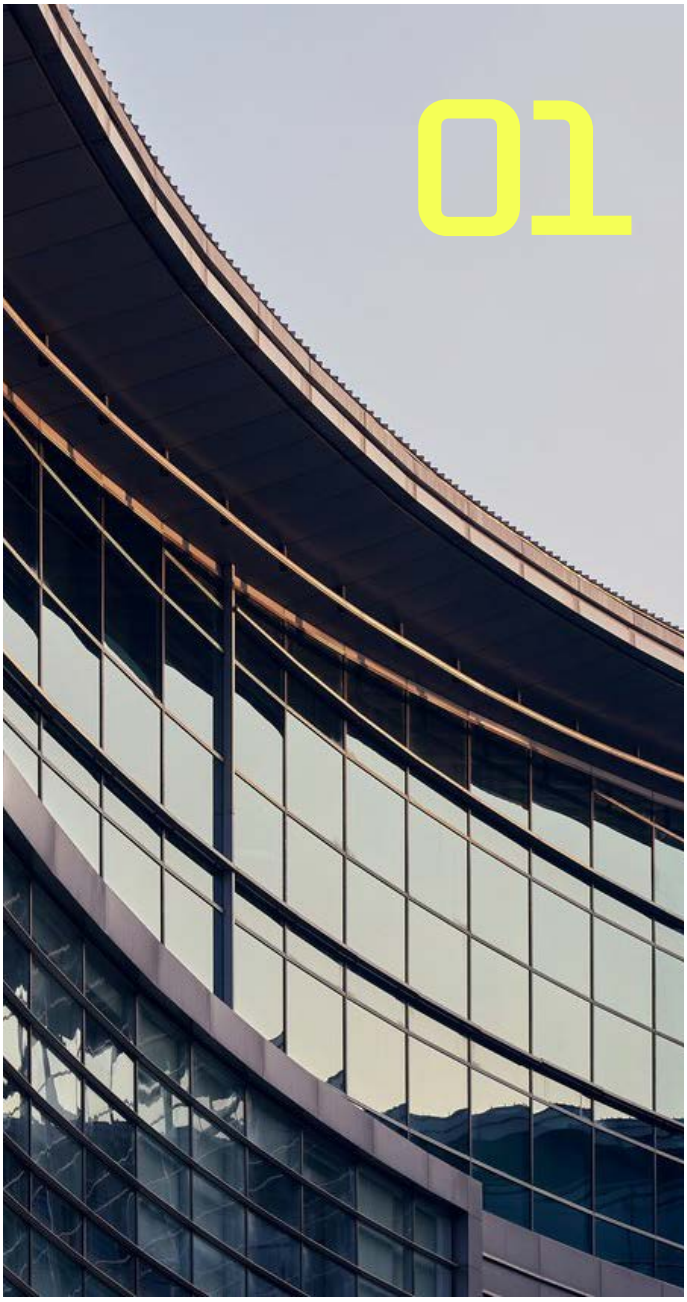
tieto
Banktech

FinCrime Insights: Payment Fraud Report 2026

Visit tieto.com


2026

Table of content



01

Strengthening Defences Against Payment Fraud During Global Unrest

Fostering Resilience Through Partnership

As Head of the Defence Centre, I am proud to present this year's Payment Fraud Report. The developments we observed in 2025 underline a reality we know well: payment fraud is no longer a series of isolated incidents, but a continuously evolving, borderless threat shaped by global instability and rapid technological change. Criminal networks are adapting faster than ever, exploiting uncertainty, regulatory asymmetry, and the growing digital pressure on consumers and institutions alike.

Despite this challenging environment, our collective resilience has strengthened. Together with more than 75 banks and financial institutions across Europe, we monitored 4.9 billion transactions and prevented EUR 1.132 billion in attempted fraud. This achievement reflects more than operational success – it represents thousands of individuals who were protected from financial harm. Reaching zero financial loss in 76% of all card fraud cases speak volumes about our shared commitment and the power of long-term partnership with our customers in the continuous fight against financial crime.

Our response is rooted in collaboration, innovation, and an unwavering determination to stay ahead of fraudsters. In 2026, we are introducing new protective layers such as Money Mule Monitoring (MMM) and Manipulation Risk Monitoring (MRM). These capabilities reinforce our strategic focus on early detection and behavioural understanding - strengthening the defence lines that protect both institutions and the people who rely on them.

As we move into 2026, our mission remains unchanged: safeguarding trust in digital payments. But how we fulfil that mission continues to evolve – through stronger partnerships, responsible use of data and technology, and a shared recognition that preventing financial crime is a societal responsibility. I want to extend my heartfelt thanks to our customers, partners, and the dedicated specialists across Financial Crime Prevention who work tirelessly, day and night, to protect millions of people.

Together, we are stronger. And together, we will continue building a safer digital future.

Mette-Lise Engø
Head of Defence Centre
Tieto Banktech

About Us

This report is published by Tieto Banktech's Defence Centre, a fully managed fraud prevention service and trusted partner to banks across Scandinavia and Europe. Our 85+ specialists operate 24/7, 365 days a year to detect and prevent digital payment fraud through real-time, multi-channel monitoring. Operating since 1997, the Defence Centre is built on nearly 30 years of transaction monitoring experience.

The Defence Centre is a core component of Tieto Banktech's Financial Crime Prevention (FCP) offering, which protects customers and financial institutions across the entire journey - from onboarding to transaction monitoring and fraud management. Positioned within FCP, the Defence Centre delivers specialized managed services such as monitoring, case handling and investigations on behalf of our customers.

Fraud Prevention is a specialised product domain within FCP that works closely with the Defence Centre to boost fraud-fighting abilities. This partnership allows for real-time operational insights to shape product development, ensuring that new innovations reinforce frontline defences. By combining product knowledge with hands-on experience, we continually improve our solutions and deliver effective results for our customers, helping create a safer and more resilient society.

Today, our combined capabilities in FCP support 130+ European banks and financial institutions, helping them reduce risk, respond faster to threats and protect end customers with confidence.

Tieto Banktech is a financial technology provider with 3,900+ experts, developing secure, compliant, future-ready banking software and services across cards and transactions, lending and leasing, financial fraud prevention, wealth management, and Banking as a Platform – serving the Nordics and beyond.

Powered by advanced AI, our specialized solutions are continuously updated to ensure maximum impact. We create financial technology that powers tomorrow.

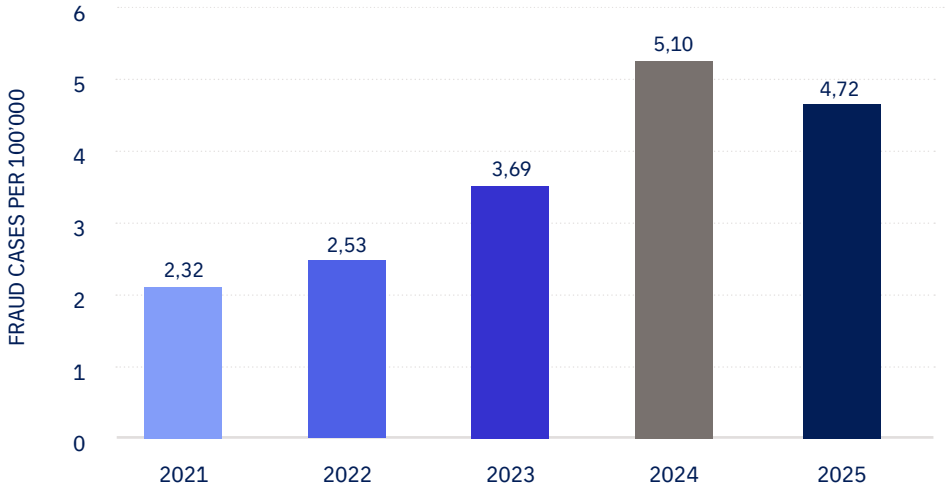
Watch this video to learn more about how the Defence Centre operates:

Key Insights From 2025

Our advanced fraud prevention solutions delivered around 90% detection rate in 2025, identifying nearly 170,000 fraudulent cases across card authorisations, account payments, 3D Secure authentications, and digital wallet enrolments. These cases spanned customers operating in Norway, Sweden, Denmark, Finland, Germany, Spain, the United Kingdom, and Ireland. By monitoring 4.9 billion transactions across our portfolio, we achieved zero financial loss in 76% of all card fraud attempts, helping protect banks, businesses, and citizens throughout Europe.

