

El blanqueo de capitales es una de las principales amenazas a las que se enfrenta el sector financiero en sus marcos de identificación, gestión y control de riesgos.

Las innovaciones en medios de pago, sobre todo aquellas orientadas a ofrecer servicios financieros a personas excluidas del sistema bancario convencional, como las tarjetas prepago o el uso de criptomonedas, han creado oportunidades en relación con el blanqueo de capitales, tanto para el crimen organizado como para grupos terroristas, favorecidas por el anonimato y la escasa aplicación de controles de diligencia debida por ciertos proveedores.

La forma de combatir y prevenir el blanqueo de capitales requiere cierto grado de sofisticación, según el método de pago que se utilice:

▶ **Tarjetas prepago**⁴⁶. La detección de actividad sospechosa de blanqueo de capitales cuando se utilizan tarjetas prepago, requiere la modelización de comportamientos que no son los que habitualmente están incluidos en los escenarios de detección tradicionales, por ejemplo:

- Clientes que compran muchas tarjetas prepago o que realizan muchas transacciones con este tipo de tarjeta.
- Carga frecuente de las tarjetas prepago, así como su uso solo para retirar dinero en efectivo.
- Carga de fondos por encima del umbral.
- Transferencia de fondos poco después de la carga.
- Clientes que, en respuesta a la notificación de la obligación de informar, se muestra reacio o no diligente a proporcionar la información requerida.
- Transacciones que se producen simultáneamente en varios estados o países fuera de la zona de residencia del titular de la tarjeta.

Con el objetivo de minimizar el creciente riesgo de la utilización de tarjetas prepago para el blanqueo, la UE, por ejemplo, ha endurecido la normativa a través de la quinta directiva contra el blanqueo de capitales, en el que ha reducido el límite de transacciones con tarjetas prepago⁴⁷.

▶ **Criptomonedas**. Hasta hace poco tiempo, la falta de regulación ha sido uno de los principales facilitadores del blanqueo de capitales a través del uso de criptomonedas. Sin embargo, iniciativas como la regulación sobre Transferencias de Fondos (TFR) o el reglamento MiCA desarrollados en Europa van reforzando las medidas de control al imponer requisitos, tanto a emisores como a proveedores del mercado de criptomonedas, de transparencia en la información y registro.

El proceso de *Know Your Customer* (KYC) sigue siendo la primera línea de defensa frente al blanqueo de capitales y, dado el repunte de casos notorios que afectan a bancos con importancia mundial sistémica, una de las actividades de prevención del delito financiero que más inversiones ha atraído en los últimos años, por ejemplo, para incluir capacidades automáticas de verificación de documentos, de verificación de la identidad, de control de personal políticamente expuesto (PEP), de análisis biométrico del rostro, etc.

⁴⁴Strong Customer Authentication | Visa.

⁴⁵<https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf>

⁴⁶La Guía Esencial Para El Blanqueo De Dinero Con Tarjetas De Prepago (financialcrimeacademy.org).

⁴⁷La Directiva (UE) 2018/843, conocida como la Quinta Directiva contra el Blanqueo de Capitales, introdujo modificaciones significativas respecto a las tarjetas de prepago anónimas. Específicamente, redujo el umbral para la identificación de los titulares de estas tarjetas de 250 euros a 150 euros. Además, estableció un límite de 50 euros para las transacciones remotas o en línea realizadas con tarjetas de prepago anónimas (<https://eur-lex.europa.eu/ES/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes-until-2027>).