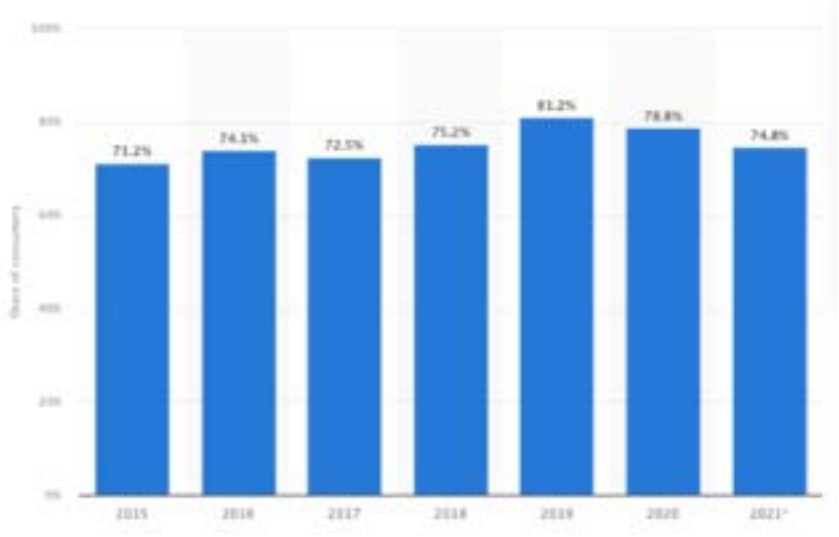
Digital payments: why it is vital to prevent fraud and how to do it?

June 20, 2022

Contactless payments and payments via QR codes, purchases on e-commerce platforms through all kinds of devices, among other online transactions present a challenge to the providers of these services and financial institutions seeking to improve their anti-fraud strategies, which marks a distinctive feature in the post-pandemic era in terms of retaining customers and offering a unique and memorable experience.

Although fraud through electronic payments is booming with the boom of digital financial solutions, companies have the ability to anticipate to avoid losing the trust of its users and avoid heavy economic losses, according to Preventor, a firm that specializes in identity verification solutions.

Last year 74.8% of the victims of online shopping fraud lost money worldwide through these attacks, a figure that although it has remained stable in recent years represents a jump compared to 71.2% in 2015, which leads to rethink the way in which these threats are being managed (Evolution from 2015 to 2021 in Statista's graph).



Online transactions became popular at an unprecedented speed during the confinement in many countries and despite the economic revival this trend continues, but not without challenges as many companies not only in the e-commerce industry but also in the financial industry, have to deal daily with the anti-fraud fight in the different products used by their users.

Preventing identity fraud in online payments requires adopting a layered approach which integrates different technologies in order to create barriers that can curb altogether or at least mitigate the impact of these events, avoiding penalties for companies and making the acceptance of legitimate customers more efficient.

As a result, more and more online payment services are adopting a whole battery of solutions that allow them, for example, to access global document databases in order to verify a user's identity, as well as perform biometric checks, document

analysis and token validations to keep cybercriminals at bay, as is done by the firm Preventor, which specializes in the sector.

"Payment service providers must work to ensure transparent global structures and build trust and visibility with respect to customer acceptance, their ability to assume credit risk and ensure efficient global monitoring structures,"a report by consultancy PwC says in this regard.

Among the main anti-fraud tools, the British consulting firm names, among others, those that are based on machine learning, which allow organizations to react against fraud practically in real time.

Also noteworthy are solutions based on analytics that, by means of statistical models, are capable of identifying operations that could be considered fraudulent based on the natural behavior of customers.

And finally, among the main trends to anticipate fraud in digital payments are modeling tools used to attack the so-called mule accounts, which are opened under false identities and are basically used to commit fraud and even money laundering. With this type of solutions it is possible to identify the patterns of these accounts to deactivate them and follow the trail of those who operate through this modality.

Avoiding the frauds in the future

Today, "fraud happens faster because fraudsters export models that worked in one region to another that is adopting similar technology," according to a report released by SAS, showing that this type of crime has taken on a global dimension never seen before.

To prevent these attacks, which caused losses of around US$20 billion to e-commerce alone in 2021, an increase of 14% compared to 2020, it is necessary to move at the speed with which the attackers are acting and not to skimp on investments.

This battle against fraud requires both payment service providers and financial institutions to work hand in hand to ensure the traceability of online transactions while preserving the security of the products used in these at a time when the phishing or deep counterfeiting are the order of the day.

In this regard, a report by the Financial Stability Institute (FSI) urges to "draw attention to these crimes so that financial institutions and the general public are better informed", in addition to promoting "additional vigilance with respect to the growing and evolving risks" and promoting "an active exchange of information between the public and private sectors" with the aim of stopping this financial crime.

Change of vision

As new technologies appear to shield users from fraud through electronic and instant payments, these types of attacks are diversifying and evolving at an accelerated pace to the point that they marked their highest rate in 2021 (37%) at least since 2018, before the pandemic, according to different figures consulted from the cybersecurity industry.

What is most striking is that despite their rigid regulations, the fintech and payment service providers (PSP) sector recorded in 2021 the highest fraud rate with 43%, higher than other sectors such as IT solutions or gaming.

Thus, identity verification and fraud prevention policies have become an asset within organizations and a differential in the midst of the diversity of offers in the online payment industry, participating in the different stages of the relationship with users.

Preventor warns that many organizations assume a rigid posture that prevents them from seeing the threats and end up paying the cost of not knowing the power that technology gives them today in order to anticipate, complying with regulations and finding the right point to keep users satisfied with the effectiveness of the service, while at the same time offering them security.

Responding to these threats implies a change of vision in the way these risks are addressed, which entails changing the culture of organizations, improving certain practices and automating responses to anomalous behavior in daily operations.

Against this backdrop, it is important for companies to focus on prevention and to strengthen their strategy against the diversification of threats as electronic payment services become more relevant in the everyday lives of users, who will strengthen their relationships with those services that offer them constant guarantees, simplify processes and adopt the technologies they are used to interacting with.