

Payment Fraud Report



Eesti Pank
EUROSÜSTEEM

2026

The Payment Fraud Report produced each year by Eesti Pank summarises the statistics on payment fraud from the previous year, the most common scams, and the measures taken to stop fraud.

The Payment Fraud Report is published on the [Eesti Pank website](#).

The report is compiled by Eesti Pank, the Estonian Banking Association, the Police and Border Guard Board and the Ministry of Finance

Online

pdf ISSN 3125-5914

Layout and design

Urmas Raidma

SISUKORD

REVIEW OF FRAUD IN ESTONIA	4
TYPES OF FRAUD	4
Authorised push payments (APP).....	4
Phishing, account takeover and identity theft	5
Card fraud	6
EXAMPLES OF CURRENT FRAUDS.....	6
Business email compromise	6
Investment fraud	6
Multi-stage telephone fraud	7
Courier fraud	7
WAYS THAT FRAUDS ARE INITIATED	9
Payment transfer fraud.....	9
Card fraud	11
Frauds affecting businesses.....	12
STATISTICS ON FRAUDS	14
Turnover and number of frauds	14
Types of fraud	14
Average losses to frauds.....	17
FRAUDS BY REGION	19
Card fraud with Estonian bank cards	19
Credit transfer frauds with Estonian bank accounts.....	19
COUNTERING PAYMENT FRAUD IN ESTONIA	21
Roundtable for countering financial fraud.....	22
The main activities involved and the results of executing the action plan of the roundtable, and the activities initiated by participants in it.....	22
Individuals as the first line of defence against fraud – how you can help stop scams	24

REVIEW OF FRAUD IN ESTONIA

A new wave of payment frauds broke in 2025 that caused much greater losses than before, though the increase in the number of fraud incidents was smaller. The greatest losses were again caused by credit transfer frauds, the most common of which were investment fraud and multi-stage telephone fraud. Telephone frauds are when the fraudsters present themselves as representing a private company or public institution such as a delivery company, a mobile phone network, a bank or the police. They claim to be providing services and verifications in order to confuse their victims and gain their trust. Most of the victims lose money by transferring it to the fraudsters themselves. In a third of cases the criminals succeeded in gaining access to the bank accounts of the victims, which allowed them to move the money that was in the account and take out loans in the name of the victim. Small businesses and their bookkeepers and owners were particularly targeted by criminals seeking access to both personal and corporate accounts. There were also cases of invoice fraud. Frauds involving cash and more specifically ATMs are becoming increasingly common among card frauds. Fraudsters try to convince their victims to place their bank card together with the PIN code in a parcel locker, or to withdraw cash and hand it to a courier who collects it from them at home. Frauds involving ATMs are by now the main form of card fraud, and the losses from them already exceed those from card fraud in e-commerce.

TYPES OF FRAUD

Authorised push payments (APP)¹

- **Sales fraud.** The victim buys goods or services from an online store or reseller, but the seller disappears immediately after the payment has been made and the goods and services are not delivered.
- **Investment fraud.** The victims are snared with promises of large returns on an investment. These are often spread through social media or through adverts in search engines, or by telephone. The promise of exceptionally large potential returns leads the victims to act incautiously. The frauds mostly use fake platforms and fake brokers who encourage the investment.
- **Romance fraud.** The fraudster creates a believable relationship with the victim, usually through social media, and over time starts to ask them for financial help. They often explain that they need the money to travel to meet the victim, to get out of debt, or to apply for a visa. They may also ask for money as a short-term loan, which is then never repaid.
- **Charity fraud.** The victim is contacted by what is apparently a charitable organisation or individual asking for a donation. The appearance of charity is used to get money from the victim, often through long-term manipulation.
- **Advance-fee fraud.** The fraudster promises the victim a large amount of money, but needs them to pay a processing fee, tax or other costs in advance. After the advance fee is paid, the promised money never arrives. This is commonly called the Nigerian Prince scenario.
- **Business email compromise (BEC) fraud.** Business customers are sent a fake invoice or a notification of a change of account number that redirects payments to the bank account of criminals.
- **CEO fraud of businesses.** The fraudster uses a compromised email address or a deepfake video or sound recording created using artificial intelligence to present themselves as the senior manager of a company and instructs their bookkeepers to make an immediate and confidential transfer to a business partner, but the money actually goes to the account of the fraudster.

¹ Frauds where the victim initiates and confirms the payment themselves even though they have often been previously manipulated or fed false information.

- **Employment fraud.** The victim is offered a job, but is asked to pay some related costs before starting work. The job that is offered does not actually exist.
- **Secure account fraud.** The victim is contacted and convinced that their money or securities are not safe in the financial institution that holds them. They are asked to transfer the money to a specified account to keep it safe. The account actually belongs to the criminals, who do not return it.

Phishing, account takeover and identity theft²

Account takeover (ATO) uses various means of attack, and the most common in Estonia in 2025 was multi-stage telephone fraud. In these events the victims themselves may authorise transactions, having been manipulated by the fraudster to give access to their means of authentication for example, or to install remote management software on their computer. Such cases are different to frauds using authorised payments in that the victim generally loses control over their own bank account.

- **Multi-stage telephone fraud claiming to be from an official or a company.** The fraud generally starts with an apparently innocent telephone call. The fraudster in this first stage may claim to work for a courier firm and say that documents need to be delivered for example, or for a mobile phone operator and say that data need to be updated to allow the client's package to be changed. The actual aim is to get the victim's identification using their PIN1 code. A new fraudster calls the victim in the second stage and generally claims to be calling from a bank or the police and to be giving a warning that the victim's bank account may now be in danger because of the earlier call. The conversation is often transferred to a different platform like WhatsApp, which the banks and the police do not actually use for communicating with clients. The victim may next be told that a secret police operation is being organised to resolve the situation, and as part of this they are asked to transfer money to an apparently secure account and to confirm the transfer using their PIN2 code.
- **Data theft by email, or phishing.** The victim receives an email sent from an address and in a format that is similar to those used by a bank or other service provider. It contains a link that leads to a fake login page that is used to harvest card data or other confidential information.
- **Data theft by SMS, or smishing.** The victim receives a text message from a sender whose data have been forged or spoofed, and is asked to reveal their card data or their PIN codes for Mobile ID or Smart ID. They may be told for example that they need to pay to collect a package.
- **Data theft by voice, or vishing.** This is similar to telephone fraud, as the fraudster claims to be calling on behalf of an institution or a company and tricks the victim into giving out their card details or their PIN codes from Mobile ID or Smart ID. Vishing is effective because the fraudsters can gain the confidence of the victim while causing them to panic at the same time and pushing them to act in haste.
- **Data theft by QR code, or quishing.** This is the newest form of fraud, where fraudsters stick QR codes they have created themselves in place of original QR codes. Anybody scanning the code is taken to a fake website, where they are asked to enter their data.
- **Advertising fraud.** The victim is shown an advert or a banner online that might offer an instant loan with a low interest rate for example, and they are asked to fill in an online form to receive it. The victim is actually handing the fraudster their sensitive personal data by doing this. The next step is often investment fraud, which attacks the victim using the data that they have already handed over.

² Actions by the fraudster to gain the sensitive data of victims that they can use to make payments in the victims name.

Card fraud³

- **Lost or stolen card.** The card falls into the hands of somebody other than the owner and is used to make as many payments as possible before the owner or the bank manage to block it.
- **Card-not-present or CNP fraud.** Stolen card data are used for making purchases online or in a similar form where the physical bank card is not required.
- **Copying or skimming of cards.** This mostly happens when the victim enters their card into an ATM or payment terminal that contains a device for copying card data. The data that are copied are used to make a clone of the card that the fraudster can use for payments.
- **Point-of-sale or POS fraud.** An inflated amount is entered into the payment terminal in the hope that the victim is inattentive, or perhaps drunk, and confirms a payment of 1000 euros instead of 10 euros for example. Alternatively the same payment may be taken off the card multiple times, or a skimming device may be fitted into the payment terminal.
- **ATM fraud.** This can take various forms, as the fraudster might for example persuade the victim to withdraw cash from an ATM and hand it over to them. They may alternatively gain access to the card data and use the physical bank card or a digital wallet to withdraw money from the victim's account.

EXAMPLES OF CURRENT FRAUDS

Business email compromise

- A company received an email that appeared to come from one of its partners asking it to use a different bank account number in future when it paid invoices. The new account was actually a fake account, and the company made two credit transfers to it. The initial data show that the amount lost to the fraudsters was over 1.6 million euros.
- Fraudsters sent a company an email that claimed to be from a lawyer who was at that time helping the company to purchase real estate abroad. The email stated that the bank details of the guarantor or mortgage holder of the real estate transaction had changed. The company transferred money to the account of the fraudsters instead of to that of its partner. The amount lost to the fraudsters was 1.7 million euros.

