Client onboarding: the next frontier in the fight against digital fraud

April 19, 2022

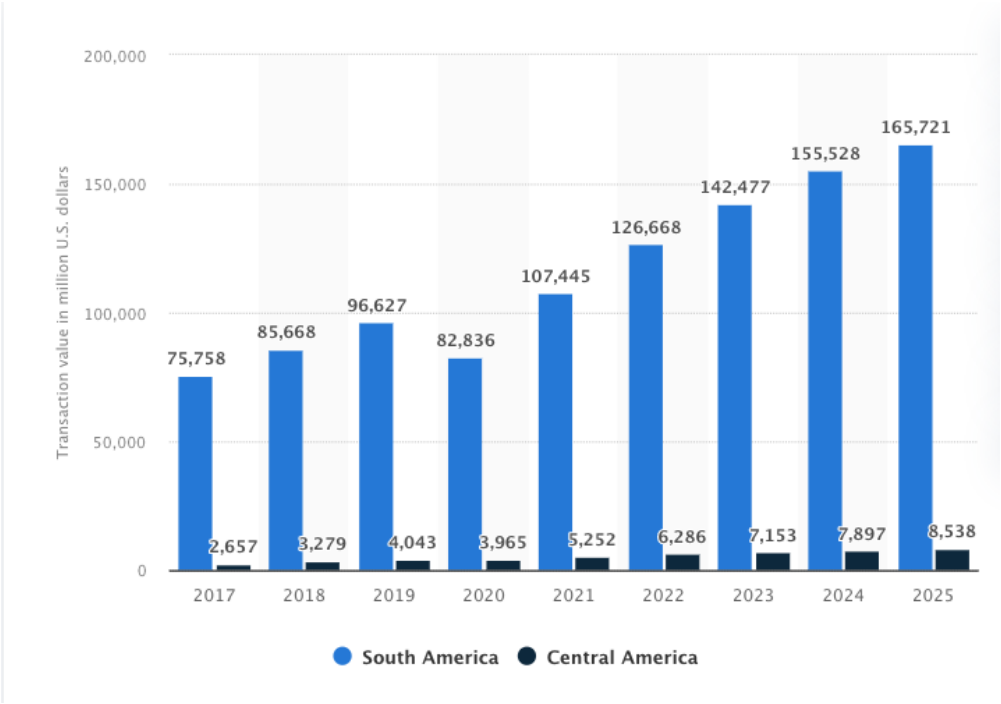
With millions of transactions taking place every day online, the rise of e-commerce and digital and no-contact payments is driving companies to strengthen their anti-fraud strategies in the face of advanced latent threats, which leave heavy losses and huge reputational cracks.

In a highly digitized scenario, attackers take advantage of vulnerabilities in the infrastructure of these organizations and those of their users, forcing them to improve their digital onboarding and Know Your Customer (KYC) processes.

Digital and contactless payments are gaining ground in Latin America along with the disruption of services through platforms in the region, ranging from

transactions with financial institutions, to the entertainment sector and food delivery.

An indication of the impact of this business is that the value of digital commerce transactions could reach US$113 billion this year in Latin America, although forecasts suggest that this figure could reach US$174 billion by 2025 as more companies adopt digital payments, according to statistics from Statista. (Statista graphic)



On this issue, a World Bank report concluded that 42% of adults in the region use digital payments in commerce, while for 11% the pandemic was a trigger and therefore adopted this modality in the context of the crisis.

"Regionally, nearly 50 million adults adopted digital payments in stores during the pandemic. However, the degree of adoption varies across the region," says the World Bank report.

But beyond this growth, as the adoption of digital and non-contact payments accelerated not only in Latin America but in many markets around the world, the

risks associated with cybersecurity also became evident, mainly in terms of identity verification and fraud, as analyzed by the specialized firm

Data from research firm Javelin Strategy & Research's 2022 Identity Fraud Study: The Virtual Battleground report shows the magnitude of identity fraud in developed markets such as the United States.

