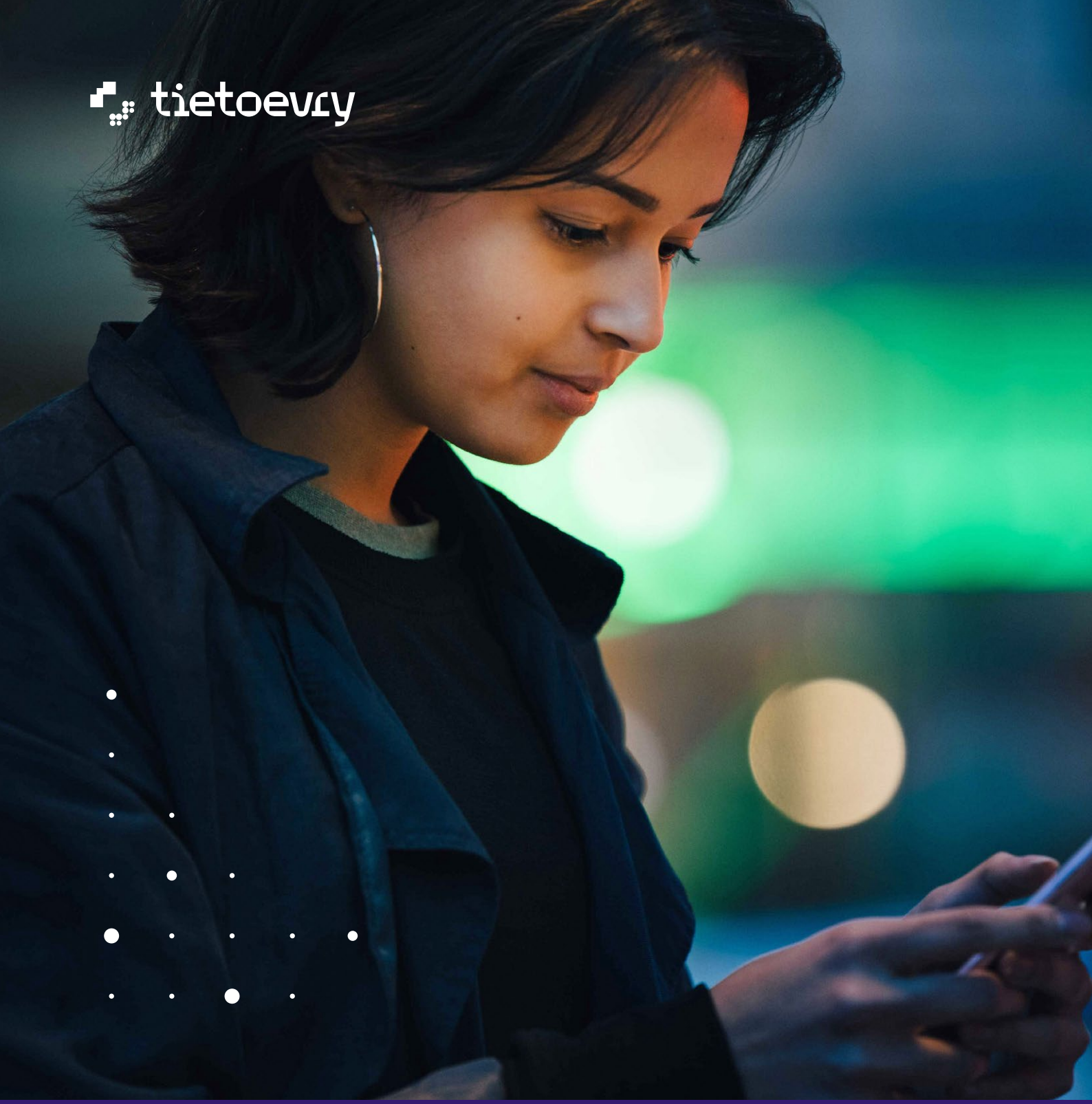


FinCrime Insights:

Payment Fraud Report

Table of Contents

Fraud Prevention:

Close collaboration is key

The scale of fraud extends far beyond financial losses. It strikes at the trust and integrity within our communities and institutions. Fraudulent activities undermine consumer confidence, investor trust, and impose significant costs on businesses, governments, and individuals.

