

Challenges faced by the payments ecosystem participants

"Banks that understand technology will survive. Those that don't will disappear."

A paraphrase of Chris Skinner - British author, speaker and consultant, recognized as one of the world's leading experts on digital transformation in financial services, banking, financial technology (fintech) and the future of money - in his book Digital Bank (2014).

The payments ecosystem is undergoing a significant transformation, driven by digitalization, technological evolution and changing consumer demands. This transformation presents significant challenges for financial and non-financial institutions. In this context, it is crucial for organizations to understand and adapt to these changes in order to remain competitive and take advantage of new business opportunities.

Scale matters

In the payments arena, scale is a crucial factor, but not the only determinant of financial success. The ability to handle a large volume of transactions is essential for any entity wishing to compete efficiently.

However, the payments business is not sustained exclusively by the fees generated per transaction, since these tend to decrease progressively and, in some models, are not sufficient to guarantee long-term profitability or to finance the necessary technological investments. The real importance of scale lies in its ability to act as an enabler of more lucrative complementary services. A large customer base and a high volume of transactions allow a significant amount of data to be collected, which can be leveraged to offer additional financial products such as credit, insurance, investments and personalized services.

In addition, scale makes it possible to negotiate better rates with suppliers and reduce operating costs through economies of scale. This not only improves efficiency, but also makes it possible to offer more competitive prices, thus attracting more customers and further strengthening growth. This phenomenon has been one of the keys to the success of companies such as Alipay, whose business model is based on optimizing the mass processing of transactions to improve the parent group's overall margin.

On the other hand, having a large scale facilitates innovation, as it enables faster and lower-risk testing and deployment of new products – such as real-time payment solutions, integrated payments, or invisible payments, ultimately enhancing customer experience and loyalty.

In short, although payment processing – even on a large scale – does not guarantee high profitability on its own, its absence can represent a competitive disadvantage. Therefore, players within the ecosystem strive to become leaders in payment processing, aiming for it to act as a catalyst to strengthen customer loyalty and increase revenues through complementary services.

Intensive use of technology is not an option

In the area of payments, the intensive use of technology has ceased to be a strategic option and has become an indispensable condition for the competitiveness and sustainability of the players in the ecosystem.

Technology not only enables operational improvements, but also defines the ability of institutions to integrate interoperability networks, adopt advanced security standards and develop business models that are adaptable to an environment of constant innovation. Ignoring this reality means being left behind in an increasingly dynamic market, where efficiency, reliability and technological convenience determine the rules of competition.

Although the initial technological investments are high and their profitability may take time to materialize, organizations that want to reach or maintain a position of relevance in the payments ecosystem must focus on constant innovation – through, for example, the creation of innovation hubs – and face the high uncertainty inherent in such ventures (more common in fintechs than in traditional banking).

For traditional players, this technological challenge is twofold: not only do they have to be able to innovate, but also to achieve scalability while living with legacy infrastructures that make transformation difficult.

In addition to these facts, the technological evolution of the payments industry is dizzying, and innovative solutions tend to standardize quickly, which requires a deeply rooted organizational culture of change, capable of pivoting according to new trends and adapting in an agile manner. Unlike fintechs and bigtechs, traditional financial institutions often lack this culture of rapid transformation, which puts them at a competitive disadvantage.

New forms of financial crime

The emergence of new payment methods and business models also introduces new inherent risks, particularly in relation with financial fraud and money laundering. This new landscape makes it necessary to update risk mitigation strategies.

How changes in Payment Services are reflecting in Financial Fraud

The implementation of more agile payment systems has led to new forms of financial fraud, including the so-called Authorized Push Payment (APP) fraud, where criminals manipulate victims through social engineering techniques to induce transfers to fraudulent accounts.

According to the report "Real-time Payments and APP Fraud Emerging Globally," published in May 2023 by Aite-Novarica Group⁴⁰, which focuses on fraud trends in real-time payment (RTP) and authorized push payment (APP) - based on surveys of fraud executives from financial institutions in Brazil, Canada, India, the UK and the US:

- ▶ 71% of financial institutions reported an increase in account takeover (ATO) via real-time payment (RTP) channels between 2021 and 2022.
- ▶ 62% observed an increase in authorized push payment (APP) fraud over the same period.
- ▶ 57% indicated an increase in mule account activity on RTP channels.

But "innovation" in financial fraud is not only occurring in RTP channels. Recently, fraudsters have also turned their attention to digital wallets and cryptocurrencies. According to Sift's report⁴¹, fraud attempts in professional transactions increased by 66 % and digital wallet fraud by 33 % in 2020. Likewise, fraud in cryptocurrency transactions grew by 4.6%.



According to the European Association for Secure Transactions⁴² (EAST), the most frequent frauds are card-not-present (CNP) transactions, followed by physical card fraud and mobile fraud (see Figure 16).

The Banco de España has reported that fraud claims rose from 911 in 2019 to 10,361 in 2022, increasing 11-fold in four years⁴³ (see Figure 16).

