WHITE PAPER

How to fight fraud's new industrial revolution

The so-called "fourth industrial revolution" in computing and artificial intelligence (AI) isn't just helping legitimate firms. As fraudsters professionalize, banks and fintechs need to fight back – and a "one size fits all" approach focused on AI alone won't work. Nexi Group explain how to counter recent massive rises in fraud.

Two major trends characterize the modern European economy: the shift from physical to digital commerce, and a rising tide of fraud in these new digital channels.

To give some idea of how rapidly Europe's economies are going digital, current e-commerce penetration in Europe stands at around 65% of all consumers[1] – but much more in leading markets such as the Netherlands, Sweden and Norway, where up to 95% of consumers shop online.

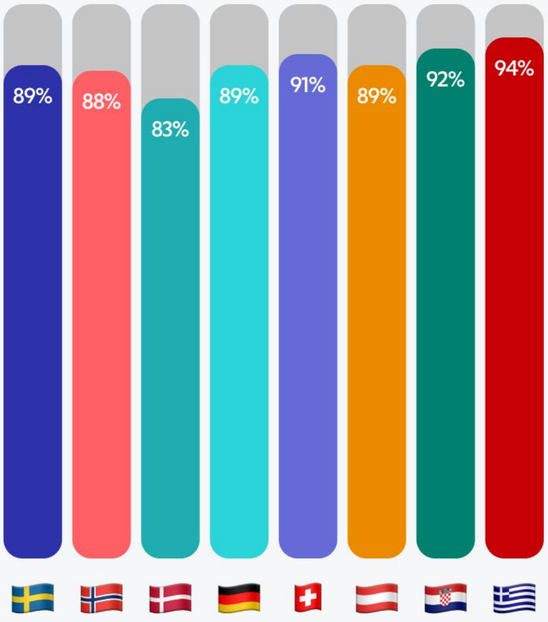
"All countries have adopted online shopping, but at varying speeds"

This year, spending in digital channels including mobile is growing at twice the rate of physical sales, and is projected to exceed four trillion dollars by 2027, just under half of all online sales worldwide[2].

Amid such rapid growth, fraud defenses are being increasingly tested by new fraud types tailored to the digital era. The blanket term, "Card Not Present" (CNP) fraud covers not just standard fraud using fake or stolen cards online, but also new and more challenging types such as Account Takeover (ATO), synthetic ID fraud and Authorized Push Payment (APP) fraud, which is becoming a significant problem in the US, India and other markets as instant payments linked to Open Banking proliferate.

> "Fraud linked to Authorized Push Payments is rising fast in markets like the US and India, where instant payments are gaining ground."

Percentage of internet users who have stated they have shopped online on a monthly basis



Credit: Ecommerce Report 2023 – Europe (nets.eu)

[1] Payments Cards & Mobile, April 2024: "The 2023-2024 Digital and Card Payment Yearbooks" http://www.paymentyearbooks.com
[2] Worldpay, 23 March 2024: "The Global Payments Report 2024": https://worldpay.globalpaymentsreport.com/en

> “Fake identities are now so convincing that they can target undifferentiated fraud defenses effectively, weakening trust and forcing issuers to seek different trust signals.”

Europe’s economies are going digital at different speeds – and the fraud they experience is also different both in type and scope. While fraud related to identity such as synthetic ID and Account Takeover (ATO) has long been a problem in Romania and other markets, Germany saw a shocking 522% rise in Card Not Present (CNP) fraud last year[3] as fraudsters sought to take advantage of perceived weaknesses in some bank defences.

Such figures offer a glimpse of how fraud type can vary from market to market, but a pan-European perspective shows yet more diversity – chiefly linked to digitalization of all kinds, and to the rising demand for instant transaction and settlement. In its **2023 Payment Threats and Fraud Trends Report**,[4] The European Payments Council (EPC) identified five kinds of threat which it said were prevalent across all European markets to a greater or lesser extent, all linked to advanced technologies. These include social engineering fraud – such as ATO and synthetic ID; malware attacks on PCs and ATMs; “denial of service” attacks such as ransomware; “botnet” fraud, in which a user’s device access information is compromised by fraudsters and linked to other devices to commit fraud; and monetization fraud, in which stolen payment information is marketed for sale and exploitation over the DarkNet. The EPC added that the rapid rise of instant payments over the next decade – which are predicted to account for one in three transactions by 2030 – has hightened risk for actors across the payments value chain.