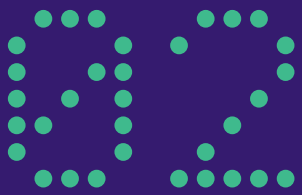
Given that fraud trends have shifted towards social engineering, we need to intensify the fight against financial crime. Many of the methods used are highly sophisticated, and criminals run various campaigns to target as wide an audience as possible. In general, we expect criminals to continue using new technology, with artificial intelligence (AI) being used to manipulate and acquire payment information. Advanced transaction monitoring and close industry collaboration are the solutions to expose more criminal activities.

This report seeks to highlight the current landscape of fraud, identifying key trends, emerging threats, and best practices in prevention and mitigation.

Since 1997, Tietoevry Banking Defence Centre has detected, stopped, and prevented financial crime. We are proud to contribute to safer payments, and to reduce the money-flow into criminal organizations. With the best of technology, combined with the best fraud fighters, we are ready to go the extra mile to prevent financial crime, now, and in the future.

André Moen Eide
Head of Defence Centre

Financial Crime Prevention
Tietoevry Banking



About Financial Crime Prevention Defence Centre

A leading provider of financial crime prevention in Scandinavia and Europe with **80+ customers**

Fully managed fraud prevention solution on card and account transactions

25+ years of experience with transaction monitoring

A team of **70+ experts** dedicated to round-the-clock detection and prevention of digital payment fraud

Integrating simultaneous **real-time monitoring** across multiple channels

Powerful financial crime prevention with customized, high-quality managed services

A Summary of 2023

What we have learned from handling over 134,000 fraud cases

In 2023, we were highly productive in our efforts to combat payment fraud. Our success rate in **detecting fraudulent activity reached 90%**, and we **handled 134,000 fraud cases**. Our real-time system **monitored over 3.4 billion transactions**, and we were able to decline approximately 70% of all fraudulent attempts without any financial loss.

Through our efforts, Tietoevry Banking Defence Centre prevented criminal organizations from obtaining over **236 million EUR**. This includes declined transaction towards rogue merchants with an intention to scam customers. **1.4 million transactions** were declined towards merchants selling false or illegal goods and additional **1.5 million transactions** were declined towards subscription and investment scams. We also launched the new service to block merchants related to mule activity.

Read about the service here

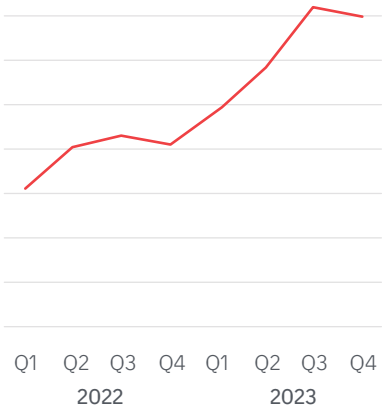
We took a proactive approach to address emerging threats. Before **Black Friday** we issued a warning about the surge in fake online stores. We noted a significant increase in fake online stores, with over 100% from the week before, and a 170% rise for the full year compared to 2022.

Be careful - don't let Black Friday turn into Blue Monday

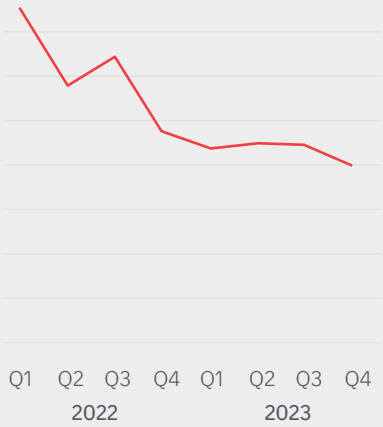
2023 was the first full year where we combined authentication data with card transaction data to get more accurate detection. **31 million EUR was detected** and prevented as fraud by the new 3D Secure Monitoring service, and we see that financial institutions that combine monitoring across different channels have reduced their losses.

