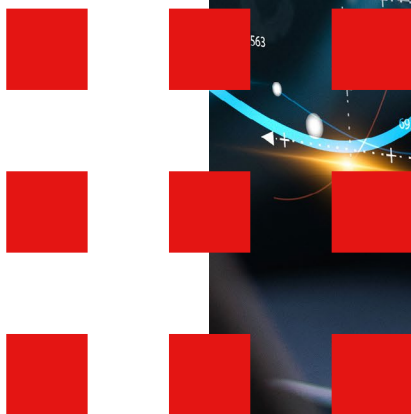


Combating the changing nature of fraud





Combatting the changing
nature of fraud

Intro

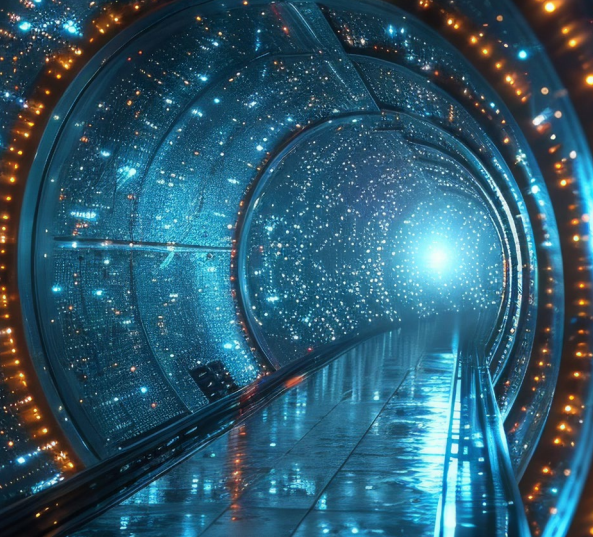
The fraud landscape is evolving at an alarming rate. The combination of economic change – coupled with the ever-increasing sophistication of fraudsters – has changed the landscape significantly over recent years.

In fact, research suggests that nearly [seven in ten businesses](#) worldwide believe that fraud losses have increased, while over half of all consumers feel they're more of a target for fraud than they were a year ago. In Brazil, there were a staggering [2,800](#) financial fraud attempts per minute in electronic channels in the first quarter of 2023 alone. In fact, [one in five](#) e-commerce transactions in Latin America is declined as fraudulent – twice as high as any other region globally. Meanwhile, in Spain, fraud attacks increased by [117%](#) in 2023, reaching recorded losses of €250 million.

The reasons behind rising fraud figures are multifaceted, reflecting the evolving tactics of sophisticated criminals. While fraudsters are finding new ways to exploit security loopholes in financial products and services, companies like Getnet are rapidly developing innovative countermeasures. Scams now take various forms – from romance to investment, purchase to impersonation. The financial industry is responding with equal sophistication, leveraging cutting-edge AI, machine learning, and biometric authentication to protect clients. This technological arms race is increasingly tipping in favour of security providers, enhancing protection for consumers and businesses alike.

With such speed of change, this paper aims to set out a comprehensive overview of the fraud landscape and highlight effective strategies for merchants to combat fraud, enhance security, and build customer trust. To ensure our insights are grounded in real-world concerns, Getnet conducted in-depth interviews with 24 selected merchants across Brazil, Mexico and Spain to identify the problems worth solving and understand their main concerns and expectations from payment providers in ensuring their peace of mind. Getnet then surveyed 900 respondents to further test the popularity of the behaviours and attitudes identified. The valuable findings from this research are incorporated throughout this paper.

In doing so, we aim to empower all businesses with the knowledge and tools necessary to stay ahead of fraudulent activities and to build a future-proof commercial environment.



Combatting the changing
nature of fraud

01

Understanding the
fraud landscape

The current trends in the fraud landscape are inexorably shaped by the proliferation of online transactions and the widespread adoption of digital payment methods. As consumers increasingly embrace the convenience of e-commerce and mobile banking, cybercriminals have seized upon these digital platforms as fertile hunting grounds. The COVID-19 pandemic served as a catalyst, accelerating the shift towards online shopping and financial transactions, providing fraudsters with an abundance of new opportunities to exploit.