Five kinds of threat faced by banks in the digital era

- Social Engineering Fraud
- Malware Attacks
- Denial of Service Attacks
- Monetization Fraud
- Botnet Fraud

[3] See FICO: European Fraud Monitor for Germany at: https://www.fico.com/europeanfraud/germany
[4] The European Payments Council, 7 November 2023: “Payment Threats and Fraud Trends 2023”: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-12/EPC181-23%20v1.0%202023%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

Such massive rises in new fraud types are caused mainly by an industrialized – and highly tech-driven – approach on the part of fraudsters. Professional teams working from offices purchase vast arrays of stolen data from the dark web and use it to create fake identities and account credentials with fraud now powered by Artificial Intelligence as much as banking is.

These fake identities, which often include legitimate accounts at licensed, legitimate banks, are now so well produced that they can target fraud defenses which are not tuned to differentiate between manipulated ID and genuine identities. This in turn weakens trust in a bank's fraud strategy, requiring issuers to redefine their analytical strategies around different trust signals.

> "The rise of deepfaking and AI-enabled fraud mean that issuers have had to redefine their analytical strategies around different trust signals."

European in scale – but local by nature

The changing dynamics of fraud in various European markets shows why different defense strategies are required. Last year, some markets demonstrated sharp rises in overall levels of fraud, from the Netherlands with an 18% increase[5], through to more modest rises in Poland (4%), Austria (3%), Germany (2%) and Norway (1%). At the same time, fraud types also vary from market to market, with counterfeiting more prevalant in Poland, compared to ID fraud in Austria and CNP fraud in Germany or the Netherlands. Even if there are communalities in the **modus operandi** of criminals and similarities between attack vectors, every market's experience is different. That's because fraudsters employ different attack vectors depending on the quality and extent of bank defences in any given market. They also change attack vectors as banks improve their defences in certain areas, moving (for instance) from phishing to ID scams or other approaches.

Given that today's fraud is European in scale, yet local by nature, we need to define, design and implement solutions that fit the challenges faced by each individual market, rather than trying to find a "one size fits all" approach. A new approach is needed – one in which traditionally silo-based data may be viewed holistically.

Card transactions, user activity at a bank account level and NetBank activity are all examples of data points and customer interactions that must be seen as part of a coherent whole. In what follows, we offer a few examples of different fraud dynamics in European markets – and how to tailor defenses to combat fraud more effectively.

The perceived weak defenses of some DACH banks following news of data breaches could – for instance – be countered by using Risk-Based Analytics engines such as Nexi Fraud Solution alongside 3DS. Fraud Expert Scoring uses technology from Nexi's Fraud Expert Checklist and takes it a step further by allowing banks to create extensive rule combinations uniquely adapted to fulfil business needs.

Nexi Fraud Expert Scoring uses a scoring system to assess the risk associated with a transaction. Based on this score, banks can automatically decide to block or accept a transaction, or add another round of detailed review for the same transaction via automated procedures that determine whether to block or accept.

[5] See FICO, European Fraud Monitor – overview at: https://www.fico.com/europeanfraud

Rising regulation drives fraudster innovation

Part of the reason for the wide range of fraud types targeting card transactions is growing regulation. As stricter regulation leads to more extensive authentication (think PSD2's requirement for Strong Customer Authentication as one example), fraudsters have had to change their modus operandi in order to continue successful criminal enterprises.

For example, fraudsters targeting UK consumers via Authorized Push Payment (APP) fraud have sought to exploit the high penetration of social media in Britain and that it's country's relatively developed Faster Payments infrastructure to move money faster. Meanwhile, the UK's regulatory regime means that customers are less concerned about their losses as liability shifts to banks enable customers to recover funds lost to fraud.

While the UK faces significant APP fraud risk, Nordic markets are seeing a huge increase in social engineering fraud attacks. Criminals now employ generative AI technologies to craft misleading content.