To read more about this solution, please find information here

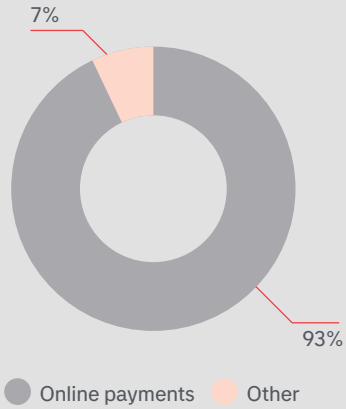
Fraud Case Development



Losses per case was lower in 2023 than in 2022



Majority is online payment fraud



There was a significant rise in fraudulent activity related to cards and accounts from the year 2022 to 2023, which is a cause for concern. In just one year, there has been a **68% rise** in fraud cases involving cards and accounts. Additionally, there has been a **63% increase** in fraud cases related to phishing fraud and a significant **153% increase** in fraud cases related to manipulation scams. It is worth noting that there was a decrease in cases involving copied cards with PIN (Payment Initiation Code) and cards stolen or lost in the mail, but an increase in cases involving copied cards without PIN codes and stolen or lost cards.

In addition to the significant increase in fraud cases, our team provided end-customer service by **handling over 225,000 phone calls.**

236 million EUR

Total value of prevented fraud

134,000

fraud cases handled

90 %

success rate in detecting fraud

225,000

customer service phone calls handled

Social Engineering

Social engineering is a rapidly expanding problem on a global scale. This manipulative strategy preys on people's vulnerabilities to gain access to confidential information or valuable assets. It is a technique that relies on exploiting human behaviour and can be carried out through various channels, such as social media, online interactions, phone calls, messages, and face-to-face interactions. Phishing fraud and social manipulation scams are the two primary forms of social engineering.

9

4.1 Phishing

Phishing is a fraudulent technique that is commonly used to acquire confidential information like payment card details or personal login credentials. Fraudsters can utilize this information to make unauthorized payments or transfers. **Phishing techniques are constantly evolving and becoming more diverse,** but the most used methods are email phishing, voice phishing, and SMS phishing.

Phishing attempts via email can take many forms, including spear phishing, generic email phishing, and CEO (Chief Executive Officer) scams. Unlike generic email phishing, spear phishing is an attack that is specifically aimed at individuals or organizations. It is intended to be more sophisticated and difficult to detect, as it often employs personalized language and information to deceive the recipient into acting. Conversely, generic phishing emails are usually easier to identify as they tend to use generic language, contain misspellings, and have poorly disguised malicious links.

AI may intensify impersonation scams

CEO scams involve impersonating a company's CEO to deceive employees into making fraudulent payments, while **Vishing** (Voice phishing) uses voice calls to deceive victims into giving away personal information. With AI, this problem will increase.

The ongoing improvements of generative AI are giving fraudsters new tools for impersonating others, and CEO scams, as well as spear phishing, will most likely increase in number and quality going forward.

Smishing (SMS phishing), another type of phishing technique, uses text messages to deceive victims into clicking on malicious links or downloading malware and often poses as familiar companies or organizations. An example of how AI is being used to great effect in CEO scams is the story about the *finance worker in Hong Kong who paid out $25 million after a video call with a deepfake of his company's 'Chief Financial Officer'.*

Read more

4.2 Quishing

A new type of phishing fraud known as "quishing" surfaced in 2023. This form of phishing involves the use of fake QR (Quick Response) codes to trick individuals into providing sensitive information. Fake QR codes are distributed via generic phishing emails but are also frequently found on restaurant tables or rental e-scooters. However, there have been reports of fraud involving fake QR codes placed on fabricated parking tickets. In some of these fraud cases, devices have been infected with malware.

4.3 Social Manipulation

Social manipulation is the practice of using persuasive techniques to influence and shape human behaviour, with the goal of acquiring valuables. This can be done in a variety of ways, such as through emotional appeals, deception, or coercion.

Psychological tactics

Social manipulation techniques are becoming highly sophisticated, and fraudsters are well-versed in exploiting human emotions for their own benefit. They often use psychological tactics such **as reciprocity, scarcity, authority, consistency, likability, and consensus** to manipulate people into giving them what they want.