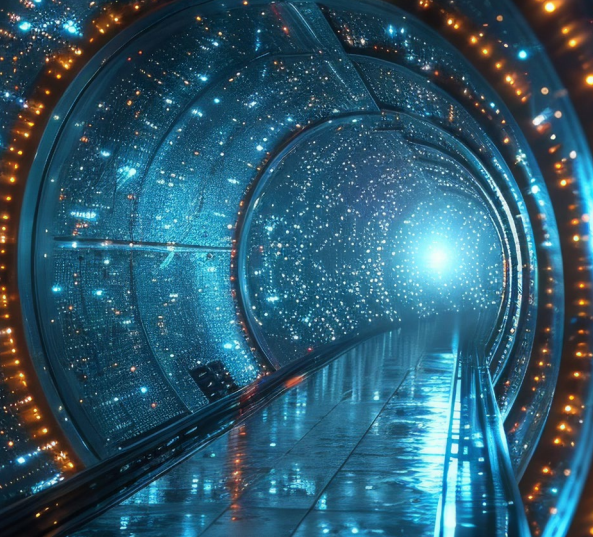
Among the most pervasive forms of payment fraud are identity theft, card-not-present (CNP) fraud, and account takeover (ATO) attacks. Identity theft involves the fraudulent acquisition and misuse of an individual's personal information, such as name, date of birth, and financial details, to facilitate unauthorised transactions or open new accounts.

CNP fraud, on the other hand, occurs when stolen payment card information is used for illicit online or over-the-phone purchases without the physical card being present. ATO attacks, meanwhile, involve cybercriminals gaining unauthorised access to victims' online accounts, enabling them to initiate fraudulent transactions or siphon funds.



"The threat landscape is constantly shifting, and fraudsters are becoming increasingly sophisticated in their tactics. It is crucial for businesses to stay ahead of the curve by adopting a proactive and multi-faceted approach to fraud prevention."

Kush Saxena, CEO PagoNxt Merchant.

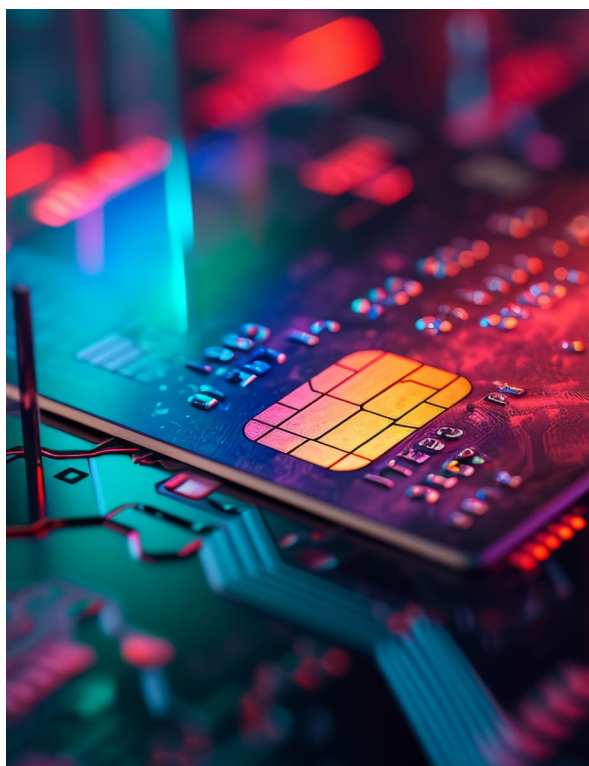


Combating the changing nature of fraud

01

Understanding the fraud landscape

Regulators are increasing efforts to mitigate fraud. However, the complexity of the regulatory landscape adds a challenge for merchants, particularly those who sell across borders. Stringent compliance requirements, such as those outlined in the Payment Services Directive 2 (PSD2) and the General Data Protection Regulation (GDPR), demand rigorous data protection and authentication protocols, necessitating significant investments in security infrastructure and personnel training.