In 2025, payment activity reached new highs across the Nordics and Europe. Even as this growth introduced greater complexity, the rate of fraudulent activity decreased relative to overall volumes. Fraud cases per 100,000 card transactions fell from 5.10 to 4.72, while the equivalent figure for account transactions declined from 0.13 to 0.10. These developments indicate that fraud attempts occurred at a lower rate relative to overall payment activity, reflecting a shift in how often – and in what ways – fraudsters sought to exploit customers.

CARD PAYMENT FRAUD OVER THE PAST FIVE YEARS



Detection capabilities strengthened further across key payment channels. Card authorisation detection improved from 88% in 2024 to 92% in 2025, while account detection rose from 84% to 90%. The improvements across core channels highlight the continued impact of our rule based controls and real time monitoring. Enhancements to our Card Transaction Monitoring (CTM) solution also increased the share of attempts ending in no financial loss for end customers (76%).

The amount of fraud we were able to prevent increased significantly. Overall, we blocked €1.132 billion in fraudulent activities during 2025 – more than three times the €355 million stopped the year before. A major factor in this success was our Blocking of Rogue Merchants (BoRM) solution, which accounted for nearly €290 million in 2025 compared to €173 million in 2024. Additionally, our 3D Secure Monitoring solution saved over €225 million, highlighting the effectiveness of using multiple layers of protection against fraud.

At the same time, fraud patterns continued to evolve. While phishing fraud cases decreased (8%) during 2025, social manipulation scam cases increased significantly (+33%). These cases often involved carefully crafted interactions in which fraudsters used authority, urgency, or trust building tactics to manipulate victims into transferring funds or revealing sensitive information. Fraud pressure also remained high within several merchant categories, including digital goods, telemarketing, easily tradeable goods, and money transfers.

Directly supporting end customers remained central to our work. In 2025, we sent over 216,000 SMS alerts and handled over 340,000 phone calls, enabling prompt intervention for at risk end customers. Our Response team

03

FinCrime Insights:
Payment Fraud Report 2026

1 160M€
Total value of prevented fraud

170.000
fraud cases handled

90%
success rate in detecting
fraud on cards and accounts

340.000
phone calls handled

played a vital role in preventing losses and assisting victims through challenging situations.

Taken together, the results from 2025 point to a strengthened security posture. Detection rates improved, fraud intensity declined, and the financial impact of fraud was significantly reduced – even as fraudsters adapted their tactics. These developments highlight the importance of continued investment in both advanced technology and human centred fraud prevention. As fraudsters increasingly target digital commerce and rely on social engineering techniques, raising end customer awareness and maintaining strong, collaborative defences will remain essential.

In the sections that follow, we take a closer look at the fraud patterns that shaped 2025 – exploring the fraud types behind these trends, the evolving tactics used by fraudsters, and the measures financial institutions can adopt to strengthen their defences.

1.1 Social Engineering: Human-Centric Fraud Threats

Social engineering represents an escalating humancentric fraud threat, exploiting behavioural and emotional vulnerabilities to compromise sensitive data and financial assets across social media, telephone calls, messaging platforms, and direct interaction. Over the past few years, we have observed a clear shift from technical intrusion towards psychological exploitation, as fraudsters increasingly adopt more manipulative methods. Phishing attacks and social manipulation scams have become significantly more sophisticated, now reinforced by AI-driven tools such as deepfakes. In 2025, phishing incidents declined by approximately 8%, while social manipulation scams rose by nearly 33%, underscoring the accelerating move towards highly personalised and emotionally targeted fraud techniques.

1.1.1 Phishing Fraud

In 2025, phishing activity demonstrated clear patterns regarding the categories of merchants targeted and the tactics utilised by fraudsters. The majority of detected phishing attempts targeted money transfer and cryptocurrency services, where our 3D Secure Monitoring (3DSM) solution continues to provide strong preventive performance. Over the course of the year, transactions totalling over €205 million were declined through this service, underscoring the scale of protection achieved.

Seasonal Patterns: Digital Goods & Travel

During the summer months, most declines were linked to digital goods merchants, reflecting seasonal peaks in low value, high volume phishing campaigns. Travel also remained a notable focus area: around 12% of phishing related fraud attempts involved airline transactions. Toward the end of the year, activity increased significantly against carriers operating to and from the Middle East, with most attempts originating from Norwegian IP addresses.

Increasingly Coordinated Multi-Channel Attacks

Fraudsters increasingly adopt coordinated, multi channel approaches, often initiating schemes through smishing before guiding victims across additional channels. Split payment strategies are frequently used to bypass transaction level controls, and there is a clear shift towards transferring funds to international banks rather than domestic cryptocurrency platforms. Fraudulent narratives are typically framed as routine financial activity – such as bookings for travel or payments for home improvement – to reduce friction and evade risk-based controls.

Enhanced Detection Performance

Improvements to the 3DSM rule set strengthened detection capability throughout the year. Updated logic enhanced pattern recognition of emerging attack types, allowing new fraud behaviours to be captured earlier. As a result, most BIN scanning activity was intercepted by newly deployed rules.

A BIN scan is a form of brute force attack where fraudsters systematically test large volumes of card number combinations that share the same Bank Identification Number (BIN). The specific goal is to uncover valid authentication details. By rapidly cycling through possible card numbers and authentication parameters, attackers attempt to determine which combinations can successfully pass an authentication step — or, if an authentication request is triggered, to simply confirm that a card number is valid.

Geographical Rotation of Fraud Attempts

Geographic indicators also shifted over the course of 2025: while Norwegian IP addresses accounted for most attempts, volumes decreased over the summer. In the same period, attempts originating from Swedish IP addresses increased. After July, activity from Moroccan IP addresses fell sharply, while fraud attempts linked to Tunisia and Italy rose correspondingly. These patterns highlight how fraudsters rapidly rotate infrastructure in response to defensive measures, underscoring the need for continuous rule optimisation and agile operational monitoring.

1.1.2 Social Manipulation Scams

In 2025, the predominant forms of social manipulation scams included love scams, various friend-in-need schemes (such as “hi mom/hi dad” scams), and investment related scams (including recovery scams). The data reveals a consistent pattern in how social engineering impacts different demographic groups, with age and gender emerging as key determinants of vulnerability. The most prominent finding is the significant overrepresentation of older adults – particularly men over the age of 60. Individuals aged 60–79 account for more than 30% of all recorded cases, and men within this segment are markedly more exposed than women.

Elevated Vulnerability Among Elder Adults

Older adults are especially vulnerable to major financial losses due to modern fraud and social engineering tactics. Phishing attacks frequently target this age group with single, high value transactions – often linked to travel, refunds or money transfers. Social manipulation scams tend instead to produce a series of smaller, repeated losses that gradually deplete savings and may remain unnoticed until significant harm has occurred.