For instance, they may offer something small or free to trigger the sense of **reciprocity** in people, making them feel obligated to give something back. They may also create a sense of **scarcity** by claiming that there are only a limited number of opportunities available, playing on people's fear of missing out. Additionally, fraudsters may pose as professionals or **authority figures**, using their perceived expertise to gain trust and credibility. They may also try to get potential victims to commit to something small first, then gradually increase the commitment, taking advantage of the **consistency** principle. Fraudsters may also try to establish a personal connection with their victims, using **likability** to their advantage. Finally, they may create a sense of **consensus** by suggesting that everyone is doing something, making people feel like they should too. Between 2022 and 2023, there was a notable increase in the number of fraud cases where people fell victim to social manipulation scams.

4.4 Four Common Types of Scams

The prevalent types of scams during 2023 included safe account scams, recovery scams, romance scams, and instances of extortion.

A **safe account scam** is a type of scam that involves vishing or smishing tactics, where the fraudster pretends to be a police officer or bank employee. The fraudster will claim that someone is trying to access the victim's account and steal their money, inducing a sense of urgency and fear. To prevent theft, the fraudster will advise the victim to transfer their funds to a "safe" account. In some cases, the fraudster may even visit the victim's home to collect their payment cards. Once the victim has provided their cards and PIN codes, the fraudster will withdraw all the funds from the account at the nearest ATM. The term used to describe these types of home visits is known as **courier scams**. Many of the safe account scams reported in 2023 was combined with a courier scam. The fraudsters who conduct these home visits are fully dressed in police uniforms and carry identification cards.

A **recovery scam** is a type of scam where fraudsters target individuals who have made previous investments. These scams usually involve fraudsters contacting victims and offering assistance in collecting their profits. These fraudsters often use social media platforms or messaging applications such as Telegram or WhatsApp to carry out their schemes, as well as vishing.

A **romance scam** is a scam where a fraudster poses as potential romantic partner to establish trust with the victim, and then deceives them into giving them money. These fraudsters usually make contact through social media platforms, dating apps, or email. They use various tactics to manipulate their targets, such as requesting money transfers or encouraging them to take out loans.

Extortion scams are a type of scam that preys on individuals by using blackmail and manipulation to coerce them into making money transfers. These scams often involve threats to release embarrassing or compromising information, such as sexually explicit photos or videos, to the victim's social media contacts or family and friends. In 2023, there were several fraud cases where individuals were forced to withdraw money from ATMs through physical coercion.

Different types of scams employ various manipulation tactics. Typically, fraudsters deceive victims into transferring funds using their personal information and credentials. In such cases, fraudsters do not require any additional personal information from the victim. However, phishing techniques can also be combined with manipulation scams, where fraudsters obtain the victim's personal information to execute unauthorized transactions.

Card Fraud

Card fraud refers to the act of obtaining unauthorized access to a credit or debit card and using it to make fraudulent transactions. This type of fraud occurs when someone steals or uses another person's card information without their permission to make purchases or withdraw funds. It can occur through various means, such as phishing fraud, skimming devices, or hacking into a merchant's database.

In 2023, there were 126,960 cases of reported card fraud, with a transaction volume totalling 3,3 billions transaction. Fortunately, due to the implementation of preventive measures in our Card Transaction Monitoring service, a significant loss of over 217 million EUR was prevented. In 67% of all card fraud cases there was no financial loss.

Fraudulent testing of cards was a prevalent issue during 2023, and a considerable number of cards were subjected to this kind of fraud. A common method used for fraudulent testing of a card is to enrol the card with a merchant and then check if the transaction is successfully authorized.

In 2023

126,960
card fraud cases

3,3 billion
transaction volume

217 million
EUR loss prevented

67%
of all card fraud cases had no financial loss

Data Breaches and Fake Online Stores

In 2023, a considerable number of Hong Kong-based merchants encountered data breaches. The breached card details were utilized to make travel-related purchases such as hotel bookings and plane tickets. Moreover, the compromised cards were also used to pay for online advertising on social media platforms like Facebook and Instagram. In some cases, the fraudsters also gained access to social media accounts. Additionally, many gaming accounts were also compromised. A considerable number of these cards were used in attempts to pay for electric bike rentals, food delivery, and visits to cafes and restaurants.