Despite the best intentions of merchants, financial service providers and regulators, fraud can still have a devastating impact; one which extends far beyond mere monetary losses. For businesses, the direct financial costs are compounded by indirect expenses associated with reputational damage, customer churn, and the need for implementation of robust fraud detection and prevention measures. Consumers, too, bear the brunt of fraud, facing not only the potential loss of funds but also the arduous process of resolving the aftermath and restoring their financial standing.

As fraudsters continue to leverage cutting-edge technologies and exploit emerging vulnerabilities, businesses must remain vigilant and adaptable, continuously refining their fraud detection and prevention strategies to stay one step ahead of these nefarious actors.



Combatting the changing
nature of fraud

02

Empowering
merchants to
combat fraud

Merchant education and training are crucial for fostering a culture of vigilance against fraud within organisations. Our research found that at least **one in five (17%) merchants view security as a low concern** and are characterised by purchasing solutions that offer tangible business value at an affordable price. However, this mindset can leave businesses vulnerable to the ever-evolving tactics employed by fraudsters.

We also found that merchants can be segmented into four archetypes based on their levels of security concern and ownership: **Proactive Guardian, Laid-back Keeper, Carefree Trader, and Effortless Steward.** Each archetype demonstrates distinct attitudes towards security, necessitating tailored messaging and solutions:

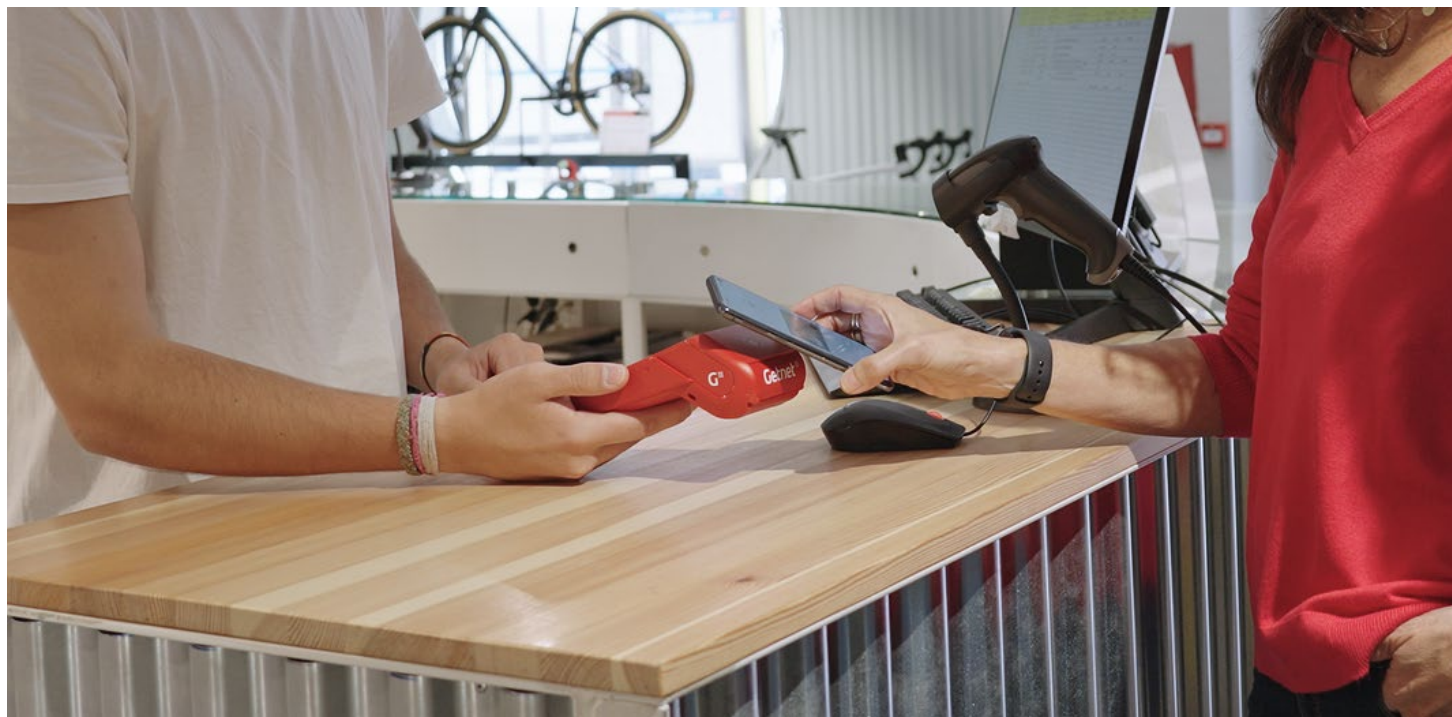
- **Proactive Guardians:** These merchants, making up 33% of the sample, have a keen understanding of risks and a vested interest in security solutions. They are more likely to invest in advanced security measures due to their high knowledge and previous bad experiences with fraud, cyberattacks, and theft.
- **Laid-back Keepers:** Comprising 45% of the sample, they show moderate concern for security, often due to past experiences such as robbery or fraud. Their approach is often reactive, taking steps to improve security when prompted by incidents.
- **Effortless Stewards:** Representing 5% of the sample, these merchants are aware of security risks but prefer to outsource security tasks to third-party providers. They prioritise peace of mind and operational ease.
- **Carefree Traders:** This group, accounting for 17% of the sample, exhibits the lowest security concern and least interest in security solutions. They tend to rely on the assumption that security is inherently provided by their payment systems and focus more on solutions that enhance business value at an affordable cost.