Investment fraud

- A 43-year-old woman met a man on Facebook, and five months into the relationship he brought up the topic of trading and investing in crypto currencies. He recommended a broker he knew, who had agreed to help and guide the woman in making investments. The woman received a phone call in early September from a person who guided her through the registration process for opening an account on the trading platform finab.pro, and she made her first payment into it of 100 dollars. Over three months the victim created several crypto wallets for herself under the guidance of the same person, and says she transferred a total of 94,000 euros to the trading platform and crypto addresses. She took out several loans in her own name and her daughter's name to be able to fund this, and she sold her daughter's apartment. She also handed cash over to couriers on several occasions, believing it to be for investment through the platform. The victim cannot withdraw the money that is in the platform and is being asked to make additional payments. The initial estimate is that she lost 122,000 euros to the scam.
- A man from Anija read a fake article on the internet that appeared to be written by the Estonian businessman Margus Linnamäe on the subject of investment, and he gave his contact

3 Fraudulent transactions where the fraudster uses a bank card, the data for the card or a copy of it.

details to the website. He later received a telephone call from somebody who helped him set up crypto wallet accounts with Revolut, Bigbank and Mercury, and he made his first payments to the platform. Over the next couple of months the victim was guided by the scammers in giving remote access to his device through the AnyDesk app, took out loans, and made transfers to a crypto wallet that had been opened in his name. The victim cannot withdraw the money that is in the platform. The initial estimate is that he lost 36,529 euros to the scam.

Multi-stage telephone fraud

- The victim was called and asked whether they and their partner receive discounts on medicines. They said no, at which the caller offered to get them a card that would allow them to buy medicines from the pharmacy at a discount in future. The caller then said that the victim and their partner would need to go to the medical centre for an analysis and health check-up. They also asked the name and home address of the victim's family doctor, which the victim gave them. The victim was then called by a second fraudster who claimed to be from the police and said that the first call was a scam. This caller then promised to take the victim through the process that would keep their money safe from the scammers. They said it was important not to tell anybody about what had happened because doing so would be a criminal offence, and they agreed on a secret password. The victim had to put their bank cards and those of their partner in an envelope and hand it to a courier who would identify themselves with the password. The scammer added that the courier would be wearing a face mask to avoid spreading any viruses. About half an hour later, the elderly couple was visited by a masked man to whom they handed an envelope containing their bank cards. A little later the scammer called again and confirmed that they had received the envelope and emphasised that under no circumstances should the couple tell anybody about this. Sometime later the victim became suspicious and tried to call the supposed police officer back, but the number was not available. They then contacted the police.
- The victim was initially contacted with an offer to change his water meter. He was then contacted by someone claiming to be a police commissioner, who said that fraudsters were targeting his apartment and would have taken it from him if the police had not intervened. He was told that he now needed to work with investigators to help identify the fraudsters so they could be caught. The caller instructed him to phone a number he was given for a company that buys real estate, and to act as bait by pretending to them that he wanted to sell his flat. The fraudster said that if the man helped the state, then the state would help him in return. He also emphasised that the man should not tell anybody about this investigation, and referred to an apparent legal requirement for confidentiality. The man then had to sign a fictitious sales agreement for his apartment, and process the apartment and the documents for it. He was also given very clear instructions on what to say to the notary so as not to arouse any suspicion. Once the money from the sale of the apartment had appeared on the man's bank account, he was ordered to transfer it to an apparent real estate fund, and register on a crypto currency exchange. As his bank refused the transaction, the criminals instructed him to transfer the money to another bank, take some of it out in cash and use the rest to buy gold. They promised that once the cash had been withdrawn, the apartment would be put back in the name of the victim. The man then gave the money received from selling the apartment and the gold that was bought with it to a cash collecting courier that the criminals had sent.

Courier fraud

- The victim received a call that was apparently from an Omniva courier saying that she had been sent a registered letter. So that she could receive the letter, the caller sent a Smart ID confirmation code to her device, and she used her pin code to confirm the transaction initiated by the criminal. Some minutes later she received another call that apparently came from the police. She was told there had been a suspicious login to her account, and it was probably the

work of criminals. The criminal claiming to be a police officer then said that the bank would contact her immediately to explain what she needed to do to safeguard her money. She was told that for the sake of the investigation she should deposit her bank cards in a parcel locker, and that she must not tell anybody about the incident because that could harm the investigation. The fraudsters then told her that an attempt had been made to take out a loan against her car, and recommended that she sell the car so that the criminals would not be able to use it. They told her where to sell the car and explained that the buyer was a criminal engaged in money-laundering, who they would be able to arrest once the transaction was complete. The victim also had to place the money received from selling the car in a parcel locker for the sake of the investigation. The criminals promised that all the evidence was secure, and that the woman would get her car back the next day. She never got the car or her money back, and lost more than 21,000 euros to the scammers.

- A businessman was called by an Estonian-speaking fraudster claiming to be a courier from Omniva. He was told that he had received a registered letter from the Tartu County Court. As the victim had recently filled in documents and handled business issues there, the call seemed quite plausible. The victim was also very busy with work at that moment, and so did not have time to think the matter through in detail. The supposed courier promised to put the letter in a parcel locker and send the code needed to collect it to the victim's phone. A Smart ID authentication request reached the man's phone during the call, and he selected the confirmation code from the display. He then had to enter his PIN1 code. The caller remained quiet during this and did not put any pressure on the man, who entered the code himself into the Smart ID app. A couple of minutes after the first call had ended, the man was called again by an Estonian-speaking man who claimed to be the police detective Heiki Reest. This caller said that the victim's data were now in the hands of criminals who had already taken out a loan in his name, and he now needed to act quickly to protect his bank accounts. The caller then explained at length how the criminals operated in order to gain his confidence. The call was then passed on to a further fraudster who claimed to be an SEB employee called Maksim Reiman. The victim followed the instructions of the callers, with the result that they logged into his internet bank and started to transfer money out of his personal and company accounts into another bank account, claiming that this would protect his money.

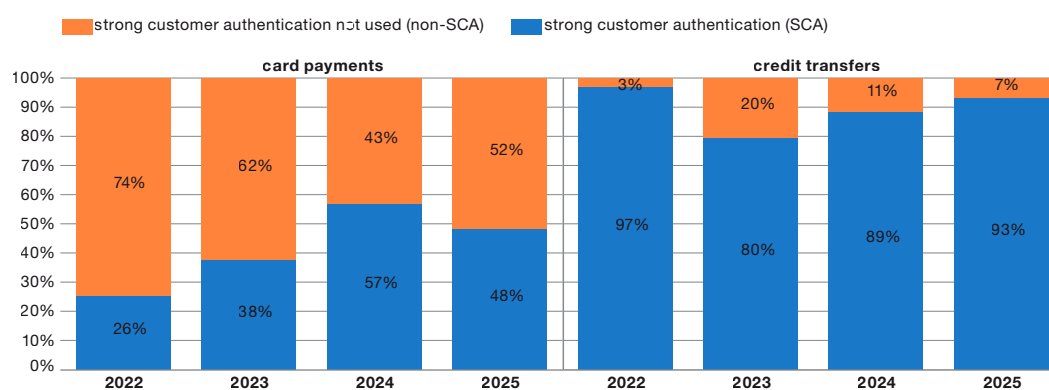
WAYS THAT FRAUDS ARE INITIATED

Payment transfer fraud

Statistics compiled by Eesti Pank show that 93% of the credit transfer frauds last year were made using strong authentication (see Figure 1). Credit transfers in internet and mobile banks use strong authentication, where the transaction is confirmed not only by logging into the site, but also with Smart ID, Mobile ID, an ID card, a PIN calculator or some other means of two factor authentication, often requiring a PIN2 code. Types of credit transfer fraud include authorised push payment (APP) fraud and various phishing and identity theft scams.

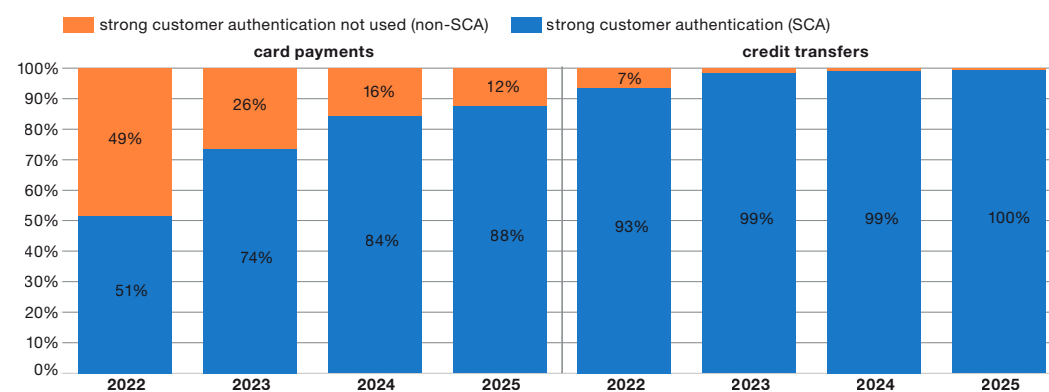
APP frauds work by convincing the victim to hand money over from their own account to one controlled by a criminal. The usual anti-fraud methods that aim to restrict access to an account do not necessarily work for such credit transfer frauds, as the victims themselves initiate and confirm the payment. The most effective means of preventing such frauds are public information campaigns and awareness raising.