A central driver behind this heightened exposure is a lower level of digital familiarity among individuals in their late seventies and eighties. This makes it easier for fraudsters to exploit fraudulent messages, misleading prompts, suspicious links or malicious attachments. Trust in perceived authority figures – such as fraudsters impersonating bank employees or police officers – further compounds the risk, as does increased social isolation, which can make older adults more receptive to contact from seemingly friendly or helpful actors.

A similar pattern is visible within the 80–99 age segment, which represents the second largest risk cluster in the dataset. Although the total number of cases is lower, the gender imbalance persists, with men disproportionately affected. This reinforces that elevated risk continues into the oldest age groups, driven by many of the same behavioural and situational factors observed among individuals aged 60–79.

Age related changes in memory, information processing and decision making add an additional layer of vulnerability. Many contemporary fraud schemes are engineered to resemble routine account activity or everyday service interactions, lowering the victim's natural defences. Emerging technologies, including voice and video based deepfakes, are now used to replicate identities with high fidelity, increasing the credibility of fraudulent requests. As a result, older adults not only face a higher likelihood of victimisation but also greater challenges in identifying anomalies and recovering from financial loss. Tailored prevention initiatives, compassionate support structures and clear, accessible communication are therefore essential to strengthening protection and resilience in this group.

Rising Sextortion Risks Among Youth

At the lower end of the age spectrum, children and adolescents – particularly young boys – face an escalating risk of sextortion. Fraudsters exploit their limited online experience by posing as peers on social platforms and persuading them into sharing intimate images or personal information. These materials are later weaponised to coerce, pressure, and intimidate victims, often resulting in significant emotional distress and, in some cases, financial loss. The youngest sextortion victim recorded in 2025 was just 14 years old. The combination of widespread digital communication and the anonymity of online interactions make it difficult for young people to recognise and avoid such schemes, underscoring the need for stronger digital awareness, parental involvement, and effective protective technologies.

Age- and Gender-Specific Extortion Patterns

Extortion cases reported in 2025 display a clear age and gender specific pattern. Among individuals aged 14–25, no women were targeted; instead, cases in this segment are overwhelmingly linked to sextortion, primarily affecting young men. A similar trend is seen in the 25–49 age group, where no female victims were identified. This suggests that perpetrators tend to employ sexualised threats almost exclusively against younger male targets, while women in these age ranges are either approached through other fraud types or exhibit lower susceptibility to this specific form of coercion.

The picture shifts notably in the 51–84 age group. Here, women do experience extortion, but the modus operandi differs markedly from sextortion. Instead of digital manipulation, fraudsters rely on direct threats involving family members – often claiming that children or grandchildren will be harmed unless payment is made. These schemes exploit emotional vulnerability rather than online behaviours, indicating a strategic adjustment by fraudsters who tailor their approach to maximise psychological pressure.

340.000
calls

216.000
SMS alerts

Frontline support for manipulated end-customers
We offer compassionate and straightforward guidance to stop funds from being transferred when people are targeted by social manipulation. In 2025, we managed over 340.000 calls and sent upwards of 216.000 SMS alerts to ensure quick intervention. Our strategy blends personalised communication with objective advice to help vulnerable customers spot risks and avoid financial loss. As social manipulation becomes more advanced, we apply specialised methods and adapt our tactics for complicated cases, especially when victims are under pressure or when fraudsters respond on their behalf. Quickly building trust is essential, so we constantly refine how we interact with customers during stressful situations. By working every day with at risk individuals across multiple countries, we learn valuable lessons about fraud methods, strengthen our procedures, and uphold our leadership in fighting financial crime.

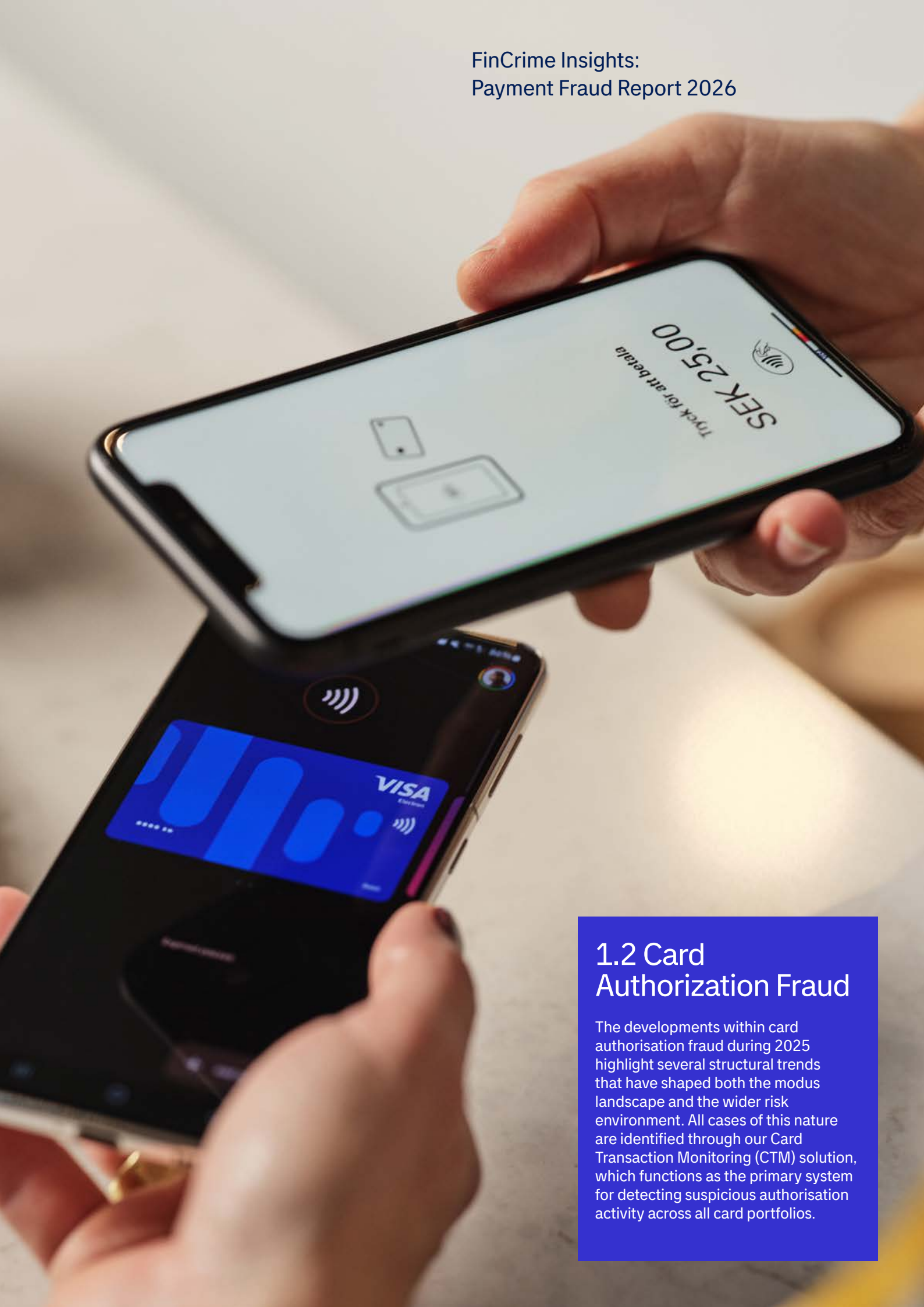
Integrating Manipulation Risk Monitoring into the Fraud Prevention Framework

To better address the risks of social manipulation scams, we have spent the past months piloting our new Manipulation Risk Monitoring (MRM) solution. The pilot has allowed us to test and refine the solution in a controlled environment, ensuring that the analytics, alerting mechanisms, and intervention workflows perform reliably in real-world scenarios.