Combatting the changing
nature of fraud

02

Empowering
merchants to
combat fraud



To effectively empower merchants to combat fraud, it is crucial to tailor strategies and solutions to the distinct needs and attitudes of each archetype. For instance, **Proactive Guardians** are already knowledgeable and invested in security measures. To further empower this group, advanced training programs that delve into the latest fraud trends, sophisticated attack vectors, and emerging security technologies can be highly beneficial. These programs should be designed to keep them ahead of the curve and reinforce their proactive stance. Meanwhile, **Carefree Traders** prioritise business value and affordability. Providing cost-effective security solutions

that offer tangible benefits without significant investment can appeal to this group. Bundling security features with other business solutions they value can also increase adoption.

The diversity of these four archetypes underscores the critical need for collaboration among merchants and industry stakeholders. By fostering an environment of open communication and knowledge-sharing, businesses can exchange insights, best practices, and actionable intelligence. This collective effort is essential for staying ahead of evolving fraud tactics and ensuring a secure and trustworthy commercial environment.



Combating the changing
nature of fraud

03

Embracing cutting-edge
tech for fraud prevention

Innovations in fraud prevention technologies offer promising avenues for combating evolving threats. As fraud techniques become more sophisticated, leveraging advanced technology is crucial in staying ahead. Three key technological advancements — **Machine Learning and AI, Biometric Authentication, and Behavioural Analytics** — play significant roles in enhancing security measures.



"In the face of evolving threats, leveraging cutting-edge technology is not just a strategy but a necessity. Merchants need the most advanced tools to combat fraud effectively, ensuring that their business can operate securely and confidently in an increasingly digital world."

**Rodrigo Braga, CEO at PagoNxt
Merchant Solutions Brazil.**



Combatting the changing
nature of fraud

03

Embracing cutting-edge
tech for fraud prevention

MACHINE LEARNING
AND AI

Machine learning algorithms and AI-driven systems have revolutionised fraud detection by enabling adaptive and proactive approaches. These technologies leverage vast datasets to train models capable of identifying intricate patterns and anomalies indicative of fraudulent activity.