During 2023, there were numerous cases of card fraud following purchases from illegitimate online stores. Typically, these fraudulent attempts occurred within a few days to a week after the purchase, but in certain instances, they occurred mere hours after the purchase.

13

Authentication Fraud

Authentication fraud takes place when a fraudster obtains an individual's authentication credentials, which may include passwords, biometric data, or other sensitive information. This can be particularly risky in the case of SCA (Strong Customer Authentication), which is intended to prevent fraud by requiring multiple forms of authentication before authorizing payments. By using stolen authentication credentials, fraudsters can circumvent these security measures and execute unauthorized payments.

Rise in authentication fraud

The number of reported incidents of authentication fraud rose by 63% in 2023, reaching a total of 17,044 fraud cases. During this period, the total transaction volume was 10.5 million EUR. However, due to the implemented measures in our 3D Secure Monitoring service, a substantial loss of 31 million EUR was prevented.

Digital wallet fraud has become a concerning trend during the recent years, following the implementation of PSD2 (Revised Payment Services Directive) and SCA in 2020. The number of fraud cases involving digital wallets has increased by a staggering 300% from 2022 to 2023. Different types of phishing fraud are the primary cause of most of these fraud cases.

When it comes to attempted authentication fraud, a common method used by fraudsters is to transfer funds through different money transfer platforms.

The number of fraud cases involving digital wallets has increased by a staggering 300% from 2022 to 2023

Account Fraud

Account fraud is a type of fraud where an individual's financial account is accessed without their knowledge or consent, and money is taken from that account. This can happen through various means, such as phishing fraud or manipulation scams. It is a serious crime that can cause significant financial harm to the victim.

The year 2023 saw a rise in the frequency of fraudulent payments towards Turkish accounts. We've also seen an increase in fraudulent activities originating from Turkish IP adresses. Additionally, Moroccan, Dutch, and Spanish IP addresses have demonstrated a higher vulnerability to fraudulent activity than other countries in Europe.

A substantial number of account fraud cases in 2023 occurred due to three specific types of manipulation scams, namely recovery scams, safe account scams and romance scams.

Customer case:

Sparebanken Sør saved millions by deploying Account Fraud Monitoring in collaboration with Tietoevry Banking