These attacks target in particular the very old and younger consumers. The elderly will typically respond because they have trust in perceived authority and are not always tech savvy, while the young are online constantly and may approve invitations and access links uncritically. Crypto platforms, travel agencies and money transfers are the verticals most affected by such fraud attacks. According to Marketing Tech News[6], 80% of all phone-related fraud attempts hit European consumers, with robocalls, SMS fraud and smishing rising for 61% of mobile carriers in 2023.

Social engineering comes in many shapes and exploits human emotions such as fear, curiosity, sympathy, or pride to deceive victims into falling for scams. Often the victims are contacted through smishing, phishing and vishing: most recently, however, fake advertising on social media platform has become a growing problem. The providers of such platforms have a huge responsibility to ensure that fake content and content supporting criminal activity will be removed from their platforms.

"80% of all global mobile fraud attacks target the EU, with robocalls, fake SMS messages and smishing rising fast."

[6] See https://www.marketingtechnews.net/news/2024/apr/15/80-of-global-smishing-attacks-targeted-eu-citizens/

The solution: constant monitoring and local strategies

At Nexi, we work with clients to continuously monitor fraud trends in the individual markets in which they operate. The strategies we develop in partnership respond to the fraud dynamics of each market with a set of robust, co-ordinated solutions: we then track the performance of these solutions, altering approaches for optimum performance as the risk environment evolves.

An important facet of any strategy is consumer education. Part of our commitment to our client base is working with them to build user education programs about how to spot social engineering tactics and misinformation promulgated by fraudsters – a situation which is getting worse given the rise of deepfaking. In developing education programs with our clients, the goal is to encourage those critical thinking skills that help users to discriminate between reliable information and deceptive content.

In our experience, the best baseline approach is an end-to-end, data-driven flow of protection throughout the transaction life cycle. Such an approach combines authentication and assessment at the point of sale through 3D Secure plus Risk-Based Analytics, followed by further assessment as the transaction proceeds to full authorization – by using tools such as the Nexi fraud authorization risk engine, machine learning based on outcomes (such as the rate of fraud prevention) and above all the expert counsel of payments analysts with experience of how fraud operates in different European markets.

We then assess the effectiveness of our approach and work with our clients to continuously monitor outcomes and fine-tune for better performance.

We always recommend that client banks consider the optimal authentication approach in any given market, whether that's passwords, biometric factors, digital ID or a combination of these factors. We also advise on other approaches that can compliment 3D Secure plus RBA, such as device ID techniques which confirm the association of a user with a particular device, or the aggregation of behaviors from previous authentications to help identify anomalies suggestive of fraud.

> “By adopting a market-specific, data-based approach, we have dramatically reduced false positives and rates of transaction decline for our clients, driving revenue and profitability growth in the process.”

Finally, it’s important to tune rules to local market conditions. For instance, clients in Germany or the Netherlands might be advised to tune their rule engines to account for rises in CNP fraud, or in markets where ID fraud is a problem, a laser focus on authentication protocols may be appropriate. By adopting such market-specific, data-based approaches, we have dramatically reduced false positives and rates of transaction decline for our clients, driving revenue and profitability growth in the process. In our experience, an end-to-end market-specific approach that combines consumer education, 3DS and RBA with optimized authentication approaches, machine learning techniques, rules tuned to the fraud dynamics of that market, analytics during authorization and evidence-based performance reviews delivers optimal performance.

New payment types such as account-to-account payments and instant are going to make optimal fraud defense more important than ever. Adopting market-specific approaches using modern technologies doesn’t just equip banks for today’s challenges – it also makes them fit for purpose in a future where payments move faster both in-market and across borders, necessitating a hitherto unseen degree of agility and flexibility on the part of banks.

Learn more about how to optimize your fraud defence for local markets to deliver higher completion rates and better growth and profitability.

Visit www.nexigroup.com for more information.

About Nexi

Nexi Group - the European PayTech with scale, capabilities, and geographic reach to drive the transition to a cashless Europe. We are committed to supporting people and businesses of all sizes, transforming the way people pay and businesses accept payments. By simplifying payments and providing the most innovative and reliable solutions we enable businesses and financial institutions to better serve customers, build closer relationships, and to grow together.

For more information please visit **www.nets.eu** or **www.nexigroup.com**