By analysing transaction data in real-time, AI systems can detect suspicious behaviours that deviate from normal patterns. This real-time monitoring allows for swift responses to suspicious transactions, minimising potential losses and mitigating risks to both businesses and consumers.

Furthermore, AI systems continuously learn and evolve, improving their accuracy and effectiveness over time. Best in class solutions incorporate these advanced technologies to bolster existing merchant practices, aligning with proactive security strategies that many merchants already employ.

Leading the charge in AI-driven fraud prevention, our proprietary technological platform in Brasil has been leveraging artificial intelligence to assess the risk of fraud on 100% of transactions in real time for the past three years. In 2024, significant investments were made to update these tools, promising even greater efficiency and security. The implementation of new models in May 2024 has already shown promising results, setting a new standard in the market for reliable payment experiences.



Combating the changing
nature of fraud

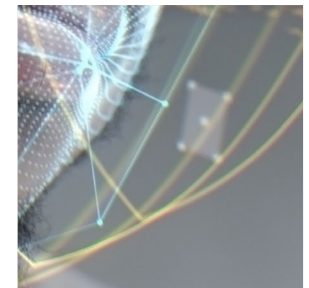
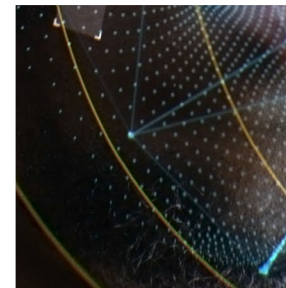
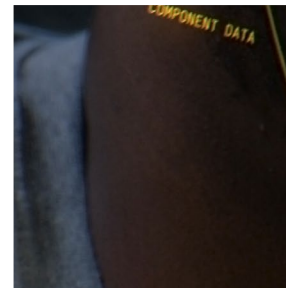
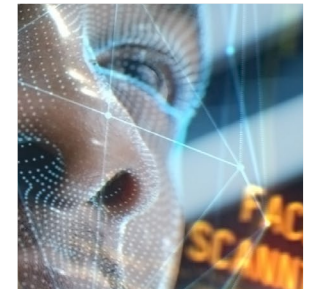
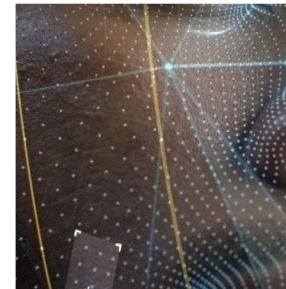
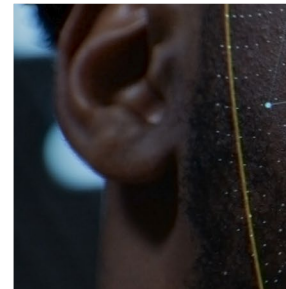
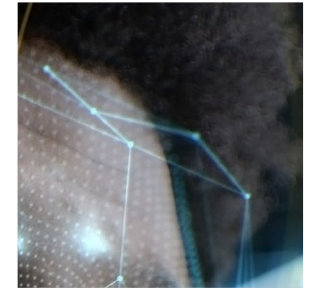
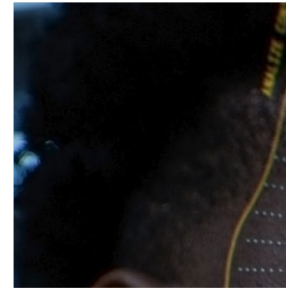
03

Embracing cutting-edge
tech for fraud prevention


BIOMETRIC
AUTHENTICATION

Biometric authentication offers a robust layer of security by verifying users' identities through unique physiological characteristics. Technologies such as fingerprint scanning, facial recognition, and voice authentication provide reliable means of authentication, reducing reliance on easily compromised credentials.

By incorporating biometric authentication into payment processes, businesses can enhance security while simultaneously improving user experience and convenience. For instance, fingerprint or facial recognition can streamline the authentication process for customers, making transactions both secure and seamless. These methods are particularly valuable in preventing unauthorised access and ensuring that the person initiating a transaction is the legitimate account holder.