Read how

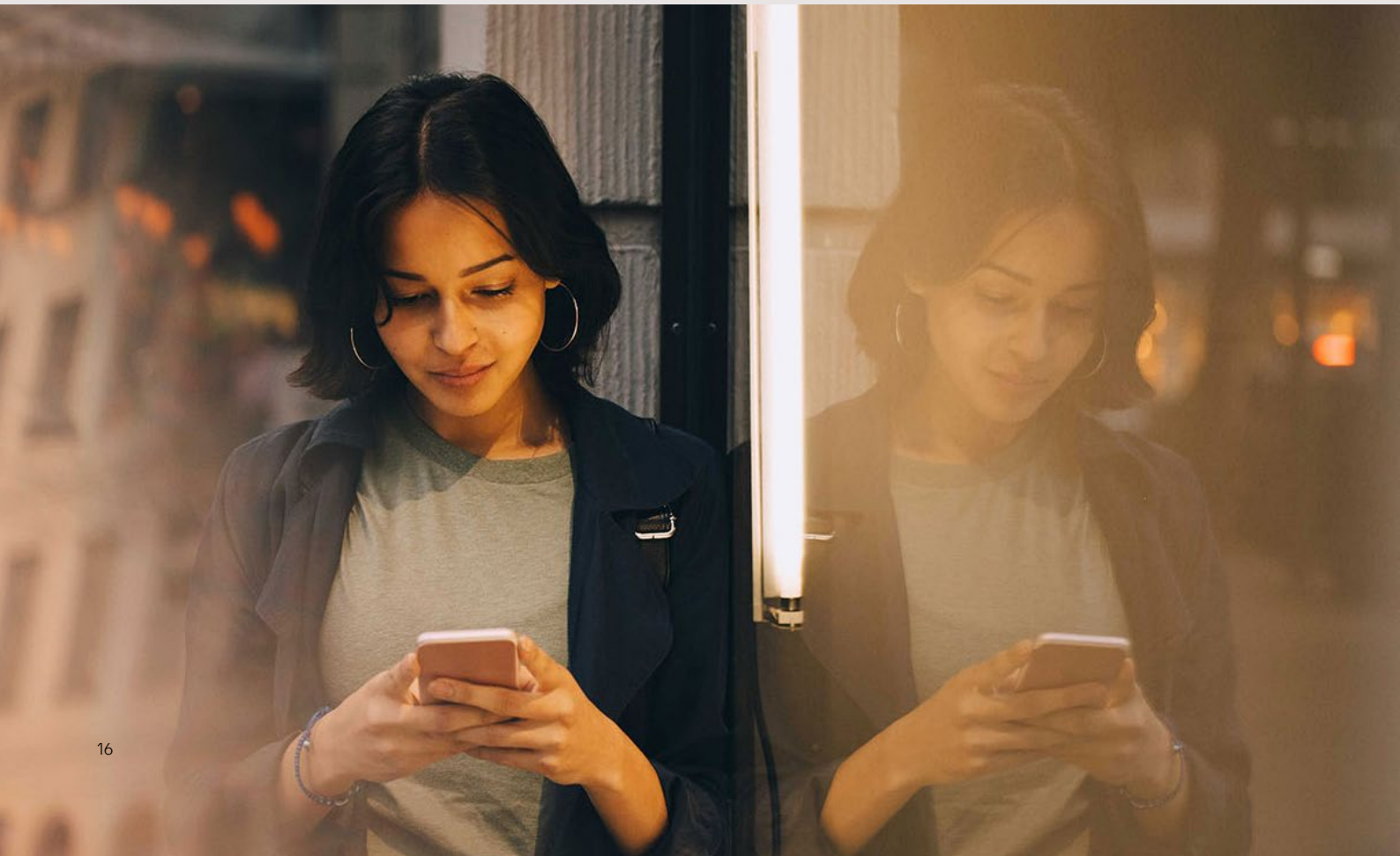
03

Mule Detection

In 2023, there was an increase in cases associated with money mules, involving both cards and accounts. Individuals are recruited to transfer illegally obtained funds in and out of bank accounts. These transfers may also travel through the card payment chain using legitimate money transfer services. The utilization of young individuals as money mules is becoming increasingly common, with the youngest known case occurring in 2023, where the individual involved was only sixteen years old. It is important to consider whether these individuals are knowingly acting as money mules or if they are unwitting victims who are unaware of the consequences of their involvement.

The Age of Money Mules is Trending Younger

Read more here



10

Forecasting Fraud Trends

As our knowledge of social engineering and methods to safeguard ourselves and our finances increases, fraudsters must adapt their tactics to obtain our payment information or persuade us to make payments. Despite our efforts to stay ahead of them, fraudsters continue to surprise us with new and cruel ways to scam individuals out of their money.

Unfortunately, as we become more informed, these fraudsters may become even more ruthless in their attempts. It is anticipated that the prevalence of safe account scams and recovery scams will persist beyond 2024, and it is highly probable that numerous new manipulation methods will emerge.

Read more about fraud trends here

Physical Extortion

Minors and young adults have manipulated other minors into making Vipps, Swish and other instant payment transfers through physical force. It appears that this type of physical extortion is proving to be successful, so it is likely that it will continue to occur for a while.

Digital Wallet Fraud

In recent years, digital wallet fraud has also been on the rise due to phishing attempts. Despite the existence of digital wallets for some time, they are becoming more prevalent, making them a prime target for fraudsters. Regrettably, these phishing attempts have been successful in compromising individuals' digital wallets, and this trend is expected to persist.

Phishing Using QR-codes: "Quishing"

There is a possibility that the new phishing scheme, "quishing", may become more prevalent during the summer months, especially in locations such as restaurant tables and electric bikes. Fraudsters are likely to succeed with quishing since many people are not aware that a QR code is essentially a hyperlink.