Building on the promising results from this pilot phase, we aim to introduce MRM as a core part of our fraud prevention solution in early 2026. MRM will continuously analyse end-customer transaction behaviour to detect subtle indicators of social manipulation, using advanced analytics and real-time monitoring. By combining historical patterns with current behaviour, the system will identify unusual changes – such as shifts in transaction timing, frequency, or destinations – that may signal manipulation or fraudulent influence.

When potential risks are detected, our teams will be able to respond quickly, offering tailored support to those affected. This includes providing clear, personalised guidance and, when necessary, immediate intervention to prevent further financial loss.

By integrating MRM into our broader strategy, we strengthen our ability to act proactively and protect customers before financial harm occurs. With earlier detection and more targeted responses, we aim to deliver even stronger protection against increasingly sophisticated manipulation-based scams.



1.2 Card Authorization Fraud

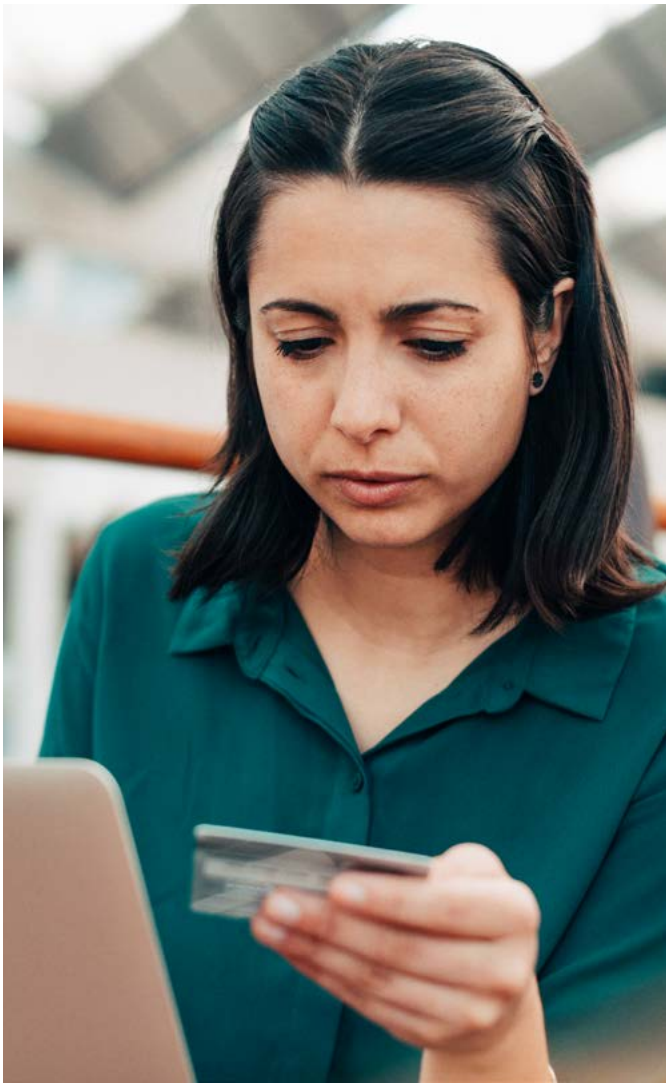
The developments within card authorisation fraud during 2025 highlight several structural trends that have shaped both the modus landscape and the wider risk environment. All cases of this nature are identified through our Card Transaction Monitoring (CTM) solution, which functions as the primary system for detecting suspicious authorisation activity across all card portfolios.

Relay Attacks and Modification of Payment

Relay attacks and modification of payment emerged as the most prominent new fraud patterns in 2025, and although case volumes remain low, several indicators suggest that they may represent the early phase of more established schemes.

This type of fraud involves a legitimate payment being altered after initiation – whether through manipulation of the amount, adjustment of transaction parameters, or redirection of the transaction flow – resulting in a charge that diverges from the cardholder's original intent.

Because such changes occur following an otherwise standard authorisation request, these cases often fall outside traditional detection mechanisms and are therefore identified primarily through behavioural patterns surfaced in CTM. Although overall volumes remain limited, these cases occur most frequently in transactions routed to countries such as Uzbekistan, the United Arab Emirates, and Bulgaria.



Persistent Risk from Fake Online Stores

A significant and recurring element of the 2025 risk landscape was the continued role of fake online stores in compromising card credentials. The majority of compromised websites identified were Asian based actors, often purpose built to closely imitate legitimate retailers. Additionally, analysis for the year shows that over 20% of all cards subjected to fraud were compromised via Asian travel related websites, confirming that exposure within this segment represents a notable and consistent risk factor. As in 2024, card fraud related to travel, with fraudulent transactions directed towards hotels and airlines across multiple countries, continued to be a persistent trend throughout 2025.

The regional concentration of fraudulent merchants, combined with the scale and global reach of major Asian platforms, continues to generate a stable flow of compromised card data later detected through CTM.

Physical Card Skimming Remains a Marginal Modus

In relation to physical card skimming, only a very small number of cases were recorded in 2025. The few cases identified were primarily linked to Brazil, consistent with historical geographical patterns. Overall, case volumes were so low that physical card copying remained a marginal fraud modus compared with digital attack vectors.

Significant Reduction in Token-Related Fraud

A marked reduction in token related fraud was also observed in 2025. These cases, which involve unauthorised use or compromise of tokenised payment credentials, are primarily detected through CTM, but the significant decline is largely attributable to the introduction of the Token Enrolment Monitoring (TEM) solution. TEM identifies suspicious token enrolments at a much earlier point in the process, preventing attempts from progressing into authorisation fraud detected by CTM.

BIN Attacks Remain an Active Vector

It is also notable that just under 10% of all card authorisation cases in 2025 were related to BIN attacks, indicating that this attack vector remains active despite reductions across other areas. The dataset for 2025 further shows a high proportion of zero loss cases (76%), reflecting a combination of test activity and increasingly effective real time controls. While this has significantly reduced financial losses, it also demonstrates that underlying fraud activity remained present – albeit intercepted earlier and more effectively before any financial impact occurred.

Across all modus categories observed in 2025, patterns of repeated and densely clustered transaction attempts continued to be the most consistent behavioural indicator of authorisation fraud. These patterns were regularly surfaced and acted upon through CTM, reflecting increasing automation and structured attack behaviour. This reinforces the need for ongoing refinement of real time detection models, rule sets, and adaptive monitoring capabilities.

1.3 Digital Wallet Fraud

Fraudulent wallet token enrolments peaked during the winter and summer, with Google Pay being the main target. Early detection and preventive actions played a crucial role in reducing the financial loss from these incidents. Throughout the year, several notable patterns were observed, providing insight into fraudster tactics. For example, many cases involved devices set to Chinese, pointing to concentrated activity among fraudsters in that language group. Additionally, suspicious transaction IP addresses often traced back to parts of Asia or the United States, indicating possible international coordination or use of global digital networks. Fraudsters also commonly provided fake local addresses to get past verification checks and make their enrolments appear legitimate. These trends show how token enrolment fraud continues to change and stress the need for ongoing monitoring, adaptable security measures, and international cooperation to protect digital payment systems.