Getnet's use of facial biometrics exemplifies the power of this technology in creating a seamless and secure user experience. By utilising a tool with proof-of-life capabilities and access to the country's largest facial databases, Getnet offers a fluid experience that guarantees identification with a high level of accuracy. The entire process is digital, allowing for complete customer registration in minutes. This user-friendly approach capitalises on people's familiarity with mobile phones and taking selfies, making the security process both robust and accessible.



Combatting the changing
nature of fraud

03

Embracing cutting-edge
tech for fraud prevention

BEHAVIOURAL
ANALYTICS

Behavioural analytics solutions analyse user interactions and behaviour patterns to detect deviations from established norms. By establishing baseline behaviours for individual users, these systems can identify suspicious activities indicative of fraud or account takeover attempts. Continuous monitoring and analysis of behavioural data enable adaptive responses, allowing businesses to dynamically adjust security measures to counter evolving threats. This approach not only helps in detecting fraud but also in understanding user behaviour better, which can enhance customer service and personalisation efforts.

Getnet's fraud prevention services

Getnet's fraud prevention offerings are meticulously designed to align with the proactive and reactive security strategies employed by merchants. We follow a detect, protect and respond methodology to give peace of mind to our customers. This includes certified payments, backup payment methods, and cyber insurance, which have been identified as the most appealing for merchants across Latin America and Spain. Our approach offers the highest level of transaction security, while backup payment methods provide a safety net in case of primary system failures.



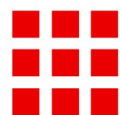


Combating the changing nature of fraud

03

Embracing cutting-edge tech for fraud prevention

BEHAVIOURAL ANALYTICS



Anti-fraud tools for Merchants

Leveraging the fraud capacity to offer a full protection

Detect

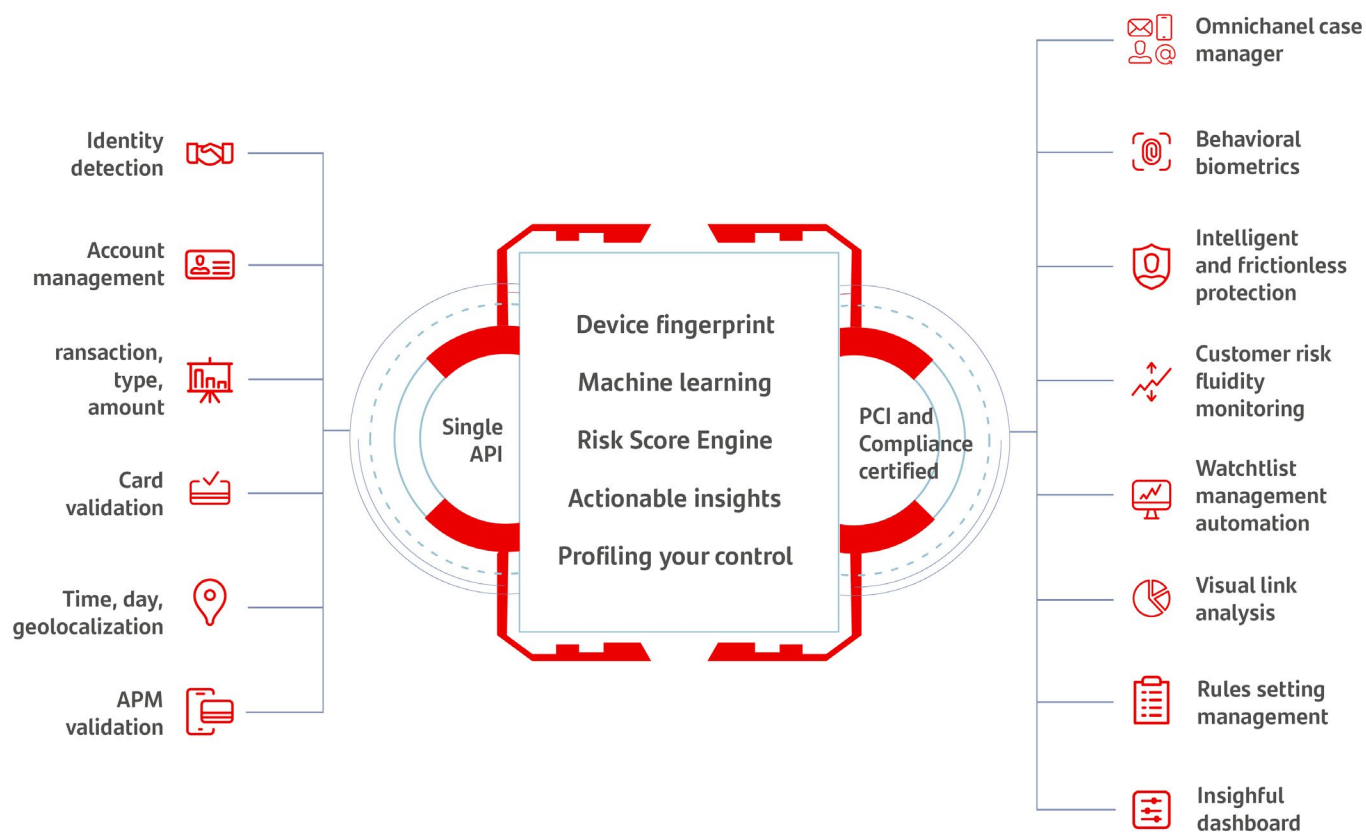
Single platform, single experience.