Figure 1. Strength of authentication by share of the number of transactions



Source: Eesti Pank

Figure 2. Strength of authentication by share of value



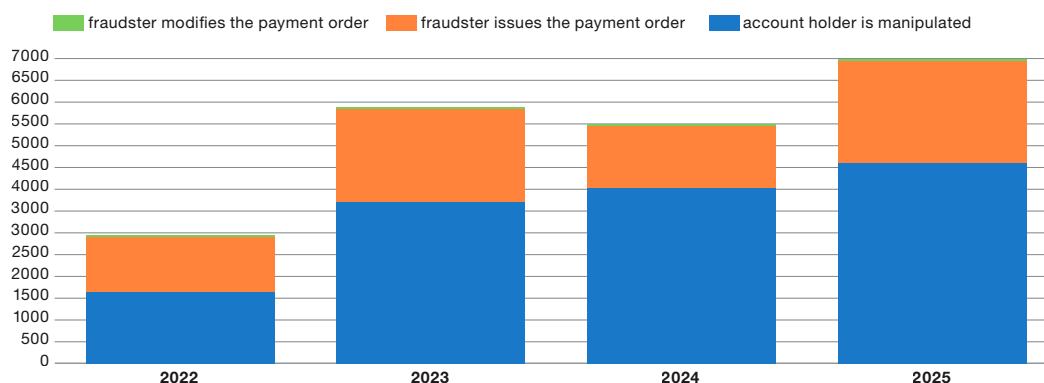
Source: Eesti Pank

Authorised push payment frauds can include investment frauds, secure account scams or multi-stage telephone frauds that persuade the victim to transfer their money to a supposedly safe place, and advance-fee frauds that promise to pay the money back later. Almost 100% of the losses from APP frauds occur in transactions with strong customer authentication (see Figure 2). The remaining transactions that do not use strong customer authentication are mainly small payments that do not need to be confirmed with the secondary PIN2, or repeat payments. APP frauds generally claim an urgent

need to complete the transaction quickly, or a promise that large profits can be earned in a short time. This causes the victims in two thirds of cases to make the transfer themselves to the criminals at the point when they are distracted from the content of the payment by the need to hurry and make it quickly (see Figures 3 and 4). Another trick that the fraudsters use is to gain access to the victim's account and enter credit transfer instructions themselves in the name of the victim. This happens in a third of cases. Such multi-stage frauds try first to get the victim to hand over their own security codes. The fraudster can then use these to log in to the internet bank, where they can change the settings on the account and increase the payment limits, apply for instant loans in the name of the victim, and initiate payments to move the money quickly to the accounts of money mules.

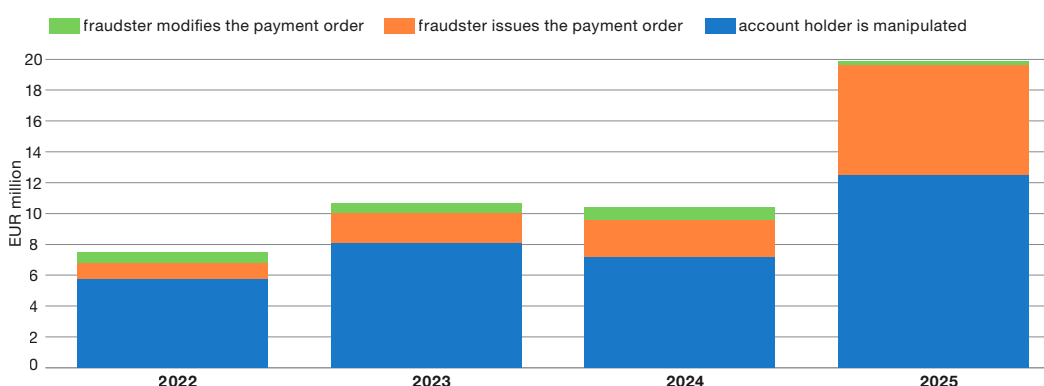
A money mule is a person who shuffles illegally acquired money through multiple bank accounts and receives a fee for doing so. The aim of this is to disguise the origins of money acquired from fraud or other criminal activity and help to move it onwards quickly. The accounts used by the money mules are often located in different countries.

Figure 3. Credit transfer fraud by initiation method



Source: Eesti Pank

Figure 4. Value of payment order fraud by initiation method



Source: Eesti Pank

The fraudsters put great emphasis on keeping the relationship with the victim going as long as possible, so that they cannot call their bank, family members or anybody else for help. The relationship does not always end once the fraud has been committed, as it may continue for several more hours to give the fraudsters time to move the money onwards, through the accounts of money mules for example. This reduces the risk to the criminals of the victim being too quick to give warning of the scam or a suspicion of it. Another reason for maintaining the relationship is to distract the victim so that they do not notice suspicious details like a fake website address, an unusual authentication site, or the need to

enter their PIN1 and PIN2 codes more often than usual. The best antidote to these cases is to take a break to calm down, even if it appears that there is a real emergency demanding immediate action. It is always important before confirming a transaction to think through how it was initiated. If it was initiated by a telephone call that was made by somebody else, the risk of a scam is high, especially if the call was made over a communication channel such as WhatsApp or Telegram. Victims are manipulated to believe that the fake police officer or other official who has contacted them through the communications platform is using them to take part in a secret operation, and so they can be engaged by the fraudsters for a long time because they believe they are helping to save their own money and that of other victims. Especially dangerous are those cases where the apparent problem can only be solved by transferring money to another account, or where the caller asks the victim to reveal their PIN codes or confirm an authentication request they have sent.

Card fraud

Card frauds can be divided by how the payment transaction is initiated into the two categories of transactions made with a physical card, and remote or card-not-present transactions, where only the data of the card are used. The first type use forged or stolen bank cards to withdraw cash or make payments in payment terminals, while the second occur when criminals have obtained the card data and use them for online transactions, including purchases from online stores. Card transactions with strong authentication are 48% of fraudulent card transactions (see Figure 1), which means that the other 52% of fraudulent transactions either used the exceptions from the requirements for strong authentication that apply in Europe, or were made at merchants operating outside Europe that are not required to use 3D Secure measures. 3D Secure makes card transactions in online stores more secure by requiring the cardholder to confirm their identity first by logging into their bank or using an alternative secure means such as Smart ID. Card transactions without authentication require nothing more than the card data to be entered into the online store. Transactions without authentication can also include NFC or contactless payments for small sums. Non-authenticated transactions account for only 12% of the losses from card fraud though, so even though they are more than half of the incidents of card fraud, they are relatively minor in terms of the losses they cause (see Figures 1 and 2).

Since the requirement for strong authentication was introduced in Europe in 2020, fraudsters have had to find new scams because there were a lot fewer opportunities for them to take advantage of transactions without strong authentication. This is particularly evident with card transactions, as the share of fraudulent card transactions using strong authentication has jumped sharply from 26% to 48% (see Figure 1). This shows that the measures to stop the criminals have improved, but those criminals now more often use victim manipulation and the number of frauds continues to rise even so. There is a lot of card fraud, and it occurs most often in frauds involving e-commerce. The criminals have started to find more ways of using stolen card data in recent years to get around the constraints of strong authentication (see Figures 5 and 6). The main approach is to use stolen data for card transactions in