Money Mules

The trend of money muling appears to be a persistent issue, with no indication of a decrease in the number of related cases. It is concerning that fraudsters may continue to target younger and younger individuals, exploiting new methods to deceive them into becoming involved in this kind of fraud, whether knowingly or unknowingly.

Fake Online Stores

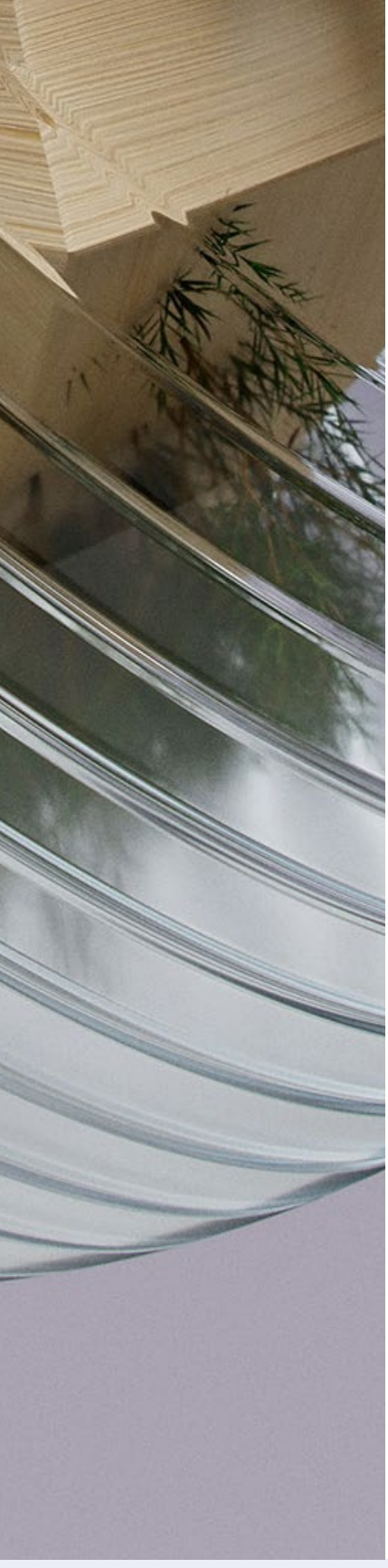
It is also likely that the trend of illegitimate online stores compromising and misusing customers' card details will persist.

> Individuals are increasingly being deceived by phishing campaigns that utilize the names of well-known hotels, streaming services, and postal companies

11

Our Approach to Battling Fraud

In our ongoing mission to combat payment fraud, we are constantly developing fraud prevention services that enable us to stop more instances of fraud. This chapter delves into our strategic initiatives and highlights the importance of staying ahead of emerging fraud trends.



Token Enrolment Monitoring: Our ongoing enhancement of fraud prevention capabilities includes the introduction of Token Enrolment Monitoring. This service monitors the enrolment of cards into digital wallets, aiming to prevent fraudsters from enrolling victims' cards into their own digital wallets. This proactive measure plays a crucial role in combating the increasing trend of token fraud.

Real-Time Mule Monitoring Solution: Recognizing the significant rise in money muling activities associated with fraud, we are in the early stages of exploring real-time solutions. Our objective is to implement measures that promptly halt transfers to and from individuals involved in money muling schemes. By adopting these proactive measures, we disrupt the operations of fraudsters and safeguard our clients' assets.

Integration of Additional Bank System Information: As part of our commitment to bolster fraud prevention measures, we actively seek opportunities to integrate supplementary information from other bank systems. By leveraging data from diverse sources, we enhance our ability to identify fraudulent patterns and protect our clients from potential threats.

Helping Manipulated Customers Understand the Risks: In addition to our prevention measures, we are dedicated to helping customers who have been manipulated understand the risks they face. Through empathetic communication, tailored conversation techniques, and by presenting compelling facts, we aim to empower these customers to recognize the potential dangers and make informed decisions, ultimately assisting them to stop transferring money to the fraudsters.