Protect

Lower customer friction.
Stronger fraud detection.

Respond

Early risk management.
Cost optimization.





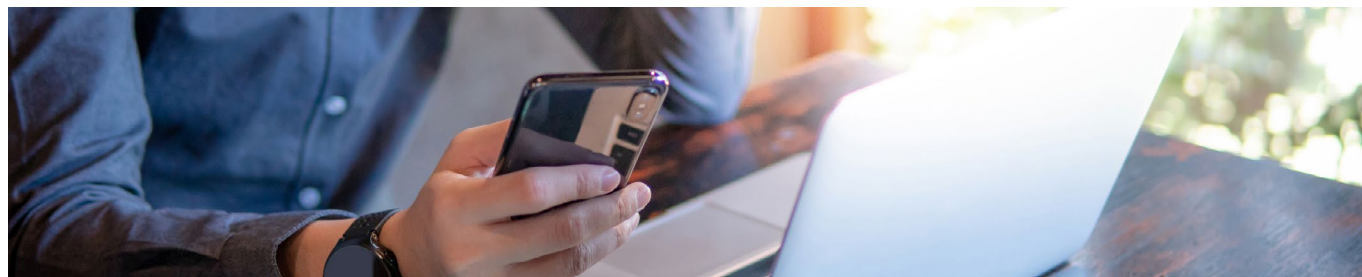
Combatting the changing
nature of fraud

04

Enhancing
customer trust
and confidence

While implementing robust fraud prevention measures is crucial, it is equally important to prioritise customer trust and confidence. **Transparency in payment processes and clear communication of security measures** can go a

long way in reassuring customers and building trust. Ensuring that customers feel secure when conducting transactions not only protects their sensitive information but also fosters loyalty and long-term relationships.



There are three key areas which merchants must prioritise in order to build trust:

1 Offering secure payment options

Offering secure payment options, such as tokenization and two-factor authentication (2FA), provides additional layers of protection for sensitive information. Tokenization replaces sensitive card information with a unique identifier or "token" that is useless to fraudsters if intercepted. This method significantly reduces the risk of data breaches and instils confidence in customers that their information is safe. Two-factor authentication adds another layer of security by requiring a second form of verification, such as a code sent to the customer's mobile device, before completing a transaction. These measures ensure that only authorised users can access their accounts, making it much harder for fraudsters to succeed.