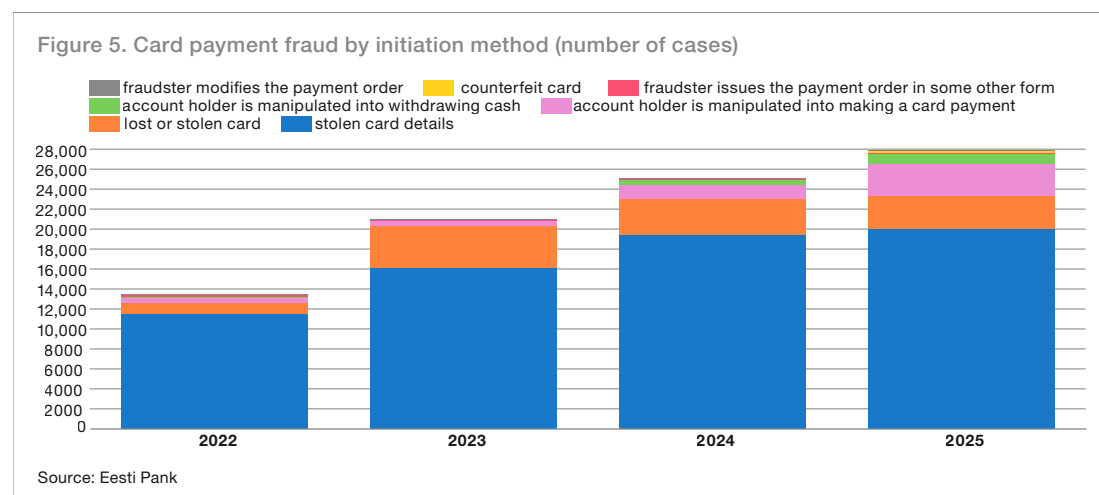
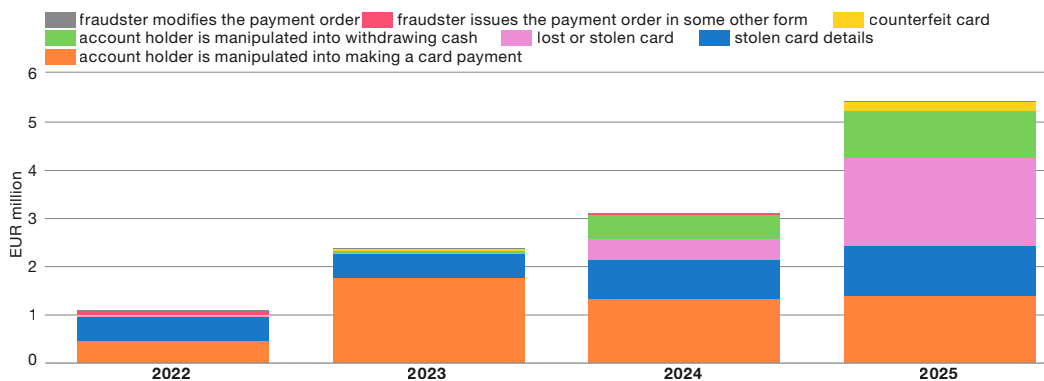


Figure 6. Value of card payment fraud by initiation method



Source: Eesti Pank

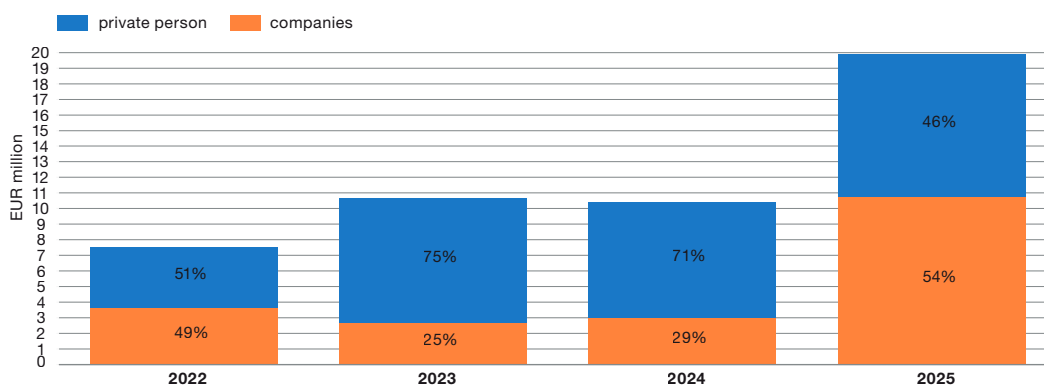
e-commerce outside Europe, and the most popular place for doing this is in online stores based in the USA. It is always wise to be cautious online, and to check the background of the online store or seller before completing any purchase. This is particularly so if the seller is offering an unusually large discount.

It is important to be very careful when shopping on the internet and to make sure about the security of the seller's site. How secure an online store is can be checked by looking out for example for the "Safe Place to Buy" trust mark issued by the Estonian E-commerce Association. It is also a good idea to do a background check on an online store, to search for reviews of it and to note how recent the positive reviews are. Whether the terms and conditions for purchases, delivery and returns and the contact details of the seller are listed on the website is also worth checking. If the goods or services are not delivered, the consumer who bought them should first of all contact the seller. It may be necessary to prove in the event of a dispute about the transaction that the seller did not agree to send the goods or return the money for them. It is worth using if possible a virtual card with a low limit or a virtual card number service that can be cancelled quickly and easily. The virtual card can be closed if the card data leak, and so the potential loss can be limited. Another common fraud using physical cards is card copying or skimming, and the banks have introduced measures to protect their ATMs and bank cards against this. Skimming is currently rare in Europe, but devices for copying card data can still be found in payment terminals outside Europe.

Frauds affecting businesses

Fraudsters have increasingly targeted businesses in recent years in order to access both personal and corporate bank accounts, as this allows them to steal more money. This is reflected in the amounts lost growing many times faster than the number of incidents. Frauds attacking businesses account

Figure 7. Losses of businesses and individuals from payment orders



Source: Eesti Pank

for only 15% of all fraudulent transactions, while 85% of frauds attack individual people. Statistics for 2025 show however that the share of total losses to fraud that was suffered by companies increased from 29% to 54%, meaning that more than half of all the money stolen was taken from businesses (see Figure 7). The largest individual losses occur through modifications to credit transfers or business email compromise. The fraudsters operate this scam by gaining access to the email accounts of business partners. As companies often make routine payments, trust builds up between partners and a message from the email account of a business partner announcing a change of bank details may not immediately appear suspicious to a company's accountants. The largest single loss in such a case in recent years was of 1.7 million euros. There is a lot of trust between cooperation partners, but it is even harder for employees to be sceptical about an instruction issued by the manager of their own company. CEO fraud generally targets employees who have the right to make payments by encouraging them to make unauthorised transfers. In a simple form of the scam, the employee receives a fake email in the name of their boss, while more complex cases might use deepfake communication and virtual meetings. The best protection against such frauds is clear internal monitoring measures within the organisation, and agreed principles for financial hygiene. Most large losses can be prevented by applying the four eyes principle for transactions that exceed a certain ceiling, and confirming significant changes through a second communications channel. A change of bank account at a major partner could for example be confirmed using contact data that have earlier been agreed by both parties.

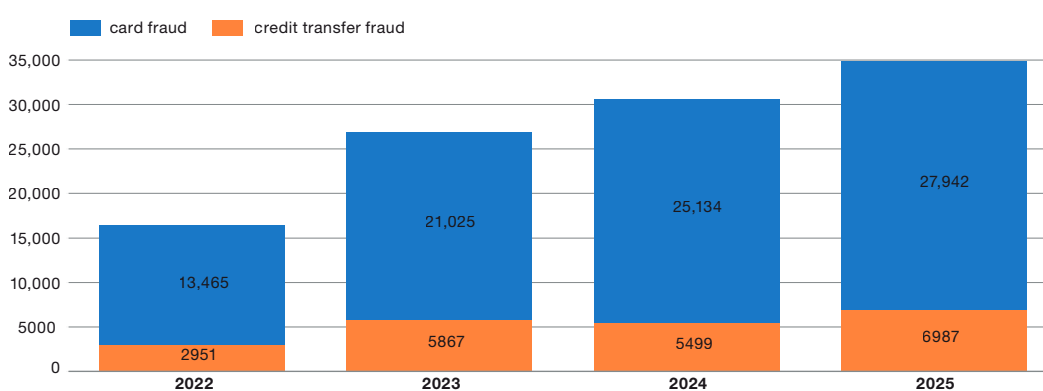
It is not only businesses that need to be cautious, but also board members of apartment associations, who have access to the money on the association's account as well as to that on their own personal accounts. A complication in this is that the fraudsters search public databases for people connected with the apartment association and attack them using standard scams like fake phone calls from couriers claiming that a registered letter has been sent to the apartment association. The criminals hope in this way to gain access to the bank account using the PIN1 confirmation of the apartment association, and from there to impersonate other officials in order to obtain the PIN-2 code. There are often large amounts on the bank accounts of apartment associations that have accumulated through contributions to a repair fund or from other fees, but the associations often do not use the same security measures as companies such as the four eyes principle when making transfers. The attacks use multi-stage telephone frauds to target private individuals with access to the accounts of legal entities, like accountants and members of management boards. Small businesses face the same problem, and the criminals are very well aware of how to take advantage of weaknesses in their security. Businesses and apartment associations should consequently review very thoroughly the security measures that they apply and consider carefully how they can best protect themselves against potential scams that could be used against them by criminals. Large or unusual payments should if possible need two people to approve and confirm them and user rights and transfer limits should be restricted to the minimum level that is actually needed. Changes to the account data of recipients of payments should always be checked using forms of contact agreed on in advance. Smart ID or Mobile ID requests should not be confirmed if it is not absolutely clear what they are for.