Collaboration with Schemes and Market Actors: Recognizing the value of collaboration in combating fraud, we are exploring possibilities to collaborate with schemes and other actors in the market. By working together, we can pool resources, expertise, and knowledge to develop comprehensive strategies and solutions that address fraud at a broader industry level. We are now integrating Visa score as an external signal in our rule engines to strengthen our fraud prevention measures and create a more secure financial ecosystem.

As we continue our efforts in combating payment fraud, we remain steadfast in our dedication to innovation, staying ahead of evolving trends, and fostering collaboration. Through initiatives such as Token Enrolment Monitoring, real-time mule monitoring, leveraging AML question and answers, integrating bank system information, and assisting manipulated customers, we strengthen our defence against fraudsters. Moreover, by engaging in collaborative efforts with schemes and other market actors, we foster a united front against fraud, creating a safer financial environment for all.

New Study Program

One approach to combating Fraud is that Tietoevry Banking is entering into a collaboration with **Nord University** aimed at enhancing education on digital financial crime prevention. Together with **Kunnskapsparken Helgeland** and **SpareBank 1 Helgeland**, a new study program will be developed to focus on strengthening skills to combat financial crimes in Norway more effectively.

Read more here

5 Tips to Reduce the Risk of Falling Victim to Payment Fraud

Fraudsters are often professional actors, and anyone can be deceived. With the rapid development of AI, there are five things everyone can consider:

- **Verify the Identity of People Who Contact You:** Fraudsters can exploit AI to create synthetic voices and conduct phone scams. It's also possible to recreate voices of people you know and trust. If in doubt, ask control questions and request the person contacting you to verify themselves with information only they would know.
- **Never Disclose Sensitive Information in Calls or Messages:** Be especially cautious with unexpected communications asking for personal or financial details. Do not approve any logins or transactions upon request without verifying the purpose. It's common for fraudsters to claim they are calling from a bank or authority.
- **Be Skeptical of Unexpected Messages:** Think twice before clicking on links or opening attachments. Be wary of messages asking for quick money transfers from friends or family. Their email or social media accounts might have been compromised.
- **Be Aware That Public Information Can Be Exploited:** Remember that all information shared publicly, both on social media and in other digital environments, is also accessible to criminals. Personal information can be used by fraudsters to craft convincing scams. With AI, it's possible to mimic individuals in voice, image and text.
- **Beware of Fake Online Stores:** Many card frauds occur through fake online stores designed to resemble reputable and established online retailers. Therefore, double-check the web address carefully and be skeptical of offers that seem too good to be true.

Closing Remarks

As highlighted in this report, financial crime is on the rise, and we need to increase our efforts to stay ahead. The banking industry needs to work closer together to fight the fraudsters. If we collaborate across the industry in conjunction with authorities, we can affect a larger and more rapid change. Close collaboration and data sharing is crucial to build the best fraud detection solutions without breaking the customer experience with too much friction. Sharing insights and best practices helps us stay ahead of evolving threats. We need to balance these measures and tune the recipe day to day.

Tietoevry Banking are confident that we have the best toolbox to fight financial crime, and the greatest asset in this solution is our dedicated people. We thank all fraud fighters for their efforts, making the world a safer and better place!

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

André Moen Eide
Head of Defence Centre
andre.eide@tietoevry.com

Silje Andrea Kvernberg
Quality Manager Defence Centre
silje.kvernberg@tietoevry.com

Line Snefrid Borgsø
Head of Fraud Product Management
line.borgso@tietoevry.com

Tietoevry creates purposeful technology that reinvents the world for good. We are a leading technology company with a strong Nordic heritage and global capabilities. Based on our core values of openness, trust and diversity, we work with our customers to develop digital futures where businesses, societies, and humanity thrive.

Our 24,000 experts globally specialize in cloud, data, and software, serving thousands of enterprises and public-sector customers in approximately 90 countries. Tietoevry's annual turnover is around EUR 3 billion and the company's shares are listed on the NASDAQ exchange in Helsinki and Stockholm, as well as on Oslo Børs.
www.Tietoevry.com