2 Transparency and communication

Transparency in payment processes and security measures is key to building customer trust. Clear communication about the steps taken to protect customer data can reassure them that their security is a top priority. This can include regular updates on security protocols, easy-to-understand privacy policies, and visible security badges on websites and payment portals. Educating customers on how to recognise and avoid phishing attempts and other common scams can also empower them to protect themselves.



Combating the changing
nature of fraud

04

Enhancing
customer trust
and confidence

3 Responsive customer support

Responsive customer support channels are essential for providing timely assistance to customers affected by fraud. Having a dedicated fraud response team that can quickly address issues and help customers recover from fraudulent activities enhances satisfaction and loyalty. Customers need to know that if they encounter a problem, there is a reliable support system in place to assist them. This includes offering multiple support channels, such as phone, email, and live chat, to ensure customers can easily reach out for help.

In line with its commitment to innovation, Getnet has implemented **AI-powered chatbots** to enhance customer interactions. These advanced chatbots are capable of understanding and responding to complex queries in real time, providing personalised support that significantly improves customer satisfaction. The AI continuously learns and adapts to user interaction patterns, ensuring an ever-improving service experience.

Moreover, these intelligent systems play a crucial role in fraud prevention. By monitoring interactions in real time, they can identify and flag potential fraud schemes, adding an extra layer of security to Getnet's comprehensive fraud prevention strategy.

Getnet's comprehensive approach to fraud prevention combines cutting-edge technology with proven expertise:

- AI-powered real-time fraud assessment on 100% of transactions
- Advanced facial biometrics for secure and swift customer authentication
- Award-winning fraud management capabilities, recognised by industry leaders
- AI-driven chatbots for enhanced customer support and real-time fraud monitoring
- Continuous investment in updating and improving fraud prevention tools

This multi-faceted strategy ensures that Getnet remains at the forefront of fraud prevention, offering merchants and consumers alike a secure, efficient, and trustworthy payment ecosystem.

Conclusion

The fraud landscape is evolving rapidly, presenting new challenges in the digital age. However, financial service providers and merchants are rising to meet these challenges with increasingly sophisticated solutions. As online transactions and digital payments grow, companies are leveraging advanced solutions to stay ahead of potential threats.

We're witnessing a technological renaissance in fraud prevention, with artificial intelligence, machine learning, and biometric authentication leading the charge. Merchants and financial institutions are adopting proactive, multi-faceted approaches to security, often outpacing the strategies of would-be fraudsters.

By prioritising customer trust and leveraging cutting-edge innovations, these forward-thinking businesses are not only safeguarding transactions but also fostering a more secure digital economy. This commitment to security is building customer confidence and driving the continued growth of digital commerce.

A large, white, stylized letter 'C' is centered on a solid blue background. The letter is thick and has a modern, sans-serif appearance.



Copyright © 2024 PagoNxt Merchant Solutions S.L. All rights reserved. Any unauthorized distribution, copying, duplication, reproduction, or sale (in whole or in part) of the contents of this document, whether for personal or commercial use, shall constitute a copyright infringement.

All information contained herein is for informative purposes only. The authors accept no responsibility for its accuracy, up-to-dateness or validity, and therefore disclaim any liability for its inaccuracy, omission, failure to update or delay, or for any loss or damage that may be caused by its use or exposure by third parties. All information is provided "as is", whether correct, accurate or not, without warranty of any kind.

PagoNxt Merchant Solutions S.L. cannot accept any responsibility for the accuracy, up-to-dateness or validity of information from third parties (external sources) added by hyperlink to this document or mention in it.

The comments that can be made to this document are the sole responsibility of the persons who have written them, and they will be solely responsible for any complaint, damage or litigation that they may cause, whether directly or indirectly. PagoNxt Merchant Solutions S.L. does not guarantee the accuracy, correctness, truthfulness of such comments