STATISTICS ON FRAUDS

Turnover and number of frauds

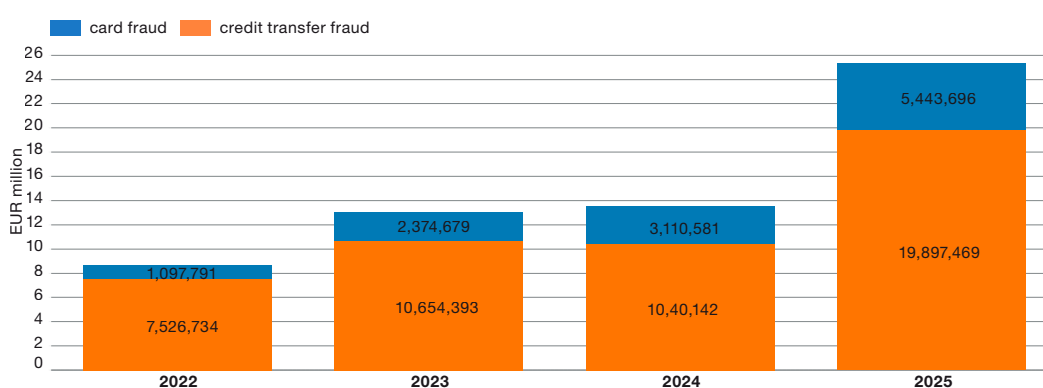
Data from Eesti Pank show steady growth over the past four years in the number of incidents of credit transfer fraud and card fraud, but of particular concern is the leap in 2025 in the amount lost to such frauds. There were 28,000 incidents of card fraud using Estonian bank cards last year, which was 11% more than in 2024, but the total amount lost to the criminals in such incidents of 5.4 million euros was 75% more than in the previous year (see Figures 8 and 9). The number of incidents of credit transfer fraud rose to 7000 in 2025, which was 27% more than in the previous year, while the amount stolen through them increased by 91% to 19.9 million euros. Data from the banks show the total losses to scams increased in 2025 to 25.3 million euros, and the number of incidents rose to 34,900 transactions. In the previous year the losses were 13.5 million euros from 30,600 transactions, meaning the losses to fraud had almost doubled.

Figure 8. Number of fraud incidents



Source: Eesti Pank

Figure 9. Value of frauds



Source: Eesti Pank

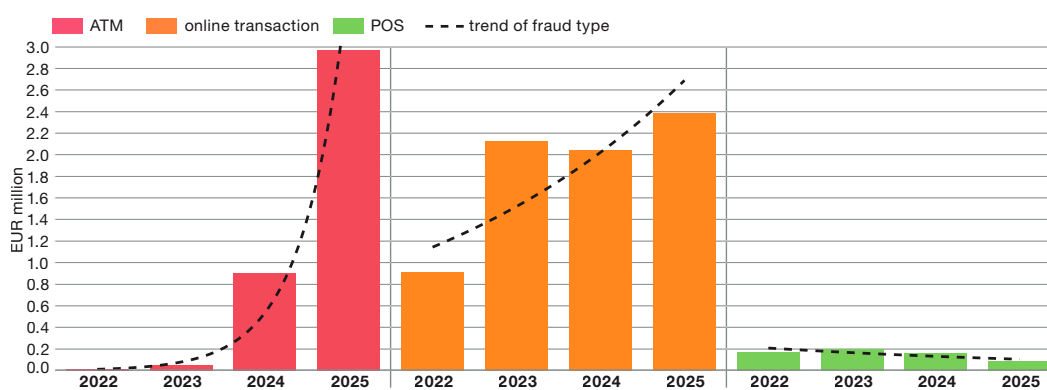
There were 526.2 million normal card transactions made in 2025 for a total value of 14.8 billion euros, while 292.3 million credit transfers were made that year with a total value of over 383 billion euros. There were 20 victims of card fraud per thousand residents of Estonia, which was two more per thousand than in the previous year. Five people per thousand residents fell victim to credit transfer fraud in 2025, which was one more than in 2024.

Types of fraud

ATM frauds were 55% of the frauds committed in 2025 using Estonian bank cards and claimed 3 million euros in losses, while 43% of incidents were online frauds totalling 2.4 million euros, and 2% were

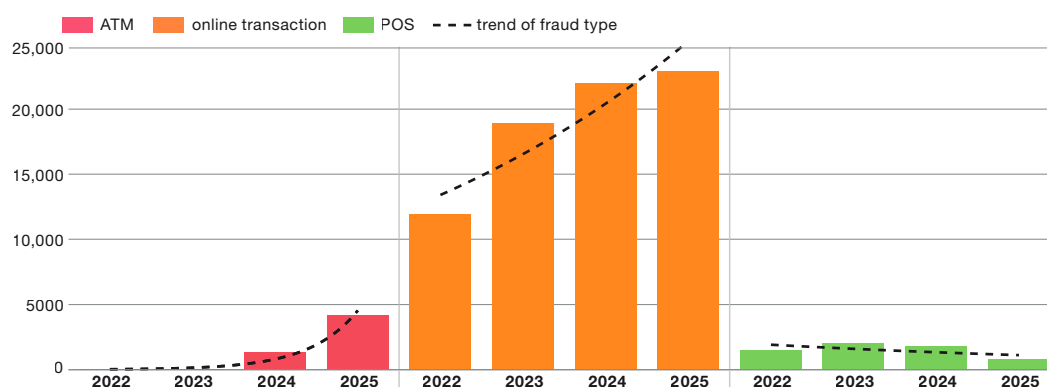
payment terminal or POS frauds with a total value of 86,000 euros (see Figure 10). The increase in losses from ATM frauds is particularly notable, as the amount lost more than tripled in 2025 and exceeded the loss from internet or e-commerce fraud. ATM frauds can be divided into three categories of frauds that use lost or stolen cards, those where the payer is manipulated into withdrawing cash, and those that use counterfeit cards (see Figures 5 and 6). Lost and stolen cards accounted for 61% or 1.8 million euros of the losses to card fraud, and came generally from people being tricked into handing over their physical card and PIN code or from cash courier scams. In these scams the victim usually hands their bank card together with the PIN code in an envelope to a cash courier or leaves it in a parcel locker as directed by the fraudster. Payers being manipulated into withdrawing cash accounted for 33% of the losses due to ATM fraud, or 960,000 euros. These scams manipulate the victim into withdrawing cash themselves and handing it over to the criminals. It may be noted that although ATM fraud accounts for the largest losses of all types of card fraud, the number of incidents of it is a fifth of the number of internet-based frauds. This illustrates that the amount lost in each incident of ATM fraud is very large (see Figure 11).

Figure 10. Value of card fraud by type of transaction



Source: Eesti Pank

Figure 11. Number of card fraud incidents by type of transaction

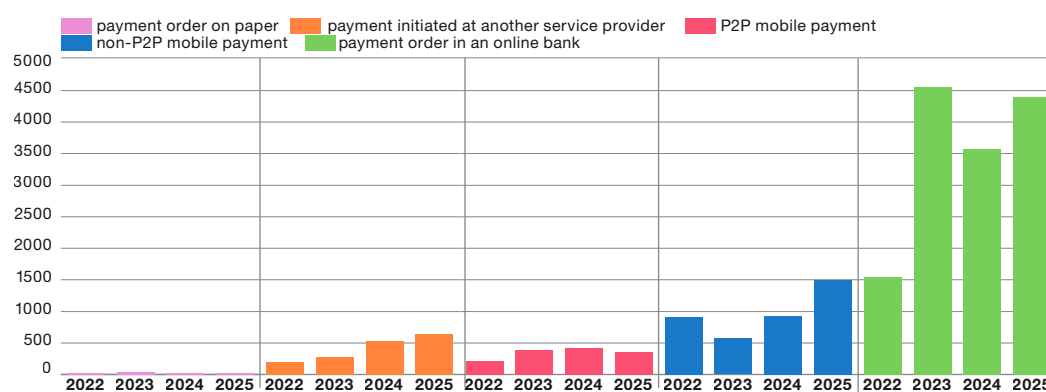


Source: Eesti Pank

Online scams have been the main source of losses to bank card fraud over the years. The two main forms they take are manipulation of a payer in a card payment, and theft of card data. Of the total losses to such online frauds in 2025, 1.36 million euros or 57% came from payer manipulation and 1 million euros or 42% from card data theft, making a total loss of 2.4 million euros (see Figure 10). There are various different scams that manipulate people into making card payments by encouraging them to make purchases from fake online stores offering large discounts, or to buy products that are paid for but then never delivered. Theft of card data occurs when people's card data are leaked or stolen and the criminal uses them later for making payments. There were almost 23,000 incidents of this type of fraud in 2025 (see Figure 11).