Early Interception Through Token Enrolment Monitoring

To address this new wave of fraud, we introduced Token Enrolment Monitoring (TEM) in 2024 – a solution that stops attempts the moment a card is added to a digital wallet. TEM analyses each enrolment attempt in real time, detecting unusual signs such as suspicious IP addresses, language settings, geographical discrepancies, or abnormal device usage. If anything deviates from the end-customer's normal pattern, the enrolment is halted before the fraudster gains access to an active payment method. For new customers, TEM has reduced digital wallet fraud losses by about 70%.

This gives banks an entirely new level of control: fraud attempts are uncovered before any misuse begins, losses are minimised, and end-customers are spared the distressing consequences afterwards. TEM acts as a proactive first line of defence and intercepts the majority of attempts – long before they reach the transaction stage. For banks, this means lower risk, less manual follow up, and a safer end-customer experience. For end-customers, it means that digital wallets can still be used easily and securely, even in the face of increasingly sophisticated threats. With TEM, banks gain a modern and data driven layer of security that protects both their business and customer trust at a time when digital fraud is growing rapidly.

1.4 Account Fraud

Account fraud remained an area characterised by increasing complexity and evolving behavioural patterns throughout 2025. We observed a clear rise in social manipulation as the primary entry point to account related fraud. Cases frequently began with smishing, e-mail phishing, or other forms of digital deception used to establish initial contact. From there, fraudsters gradually built trust and influenced victims' decision making over time. This type of manipulation grew increasingly structured and persistent, with many victims receiving repeated guidance designed to shape their actions. A notable behavioural shift during 2025 was the use of multiple smaller payments, reflecting how fraud networks continuously adjust the way they initiate and disguise activity. These developments were consistently identified through our Account Fraud Monitoring (AFM) service, which provides early behavioural detection of account based fraud patterns.

Evolving Narratives in Investment Related Scams

Investment related scams continued to represent a substantial share of account fraud in 2025, although the narratives used by fraudsters developed considerably. These scams were increasingly intertwined with romance based manipulation, where emotional rapport was used to build influence and compliance. Fraudsters often provided victims with detailed scripts and explanations intended to guide how they communicated about the payments. A clear pattern throughout the year was that victims seldom described their transfers as investments. Instead, they referred to travel, property related expenses, or seeking improved savings conditions abroad. This shift demonstrated how fraud networks adapted their narratives in response to growing public awareness of investment fraud.

Increasingly Global Footprint of Fraud Networks

We also observed a shift in the profile of payment recipients during 2025. While domestic cryptocurrency platforms had appeared more frequently in earlier periods, the pattern in 2025 showed a broader dispersion of recipients, including a rising share located outside Norway. This reflected the increasingly international footprint of fraud networks, which often distributed funds across several jurisdictions. As a consequence, case handling involved more cross border considerations, aligning with the wider global development of financial crime.

Phishing as an Entry Point for Broader Fraud

In parallel, standard e-mail phishing increased in volume throughout 2025. Although phishing may appear less advanced than more sophisticated forms of manipulation, it frequently served as the initial phase of a broader fraud sequence. Information gathered at this early stage was later used to support direct engagement and further manipulation. Phishing campaigns became more polished and personalised, employing realistic sender details and improved formatting that indicated a general professionalisation of fraud attempts rather than any specific vulnerability within the financial sector.

Taken together, developments observed in 2025 illustrated that account fraud was increasingly defined by sophisticated manipulation techniques, adaptive and carefully crafted narratives, and an international distribution of fraud activity. These trends reinforced the importance of strong analytical capabilities, continued collaboration across the financial sector, and proactive measures to identify manipulation early – supporting the broader industry effort to reduce fraud losses and protect customers within an evolving threat landscape.

1.5 Money Mules

The prevalence of money mules persisted as a notable trend from 2024 through 2025. Analysis of confirmed cases demonstrates a consistent pattern aligned with previous years. Young adults continue to constitute the primary risk group, with individuals aged 20–29 representing more than half of identified cases and those aged 20–25 comprising the largest segment.

Significant Gender Imbalance in Mule Cases

A significant gender disparity is observed, as approximately 80% of known cases involve men; this imbalance is even more pronounced in younger cohorts, where male representation ranges from 84 to 91%. Data indicates that young men, particularly those transitioning from education to early career stages, remain disproportionately targeted by organised networks promoting effortless income opportunities. Notably, the youngest individual linked to a mule case in 2025 was 16 years old.

Mule activity declines progressively after age 30, and gender distribution becomes more balanced among older groups. Collectively, these findings suggest that criminal networks intentionally direct recruitment efforts toward younger men, reinforcing the importance of targeted prevention strategies across banking institutions, digital platforms, and monitoring services to effectively disrupt these patterns.

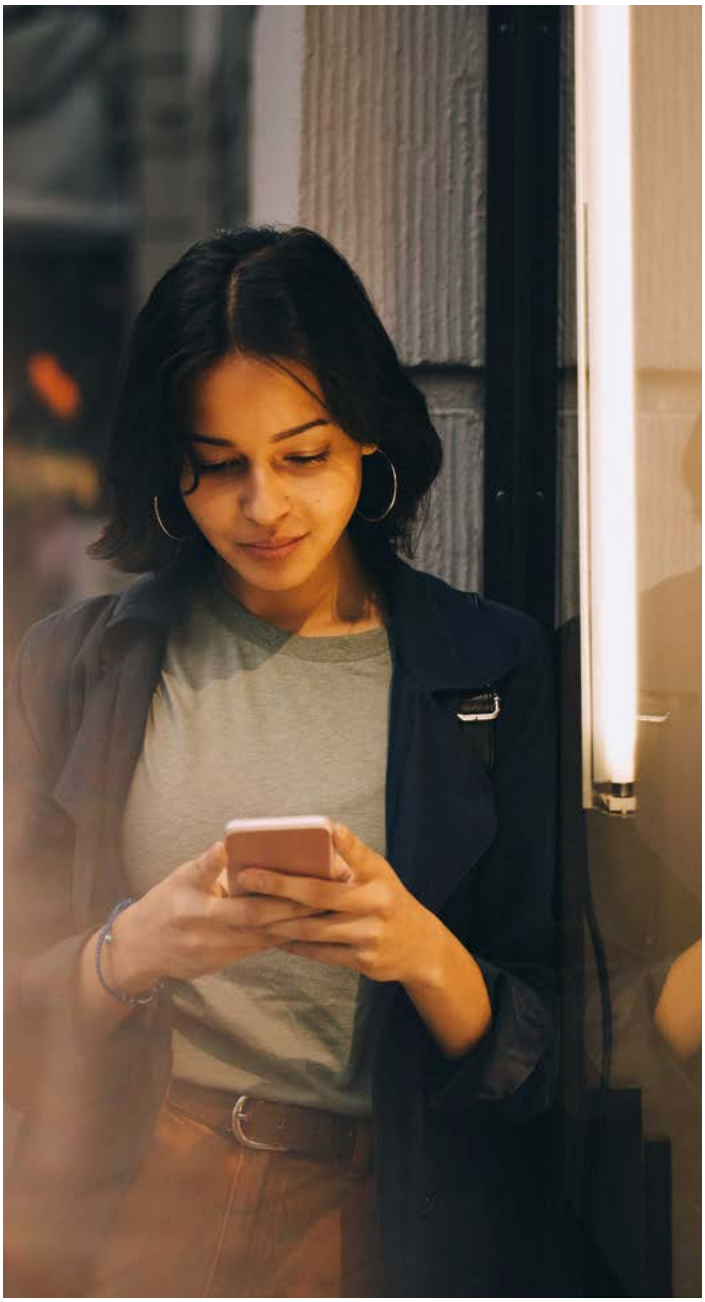
Individuals Exploited Without Awareness

The number of cases involving involuntary money mules has increased significantly, doubling from 2024 to 2025. An involuntary mule is an individual who, often without realising it, is used by fraudsters to transfer funds on their behalf typically by being lured or manipulated into carrying out transactions. This means that more people are being exploited in financial crime without being aware of their involvement, presenting challenges for both prevention and follow up. Over 80% of all cases related to mules involved transactions via well known money transfer services, underscoring the urgent need for targeted measures to address both recruitment and the use of such services in fraud.