According to their calculations, these breaches generated in digital transactions affected some 42 million adults in that country, leaving a balance of US$52 billion in losses in 2021, a year where the cyber criminals relied on tactics such as bot attacks and malware.

These types of malicious campaigns take advantage not only of vulnerabilities in the infrastructure of these systems, but also of users' bad practices through social engineering techniques, with which they exploit these breaches to their advantage.
Just to cite one example, worldwide "ransomware attacks cost an average of US$4.62 million, more expensive than the average data breach (US$4.24 million)," according to IBM's Cost of a Data Breach Report 2021.

Automation, the armor against fraud

Along with technological advances, the strategies for committing this type of fraud are based on pioneering digital tools, so it is important for companies to be aware that they must protect themselves with tools that are up to these challenges and at the same time guarantee the traceability of these operations.

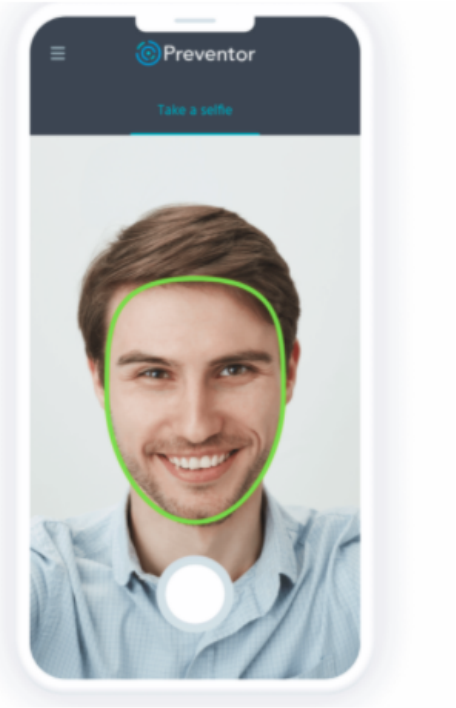
Preventor sees it as key that this wave of e-commerce and virtual payments is supported by digital automation and artificial intelligence in its different processes in order to fight against fraud and identity theft, in the midst of the constant threats faced by organizations.

Thus, the incorporation of new customers in companies that perform critical processes, such as financial or insurance companies, is increasingly leveraging these tools in order to validate the identity of their users in seconds.

This process is crucial and in most cases defines the longevity of the company-customer relationship, which must be based on process efficiency, transparency, agility and security.

In line with current challenges, the verification of identity today relies on top-level tools such as biometrics, with high-definition images, or voice recognition to make these processes simple and effective.

Preventor, for example, uses optical character reading (OCR) technology which is capable of extracting data from any ID document automatically, displacing cumbersome processes and reducing them to just 60 seconds. In addition, this analysis makes it possible to verify the information in the machine-readable areas of electronic documents, thus ensuring much more efficient and secure onboarding processes.



Thanks to NFC technology, through which data can be exchanged between contactless devices, other key information can also be extracted in order to advance these identity verification processes, including barcodes and RFID chips, which use radio signals acting as localization systems.

According to a PwC blog post authored by the firm's UK Banking and Capital Markets partner James Morgan, "it is not surprising when lending decisions can take up to 100 days or more" because of tortuous processes that scare off customers.

This is why he believes that "the future success of banking depends on the value the industry attaches to its customer relationships and this starts with onboarding," as well as valid authentication processes and effective Know Your Customer policies in order to take full advantage of this wave of digitization that has brought e-commerce and digital payments to the forefront.

In short, these technologies are key because thanks to them companies in sectors such as retail or e-commerce can increase their sales, allowing scalability and geographic expansion, but above all improve the end user experience and privacy, according to Preventor.

On the side of financial institutions, this is also decisive since the automation of the digital onboarding process facilitates the approval of instant loans and microcredits, changing the paradigm since personal information is obtained directly electronically and not manually by an employee of the establishment, reducing or eliminating possible identity theft.