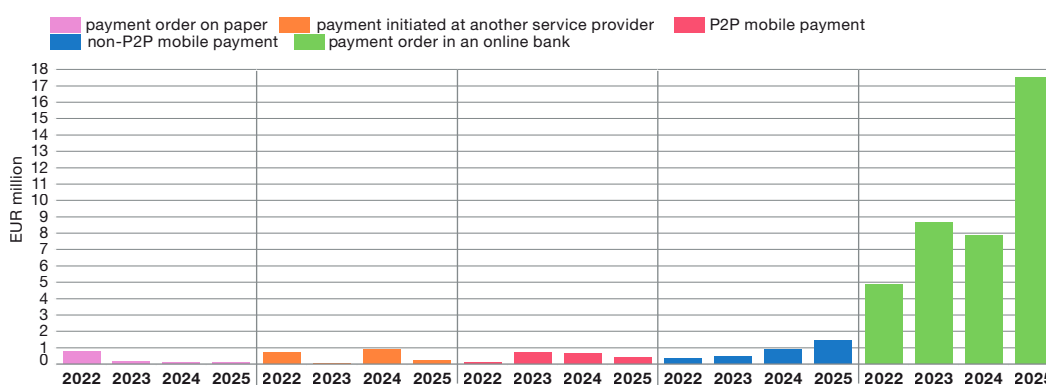
Credit transfers made from an internet bank were 89% of credit transfer frauds and they accounted for 17.5 million euros of the value of credit transfer frauds in 2025 (see Figures 12 and 13). Other credit transfers initiated from a mobile other than P2P were 7% of credit transfer frauds at a value of 1.4 million euros. The other 4% of such frauds were P2P mobile payments, credit transfers submitted on paper, and payments initiated at other service providers. The most common form of credit transfer fraud by the number of incidents and their value is manipulation of the victim, where the victims themselves hand the money over to the fraudsters (see Figures 3 and 4).

Figure 12. Number of credit transfer fraud incidents by type of transaction



Source: Eesti Pank

Figure 13. Value of credit transfer fraud by type of transaction



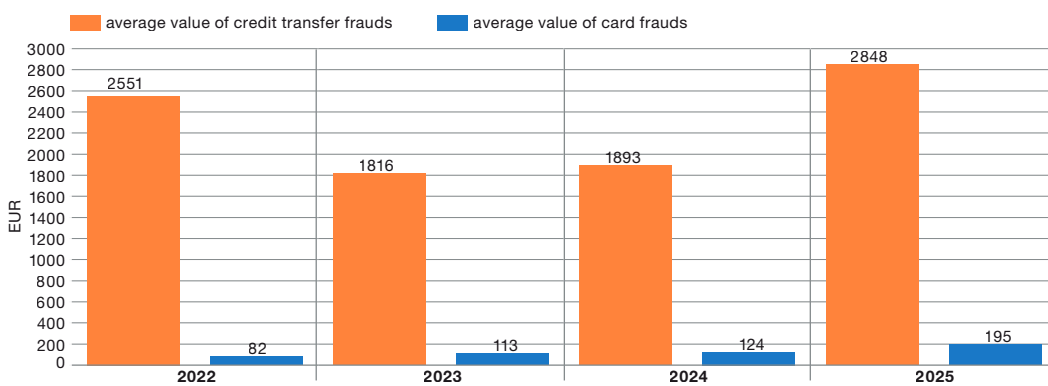
Source: Eesti Pank

There are many different types of scam and the fraudsters often try to approach their victims through different channels using email and messaging apps, social media, computer viruses, purchases or sales of second hand goods, and simple real-world means like cash couriers. Some scams use specialised software that is adapted so that the victim's telephone shows them a faked bank website or other log on page. The development and spread of large language models (LLMs) should also be noted as a tool that makes it easier for organised criminals to set up temporary websites that imitate those of banks or other institutions like telecommunications companies. Once a victim has been tricked by a telephone call into entering their PIN code in a site that looks like the website of their own bank, the criminal can see the code in real time and can send a new screen to the victim's telephone asking for additional information. It remains particularly important to be careful when shopping in foreign online stores to avoid visiting fake websites made by scammers, or handing over money to unknown people or companies. The criminals are skilled at taking advantage of people's ignorance, applying psychological pressure and using convincing fakes and phishing, so they can trick their victims into making transactions or revealing sensitive data. Contact with the victim is however only a small part of the entire fraud process in the larger view. It is often preceded by thorough preparations and after the fraud has been committed, the criminals then need to use money mules to move the stolen money onwards.

Average losses to frauds

The average amount lost in each incident of card fraud was 195 euros in 2025, and in 2024 it was 124 euros. The average amount lost to credit transfer fraud also rose from 1893 euros in 2024 to 2848 euros in 2025 (see Figure 14). The average loss from credit transfer fraud is calculated from the total losses of individuals, businesses, and other associations and funds. The average loss of private individuals alone was 1570 euros. It may be noted that the average amount of the usual credit transfers of private individuals is 160 euros, meaning the amounts involved in credit transfer frauds are about ten times larger than typical credit transfers. This difference can partly be explained by investment frauds, which frequently involve larger sums. The value of the average usual card transaction is 28 euros, and the average loss in a card fraud incident is about seven times that. The average amount lost to card fraud is affected by the larger amounts involved in e-commerce frauds and cash withdrawal scams.

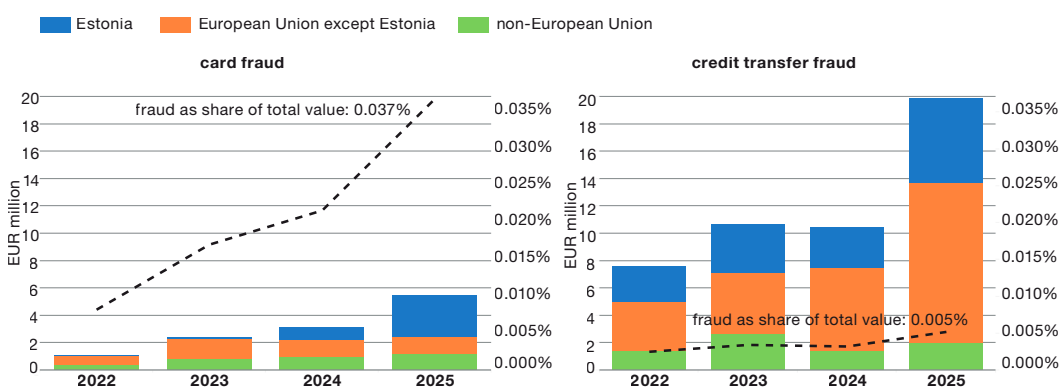
Figure 14. Average value of card payment and credit transfer fraud incidents



Source: Eesti Pank

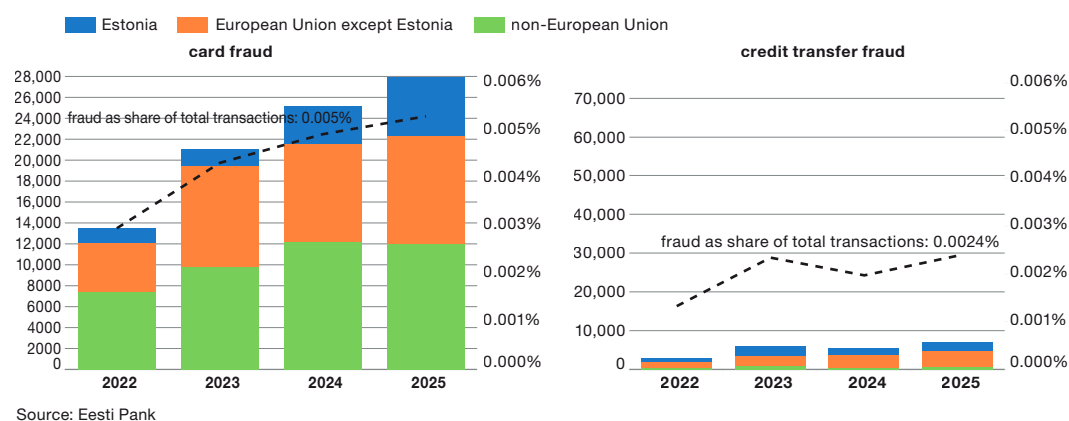
The amount stolen by fraudsters on average rounds to four euro cents for every 100 euros of the total turnover of all card transactions, or 0.037%, and half a euro cent for every 100 euros of all credit transfers, or 0.005%. Stable growth in frauds as a share of both the total turnover and number of normal transactions is particularly evident with card frauds (see Figures 15 and 16). Where there were three fraudulent card transactions per 100,000 transactions in 2022, this had risen to five frauds or 0.005% in 2025. Particularly noticeable is the increase in 2025 in card frauds as a share of total value, which was almost twice the level of 0.022% recorded in 2024. The share of credit transfers that are fraudulent has remained stable, as there are on average two frauds per 100,000 credit transfers, or 0.002% (see Figure 16). This may have been affected by increased awareness among the Estonian population, and the positive trend that people are informing their financial institutions about both attempted frauds and

Figure 15. Fraud as share of total value



Source: Eesti Pank

Figure 16. Fraudulent transactions as a share of total transactions



successful ones. There was though a sharp increase in 2025 in the losses caused by credit transfer fraud to both businesses and individuals. The number of fraudulent transactions increased much more slowly than the amount lost, indicating that the losses in each incident have grown significantly.