Introducing Money Mule Monitoring

To address the challenge of widespread use of money mules, we are launching the Money Mule Monitoring (MMM) service in 2026. This solution will monitor transactions in real time to detect suspicious patterns linked to the recruitment and use of money mules. Leveraging advanced data analysis, the system uses multiple metrics to identify individuals in risk groups.

The MMM solution is designed to be flexible: it can either block transactions directly or simply flag them, depending on the bank's policy and preferences. For each flagged case, a notification is sent to the bank, ensuring they are promptly informed and able to act as they see fit. With Money Mule Monitoring, banks will receive a powerful tool for preventing funds from being channelled through criminal networks.



1.6 Fake Online Shops

Fake online shops remained a significant and consistently high volume fraud category in 2025, with 2.87 million blocked transactions and a declined amount of nearly €226 million. This marks a clear increase from 2024, when 1.77 million transactions were blocked, corresponding to €124 million. The year on year rise in both attempted transactions and declined value demonstrates how fraudulent e commerce environments continue to expand and mature within the online payments landscape.

A key factor driving this development is the continued proliferation of highly convincing fraudulent retail sites, often designed to closely mirror legitimate online shops. These sites typically promote sought after goods at appealing price points and employ professional imagery, coherent branding and persuasive messaging. This reduces consumer scepticism and contributes to sustained transaction volumes throughout the year.

The continued rise in this category also reflects the increasing operational maturity and agility of fake online shop networks. Fraudsters reuse templates, automate domain creation and rotate merchant identities frequently, allowing activity to continue with minimal interruption even when individual sites are blocked. The sharp increase between 2024 and 2025 suggests that these networks can replicate and re-establish their operations quickly and at low cost.

Blocking of Rogue Merchants as a Key Defence Layer

Central to mitigating this threat is our Blocking of Rogue Merchants (BoRM) service, which played a decisive role in intercepting and preventing these transactions. BoRM's ability to identify and block fraudulent merchant activity in real time was instrumental in halting millions of attempts linked to fake online shops during the year. The substantial increase in blocked transactions from 2024 to 2025 highlights both the growing scale of the problem and the critical importance of maintaining robust merchant level controls within the broader fraud prevention framework.

1.7 Consumer Survey 2025: Shifting Trust in Data and AI

Our 2025 consumer survey shows that 12% of Norwegians and 16% of Swedes have been exposed to financial fraud or identity theft in the past 12 months. While Sweden reports its highest level to date, Norway has seen a decline from last year's peak. This indicates that awareness campaigns and strengthened countermeasures may be contributing to improved outcomes in the Norwegian market.

Declining Willingness to Share Personal Data

The survey, conducted by YouGov in June 2025, also highlights clear differences in public attitudes toward fraud prevention measures. Willingness to share personal financial information has decreased compared to previous years. In both Norway and Sweden, around two thirds of respondents are still open to sharing data, but this represents a notable drop from the mid 70% range seen previously. A similar trend is evident when it comes to AI: 43% of Norwegians and 46% of Swedes say they would allow AI to analyse their financial data for fraud prevention, down from over 50% last year.

Rising Concern About AI-Enabled Fraud

At the same time, concern about AI enabled fraud is increasing. Nearly half of respondents – 43% in Norway and 48% in Sweden – report being quite or very worried that rapid advances in AI will raise the risk of fraud. This shows a growing public awareness of how criminals are adopting AI to create more convincing scams and social engineering attacks.

Despite these concerns, consumers remain supportive of practical measures that strengthen protection. More than 70% of respondents in both countries say they are willing to accept delays in money transfers if slower processing increases the likelihood of detecting fraud attempts. This suggests that people recognise the need for more robust safeguards, even when it introduces friction into everyday payments.

Overall, the 2025 results point to a public that is increasingly aware of evolving fraud threats but more cautious about the use of personal data and AI. As financial crime grows in sophistication, building trust in advanced fraud prevention tools – together with strong collaboration between banks, authorities, and consumers – remains essential.

Read more about our survey and download the full report for key insights from over 2000 respondents in Sweden and Norway

04

Payment Fraud Forecast: Predicting Fraud Trends for 2026 and 2027

As we look ahead to 2026 and 2027, the patterns we observed in 2025 reveal not just incremental changes, but a deeper shift in how fraud unfolds across the digital payments landscape. Five developments in particular stand out – each reinforcing the others, and together shaping a more adaptive, psychologically driven and globally distributed threat environment.

From Single Attacks to Long-Form Engagement

The first and most defining trend is the transformation of social engineering into a sustained, behavioural manipulation process rather than a quick, transactional attack. What once took the form of a single deceptive message has evolved into multi-stage, trust based engagement, often stretching over several days or weeks. Fraudsters now take time to learn about their target, mirror their communication style, and gradually guide them toward harmful decisions. This shift marks a fundamental change: fraud is no longer merely a technical intrusion, but a deep intrusion into human judgement.

Blurring the Line Between Real and Fabricated

Closely linked to this is the accelerating rise of AI-driven deception, which is rapidly changing what "credible" looks and sounds like. Tools that generate realistic voices, synthetic video and personalised text allow criminals to create fraud scenarios that feel authentic, even to digitally experienced individuals. As these technologies mature, victims are less likely to question what they see or hear. The line between genuine and fabricated interaction becomes increasingly blurred, creating a threat landscape where traditional cues of suspicion lose much of their usefulness.

Continued Evolution of Fake Online Shops

A third trend shaping the next years is the continued evolution of fake online shops as a highly organised and resilient fraud ecosystem. These sites no longer resemble improvised scam pages – they are professionally designed, commercially convincing and deeply integrated into digital marketing channels. Fraudsters replicate and relaunch new shopfronts within hours, adjusting their appearance and messaging with startling agility. As online commerce expands, fraudulent retail environments are becoming a central, persistent pillar of the broader fraud economy.

Increasing Complexity in Cross-Border Fraud Operations

Fourth, we see the growing internationalisation of payment fraud operations, particularly in the movement of funds. Fraud networks are increasingly

dispersing transactions across multiple jurisdictions, using both willing and manipulated intermediaries to break the flow into smaller, less detectable segments. Mule recruitment has become more psychologically driven, relying not only on promises of income, but on social influence, emotional appeal and situational pressure. This shift signals a more distributed, transnational criminal infrastructure – one designed to withstand disruption and complicate intervention.