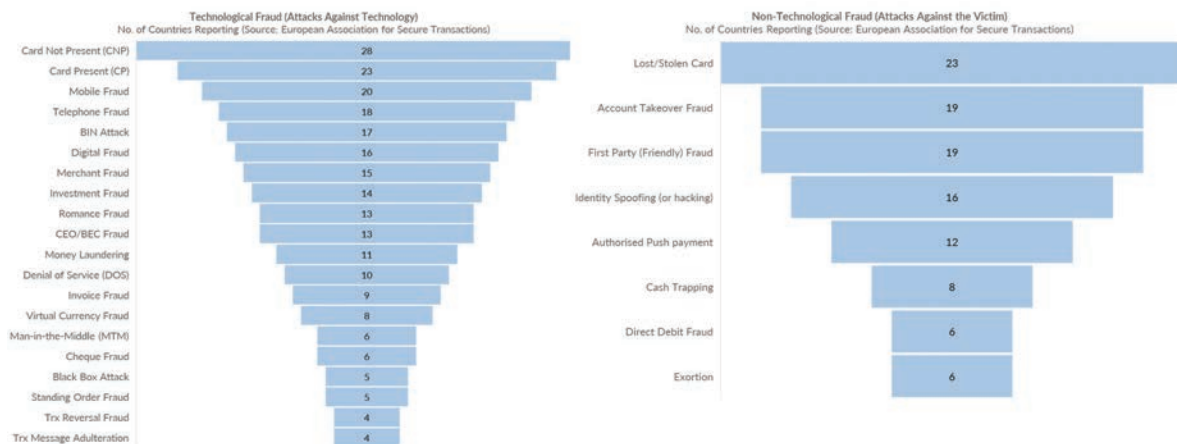
⁴⁰Aite-Novarica: Faster Payments, Faster Fraud - Outseer™.

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

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

⁴³Bank of Spain: Claims Report 2022 (Memoria de Reclamaciones 2022).

Figure 16. Types of fraud reported by entities participating in the study.



To date in 2023 the EAST Expert Group on All Terminal Fraud (EGAF) has published five related Fraud Alert

To date in 2023 the EAST Expert Group on Payment and Transaction Fraud (EPTF) has published one related Payment Alert.

Source: European Association for Secure Transactions.



Developments in fraud prevention methods

In the evolution of fraud prevention methods, the implementation of Strong Customer Authentication (SCA)⁴⁴ stands out. In this context, the European Central Bank (ECB) and the European Banking Authority (EBA) published a joint report in August 2024⁴⁵ analyzing payment fraud data within the EU. The report highlights the following:

- ▶ The total value of fraud was €4.3 billion in 2022, decreasing to €2 billion in the first half of 2023, thanks to the effective implementation of SCA under PSD2. Transactions authenticated with SCA showed significantly lower fraud rates, especially in card payments.
- ▶ The majority of card fraud (71% of total value in the first half of 2023) involved cross-border transactions, where the application of SCA is not mandatory.

Money laundering

Money laundering is one of the main threats facing the financial sector in its risk identification, management and control frameworks.

Innovations in payment methods – especially those aimed at offering financial services to people excluded from the conventional banking system, such as prepaid cards and the use of cryptocurrencies, have created opportunities in relation to money laundering, both for organized crime and terrorist groups, favored by anonymity and the poor application of due diligence controls by certain providers.

Combatting and preventing money laundering requires a certain level of sophistication, depending on the payment method used:

- ▶ **Prepaid cards**⁴⁶. The detection of suspicious money laundering activity involving prepaid cards requires the modeling of behaviors that are not typically included in traditional detection scenarios, for example:
 - Customers who buy a lot of prepaid cards or who make a lot of transactions with this type of card.
 - Frequent loading of prepaid cards, as well as their use only for cash withdrawals.
 - Loading funds above the threshold.
 - Transfer of funds shortly after loading.
 - Customer who, in response to the notification of the obligation to report, is reluctant or not diligent in providing the required information.
 - Transactions occurring simultaneously in several states or countries outside the cardholder's area of residence.

To minimize the growing risk of prepaid cards being used for money laundering, the European Union has tightened regulations through the Fifth Anti-Money Laundering Directive (5AMLD), which includes a reduction in the transaction limit for prepaid cards⁴⁷.

- ▶ **Cryptocurrencies**. Until recently, the lack of regulation has been one of the main enablers of money laundering through the use of cryptocurrencies. However, initiatives such as the Transfer of Funds Regulation (TFR) or the MiCA regulation developed in Europe are reinforcing control measures by imposing transparency and registration requirements on both issuers and service providers in the cryptocurrency market.

The Know Your Customer (KYC) process remains the first line of defense against money laundering. In light of the rise in high-profile cases involving globally systemically important banks, KYC has become one of the financial crime prevention activities that has attracted the most investment in recent years. This includes the adoption of technologies such as automated document verification, identity verification, politically exposed personnel (PEP) screening and biometric face analysis.

⁴⁴Strong Customer Authentication | Visa.

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

⁴⁶The Essential Guide To Money Laundering With Prepaid Cards (financialcrimeacademy.org).

⁴⁷Directive (EU) 2018/843, known as the Fifth Anti-Money Laundering Directive, introduced significant amendments regarding anonymous prepaid cards. Specifically, it lowered the threshold for mandatory identification of card holders from €250 to €150. In addition, it established a limit of €50 for remote or online transactions conducted with anonymous prepaid cards (<https://eur-lex.europa.eu/ES/legal-content/summary/preventing-abuse-of-the-financial-system-for-money-laundering-and-terrorism-purposes-until-2027>).