It is the user of payment services, meaning the customer, who bears the losses from incidents of credit transfer fraud in 96% of cases (see Figure 17). The main reason for this is that customers are committing gross negligence when they authenticate fraudulent transfers that transfer their money directly to the fraudster or when they hand over confidential data that allow the criminals to make authenticated transfers from their bank account. The requirements of the payment services directive 2 (PSD2) for the banks to compensate losses to clients do not apply in cases of gross negligence. Customers bear the losses in 84% of incidents of card fraud (see Figure 18). The losses are borne in 10% of cases by another

Figure 17. Bearer of losses to credit transfer fraud

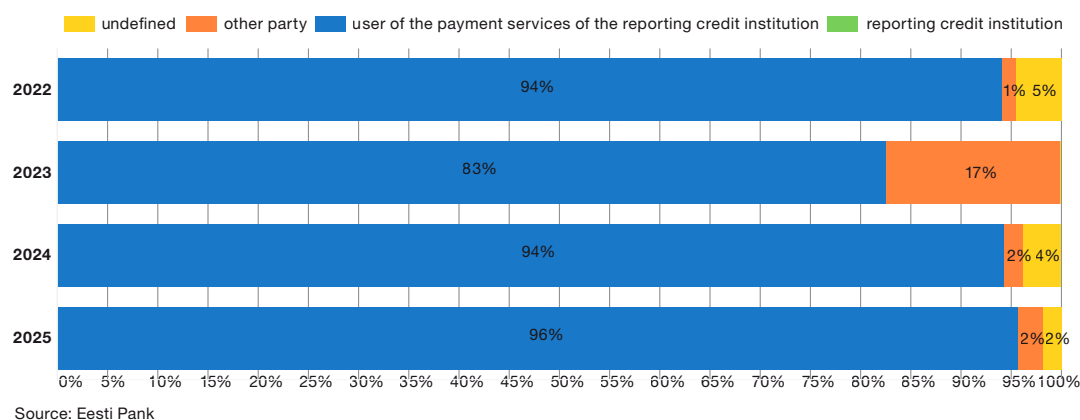
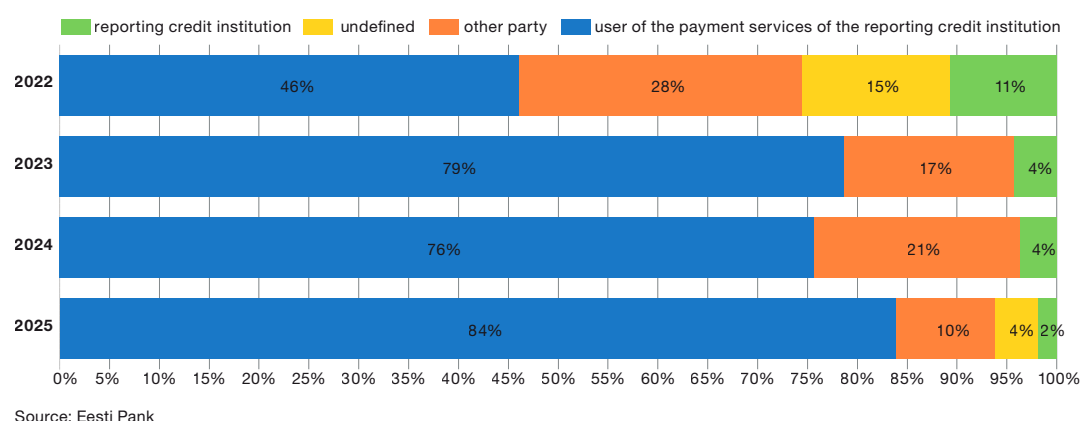


Figure 18. Bearer of losses to card fraud



responsible party such as a merchant or an acquirer, who receives the payment and who the merchant has signed a payment solution service contract with. It is not defined in the remaining 6% of cases who bears the losses, or else it is the customer's bank that does so. When a bank bears the loss, it compensates the customer for the amount taken in the fraud. The banks assess with card fraud whether the client has been grossly negligent and whether the merchant has met all of the security requirements such as using 3D Secure. If the transaction has not been strongly authenticated as required, then the merchant is responsible for the loss from the fraudulent transaction.

Secure shopping online under the official name of 3D Secure provides another layer of security by using additional authentication to identify the card holder and so prevent fraudulent card transactions being made in online stores.

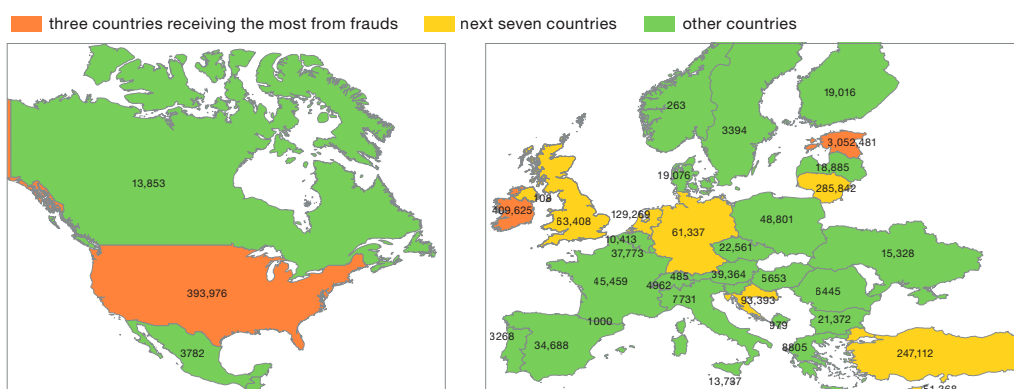
FRAUDS BY REGION

Card fraud with Estonian bank cards

The frauds using Estonian bank cards can be divided into three groups of those committed in Estonia, those elsewhere in Europe, and those outside Europe. The distribution across those regions is shown in Figures 15 and 16. More than half of the total losses in 2025 at 56% came from card frauds committed in Estonia, while 23% of total losses came from frauds elsewhere in Europe and 21% from frauds outside Europe. The statistical picture across regions by the number of frauds committed is quite different. Some 12,000 fraudulent card transactions, or 43% of all those made with Estonian bank cards, were committed outside Europe. The region with the smallest share of all the frauds was Estonia, where 5600 card frauds were committed in 2025, or 20% of the total. There were 10,300 frauds committed elsewhere in Europe meanwhile, or 36%. The requirements for strong authentication are not always applied to card transactions outside Europe, meaning that the risk of fraud with such transactions is highest there.

The countries where the largest losses to fraud with bank cards issued in Estonia occurred were the United States of America, Ireland and Estonia (see Figure 19), and those countries also saw the largest number of fraudulent transactions. The statistics in the report on fraud issued by the European Central Bank and the European Banking Authority show though that there were a third as many card frauds in 2024 using bank cards from Estonia as there were with bank cards issued by other European countries (ECB, 2025).

Figure 19. Estonian card fraud losses by country (EUR)

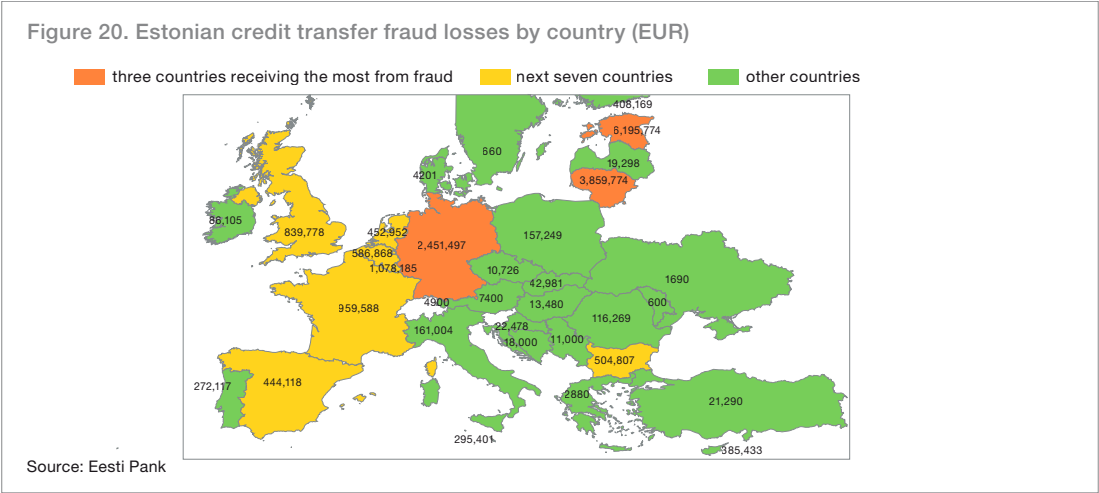


Source: Eesti Pank

Credit transfer frauds with Estonian bank accounts

Fraudulent credit transfers from one Estonian bank account to another Estonian account accounted for 31% of the value of frauds and 30% of the number of them (see Figures 15 and 16). The majority of