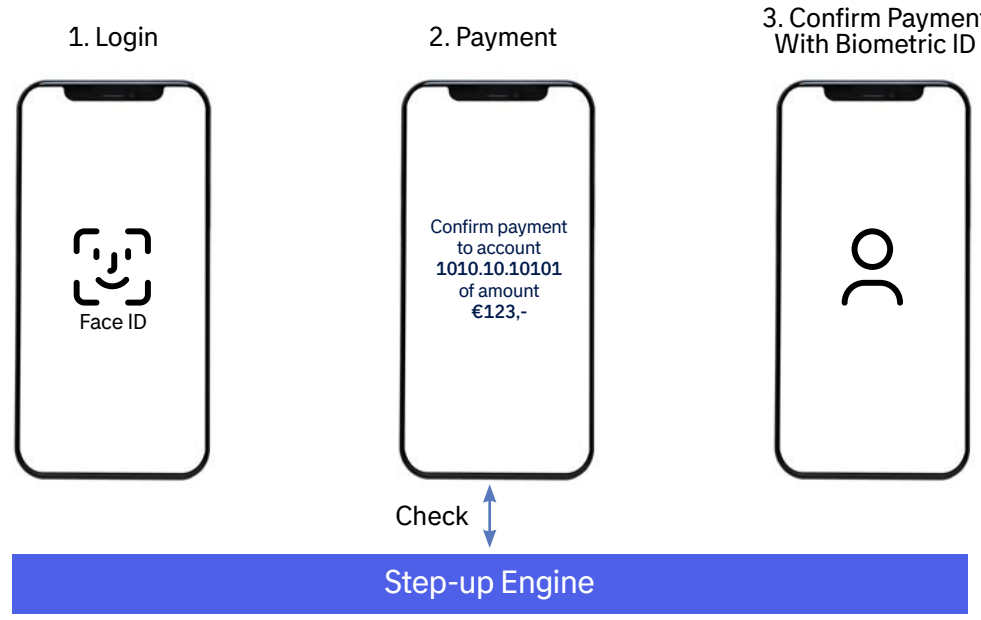
Trust as a Critical Component of Fraud Prevention

Finally, the fifth trend centres on the gradual erosion of public trust in digital systems, especially regarding data sharing and the role of artificial intelligence in fraud prevention. Consumers are more cautious about how their information is used, yet simultaneously expect stronger protection in an increasingly digital environment. This tension creates a fragile trust balance, where the need for robust security measures must be weighed carefully against the public's growing sensitivity to surveillance and automated decision making. Maintaining confidence will require not only effective technology, but transparent communication, responsible data governance and a more empathetic approach to customer interaction.

Together, these five developments point towards a future in which fraud becomes more human centred, more technologically amplified, more embedded in global networks, and more interlinked with public perceptions of trust and safety. The institutions best prepared for 2026 and 2027 will be those that understand these trends not as isolated movements, but as parts of a single, evolving ecosystem – one that demands earlier behavioural insight, stronger identity focused controls, and deeper collaboration across borders and sectors.

Identity Proofing: Raising the Bar in Fraud Prevention

Tieto Banktech's Identity Proofing service provides secure facial biometric verification by comparing the user's live video with a government issued identity document, such as a passport or national identity card. Once Identity Proofing is completed, a reusable Biometric ID is created, enabling a consistent and secure method for strengthening authentication across the customer journey. Biometric ID is applied in step up scenarios to elevate the authentication level and to ensure that a transaction is firmly linked to the correct individual.



The user will log in with one authentication method and will experience that the authentication requirement for confirming the payment is different than what he logged in with

Step-up Authentication: Enhancing Trust Through Robust Identity Checks

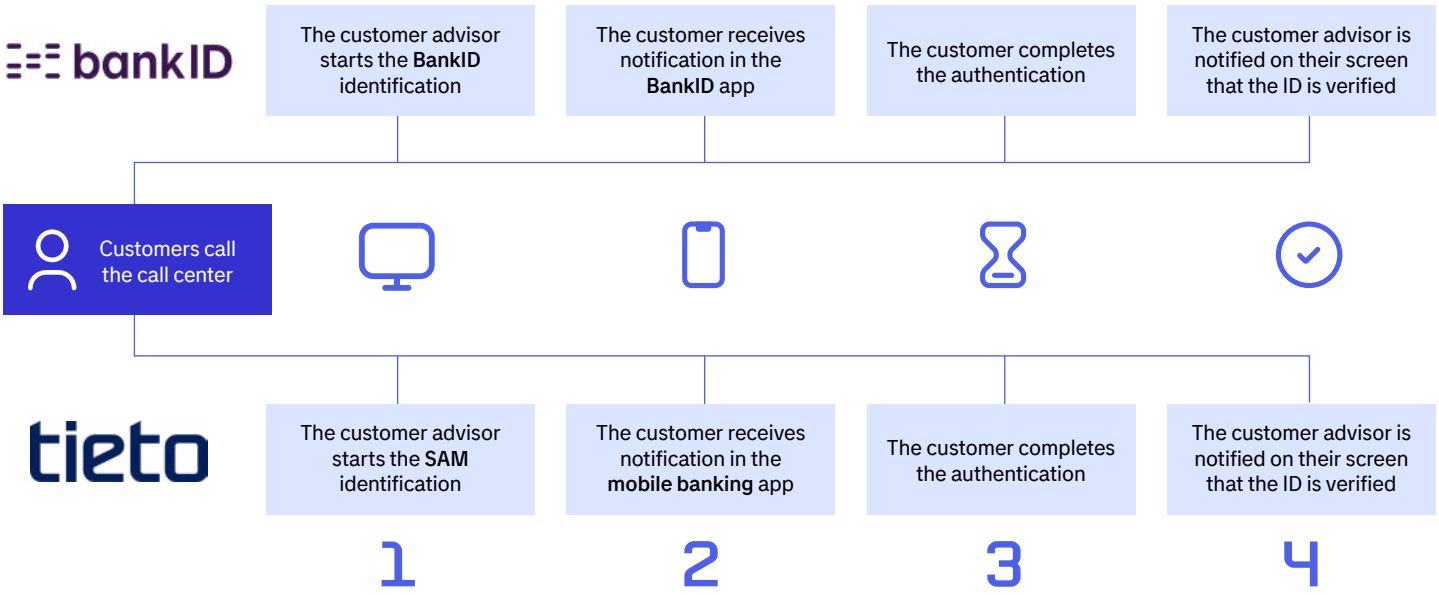
Step-up introduces an additional layer of assurance, requiring the user to provide stronger evidence that they are the legitimate account holder. This enhanced verification is triggered when a transaction carries heightened risk or value, ensuring that critical actions are protected by stronger controls. By defining tailored rules for different payment types, organisations can calibrate Step-up requirements to match the risk profile of each channel and scenario.

The selected Step-up method can be applied at the appropriate level within the preferred channel, ensuring that additional friction is introduced only where it strengthens security and reduces exposure to fraud. Step-up creates a controlled pause in the user journey, prompting the user to confirm their identity with more robust factors and allowing the transaction to be tied to verified biometrics. In practice, Step-up ensures that when high risk or high value actions are executed, the person carrying them out is indeed who they claim to be.

Caller Authentication: Elevating Trust in Customer Support

Caller Authentication provides a secure, modern, and high assurance method for validating a end-customer's identity during inbound calls. Rather than relying on traditional security questions, which are often unreliable, easily guessed, and susceptible to social engineering attacks, the advisor can initiate a biometrically anchored verification by entering the end-customer's Social Security number. This triggers a secure authentication request in the end-customer's mobile banking app, along with a clear contextual message explaining why verification is required.

05



The end-customer confirms the request and completes biometric authentication, such as Secure Access Mobile, BankID with biometrics or Biometric ID, ensuring that identity verification is tied to a unique, non-transferable, and high trust identity factor. Once authentication is complete, the advisor receives an instant confirmation, enabling the conversation to continue with confidence that the correct individual is on the line.

Caller Authentication delivers measurable value by enabling support teams to operate more efficiently and focus on higher-value tasks. By replacing manual checks with secure biometric identification, the solution strengthens digital trust and significantly lowers impersonation risk. End-customers benefit from a frictionless and familiar user experience, while organizations gain the flexibility to integrate the service seamlessly into existing web clients and advisor interfaces, ensuring minimal operational disruption and maximum security impact.

By introducing a controlled verification moment early in the call, Caller Authentication creates a predictable, secure, and user friendly process. The solution strengthens fraud prevention, increases advisor confidence, and ensures that critical actions are carried out by the legitimate account holder.

06

Artificial Intelligence to Enhance Payment Fraud Detection

Fraud Explore, which's engine is powered by our new and advanced Large Financial AI Model, represents the next step in strengthening real-time fraud detection across the Nordics and beyond. Instead of relying on predefined rules or known fraud patterns, Fraud Explore Engine learns how normal financial behaviour appears across billions of transactions. This enables Fraud Explore to detect unusual activity at an early stage, even when it does not match previously documented fraud. This can help banks to stay ahead of increasingly sophisticated tactics across cards, accounts, and digital payment channels.

What sets Fraud Explore apart is its integration with our upcoming real-time AI service layer. As transactions accelerate and fraudsters operate at machine speed, prevention must occur within the transaction itself. Fraud Explore evaluates risk within milliseconds, combining behavioural insights, anomaly detection, and contextual signals across all Defence Centre-monitored payments. This supports earlier intervention, fewer false positives, and clearer explanations for fraud analysts.

With Fraud Explore, we introduce a more adaptive and responsive layer of protection for financial institutions. The solution strengthens defences, reduces losses, and safeguards end-customers in an increasingly complex fraud landscape.

Customer-Driven Innovation: Our Strategy for Strengthening Fraud Defences for the Future

In an increasingly complex financial landscape, customer collaboration has become essential to safeguarding society against payment fraud. As criminal methods evolve rapidly, a coordinated response across organizational boundaries enables more proactive and comprehensive protection. By combining intelligence, aligning operational practices, and sharing effective methodologies, we can together ensure secure, reliable, and uninterrupted financial services.

Tieto Banktech's overall strategic direction, including for Fraud Prevention, builds on the principle that we innovate with customers, not just for them. Our approach combines long-term platform evolution with rapid, targeted co-development, ensuring that our solutions address real, validated fraud challenges faced by financial institutions across the Nordics and Europe.

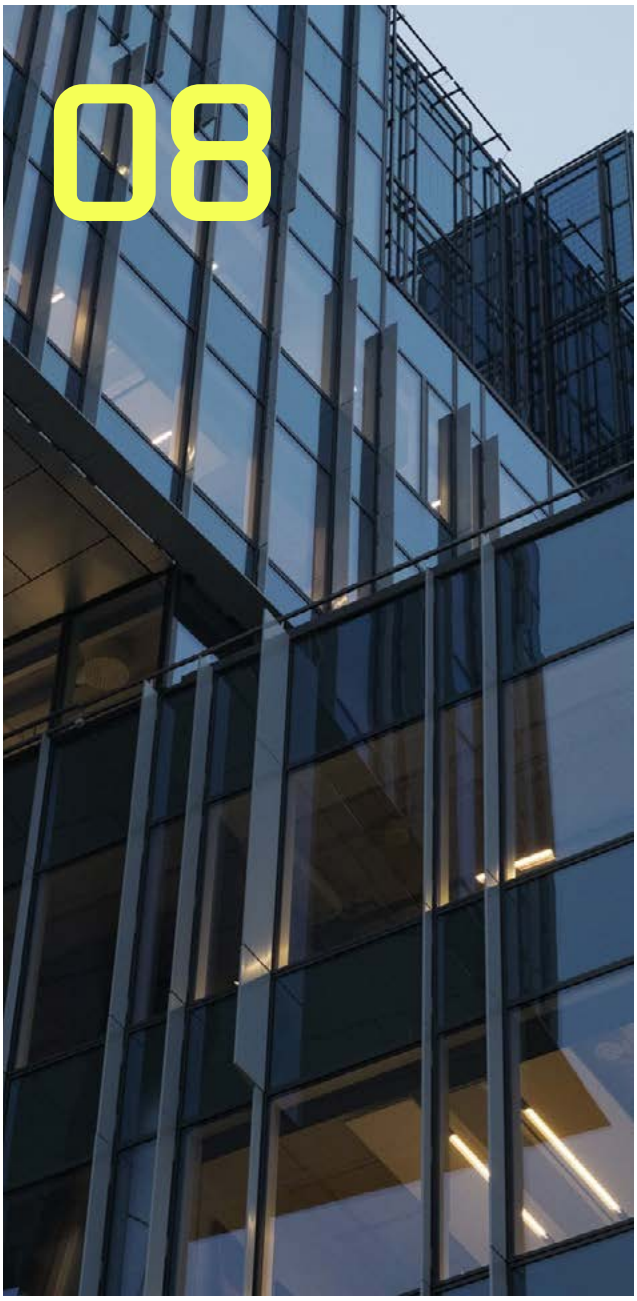
Joint initiatives across institutions and technology providers strengthen our collective ability to identify, mitigate, and prevent emerging fraud risks with greater accuracy. By integrating customer insights, pilot learnings, and real time observations from our 24/7 Defence Centre, we create a more resilient fraud prevention ecosystem – one that continuously adapts to new threats and reinforces trust in digital payment channels.

We operate in a threat landscape where criminal methods evolve faster than traditional delivery cycles. To stay ahead, we have established a structured innovation framework rooted in close collaboration, enabling earlier detection of new attack patterns and accelerating the development of countermeasures. This shared situational awareness is vital as fraud types such as social manipulation, identity theft, and mule activity increasingly require a unified and holistic perspective.

New regulatory frameworks such as PSD3 and PSR further reinforce the need for robust real time monitoring, strong identity assurance, increased transparency, enhanced data sharing practices, and state of the art security and privacy measures. These changes drive the industry toward stronger collective responsibility and higher protection standards.

To enhance our capabilities even further, we are embedding advanced AI across our platform, creating a more adaptive and responsive protection layer for financial institutions. By combining behavioural modelling with enriched internal and external signals, AI strengthens defences, reduces losses, and safeguards customers in an increasingly complex fraud environment.

Looking ahead, the need for close customer collaboration and shared innovation will only intensify. By uniting insights, analytics, and coordinated responses, we can collectively prevent and stop financial crime at a higher level – maintaining trust, protecting financial well being, and ensuring resilient payment services in an evolving threat landscape.



Contact us

If you have any questions related to this report or other matters, please do not hesitate to reach out to us:

Mette-Lise Engø
Head of Defence Centre
mette-lise.engo@tieto.com

Silje Andrea Kvernberg
Quality & Risk Manager
silje.kvernberg@tieto.com

Maria Helena Hestetun Midtbø
Head of Fraud Prevention
maria.midtbo@tieto.com

At Financial Crime Prevention, we don’t just fight fraud, we change lives.

Tieto is a leading software and digital engineering services company with global market reach and capabilities. We provide customers across different industries with mission-critical solutions through our specialized software businesses Tieto Caretech, Tieto Banktech and Tieto Indtech, as well as Tieto Tech Consulting business. Our around 15 000 talented vertical software, design, cloud and AI experts are dedicated to empowering our customers to succeed and innovate with latest technology.

Tieto's annual revenue is approximately EUR 2 billion. The company's shares are listed on the NASDAQ exchange in Helsinki and Stockholm, as well as on Oslo Børs.

www.tieto.com

tieto