fraudulent transfers went to other countries in Europe, as 59% of the value and 62% of the individual payments went there. The initial transfer went to an account outside Europe in 8% of cases, accounting for 10% of the value of the frauds. The country in which bank accounts received the largest amount of money taken from the accounts of victims was Estonia, with Lithuania in second and Germany third (see Figure 20). The same three countries were the three leaders for the number of frauds committed. The data show that the money mules have sent the money received from frauds to bank accounts across the whole of Europe. Banks are better able to know their clients if they take additional measures to counter fraudsters and so help prevent the losses that arise from credit transfer fraud. There is an increasing trend though for both legal entities and private individuals in Estonia to prefer to make settlements through European payment institutions, and so it is no longer a risk indicator if an account sends money only to other accounts outside of Estonia. The report from the European Central Bank and the European Banking Authority finds that credit transfer fraud in Estonia as a share of all transfers is around the average level in Europe.



COUNTERING PAYMENT FRAUD IN ESTONIA

The number of attempts at fraud is incredibly large, but the majority of them do not connect with a victim, as service providers have taken powerful steps to block fraudsters. In the first five months of 2026 alone, Telia blocked over 20 million threats, the majority of which were phishing websites or sites with a bad reputation. There was a steep drop from the start of the year in the number of scam calls made to the Telia network, as Telia identified and blocked over two million attempted scam calls in January, but only 223,000 in April. Similar measures have been applied by Elisa and Tele 2. Elisa blocked over six million attempted scam calls in the first half of the year, and its statistics also show a fall in the number of attempted calls. Tele2 reports that scam calls are being directed more at businesses, which lose larger amounts. Technological measures cannot block all scam calls despite these efforts though. A single scam call made successfully from a forged or spoofed number is sufficient, and the losses that result for an individual or a business can be extremely large.

Criminals that use spoofing employ technical means so that the telephone screen of the person receiving the call shows a number that appears to be an Estonian one. This makes it more likely that the person will accept the call and will trust the fraudster on the end of it. In many cases the owner of the number is not even aware that their number has been spoofed.

The banks have been using various high quality security solutions for years by now, and various measures are used to reduce **POS and ATM fraud**:

- Chip technology that meets EMV standards and saves data securely and generates a one-time transaction code, making it harder to clone or skim the card.
- Sensors installed in ATMs that help to detect skimming devices.
- Geoblocking that prevents the card being used in areas with low levels of security.
- Liability shifting to protect merchants that moves the responsibility for fraudulent transactions from the merchant to the card issuer or other participant in the payment chain if the merchant has correctly used EMV technology and 3D Secure to protect customers.

Measures taken to reduce **internet-based fraud** including fraudulent credit transfers:

- Secure online shopping, or 3D Secure. This plays a major part in preventing online frauds, as the shopper is generally required to show additional personal identification when they confirm their purchase. This is usually done by redirecting them to the authentication site of their internet bank, where the transaction is confirmed using Smart ID, Mobile ID or some other means of authentication.
- Tokenisation, where the sensitive card data like the card number are substituted for a digital symbol or token.
- Verification of payee, which checks that the name and account number of the payee match when payments are made.
- Constant monitoring of transactions by the banks that uses client-based risk scores and behaviour patterns among other techniques.
- Updating and development of the technological monitoring systems of the banks.
- Additional levels of authentication for accessing client accounts, and warnings when new devices and IP addresses are identified.
- Restrictions on devices in certain cases, such as not allowing transactions while a telephone call is in progress, or limits on high-risk transactions.

The police are also working actively to tackle fraud. The police identify and block the bank accounts and telephone numbers of fraudsters to make their lives more difficult, and are working constantly to raise public awareness. This makes it harder for the criminals to succeed in manipulating their victims.

Roundtable for countering financial fraud

Eesti Pank set up a roundtable for tackling financial fraud in 2025 that brings together institutions from both the public and private sectors. The main aim of the roundtable is to collect all the parties involved in a single information space and compile and apply an action plan for tackling fraud, to propose any legislative amendments that may be needed for it, and more. The Ministry of Finance is responsible for the action plan, and the meetings of the roundtable are coordinated by Eesti Pank. Efforts to counter fraud fall under the purview of the [Ministry of Finance](#), the [Ministry of Justice and Digital Affairs](#), the [Ministry of Economic Affairs and Communications](#) and the [Ministry of the Interior](#), and other institutions and organisations including the [Police and Border Guard Board](#), the [Estonian Banking Association](#), [Eesti Pank](#), the [Consumer Protection and Technical Regulatory Authority](#), the [Prosecutor's Office](#), the [Information System Authority](#), and [Finantsinspeksioon](#). The private sector is also involved in the work of the roundtable, particularly banks, telecommunications companies and technology companies including [SALV](#) and [SK ID Solutions](#), and payment intermediaries and crypto companies.

The roundtable managed by Eesti Pank has created forms for cooperation to tackle fraud at the Police and Border Guard Board and the Estonian Banking Association. The different formats for cooperation have different focuses. The aim is to avoid duplicating activities and to set clear strategic targets for the division of work and for the effective execution of activities.

The main activities involved and the results of executing the action plan of the roundtable, and the activities initiated by participants in it.

Legislative changes

- A draft act for combating financial fraud reached the Riigikogu in summer 2026 and would give providers of payment services the legal right to refuse to accept payment orders if they have grounds to suspect fraud. The banks would also have the right to share data with other credit institutions and the police if there is a suspicion that a client or a payment transaction is affected by fraud. This is a very important legislative change, as gaps in information exchange have so far been very beneficial to the fraudsters. It is also important that the banks get the right to halt client payment transactions if they suspect that the client is making the payment having been manipulated by a fraudster. The draft would also amend the Creditors and Credit Intermediaries Act to prevent criminals taking loans in the name of the victim.
- The European Union reached a political agreement in November 2024 on a new payment services package of legislation, with a new payment services regulation and directive. The Payment Services Regulation (PSR) has a central place among the measures to tackle fraud. The new regulation and directive will replace the second payment services directive (PSD2) that is currently in force. The new regulation contains multiple measures for combating fraud, such as requiring payment service providers to block payments that are suspected of being fraudulent, and to share information about frauds between themselves and with the police. The draft act to tackle financial fraud gives similar rights to providers of payment services, but the new payment services package would also make the payment service provider liable for the losses to fraud suffered by clients in certain circumstances, even when it is the client themselves that has confirmed the payment. This would require the payment service provider to compensate people for the amount they had lost because of the fraud. It is expected that the regulation will start to apply at the end of 2028.
- The national regulation on the provision of communication services is being amended. The amendments are designed to require providers of communications services to employ measures

to block scam calls. The larger telecommunications companies already use such measures and have invested in stopping scam calls, blocking millions of them each month in anticipation of the regulatory obligation to do so. The obligation to apply such measures will be extended to smaller telecommunications companies as well when the regulation comes into force, which will be at the start of 2027.

- Transactions with crypto assets will start to be regulated more strictly by the European Union's new Payment Services Regulation.

The work of the banks

- The banks have made substantial investments in systems and security measures for preventing fraud. The banks believe that the draft act on preventing financial fraud will provide the best tools for countering scams and fraud. They have put together a description of best practice in combating fraud and a programme of measures. The aim of setting out best practice is to:
 1. describe the shared values, approaches and principles that the banks work with when countering fraud;
 2. raise awareness at the banks and among the public about the risks of fraud and measures that can be taken against it;
 3. promote effective cooperation in tackling fraud in the banking sector and between various sectors including the public sector, while respecting the autonomy of each bank in choosing and applying specific measures.

The programme of measures for 2026 includes a review of limits on cash withdrawals and transactions, and the introduction of Smart ID+. It also raises awareness among businesses of the four eyes principle to encourage them to apply it more broadly when making payments.

The best practice and the measures of the Estonian Banking Association can be found [on its website](#).

It is important to stress that although banks are often first to be looked at together with people and businesses when fraud is discussed, the banks are not the only ones responsible for preventing frauds involving payments. The responsibility is shared between customers, the banks, state institutions, technology companies, communications operators, and other service providers. Scams have often started before any payment is made and outside the bank, as people are contacted by telephone, social media or email, or through a fake website. The banks apply all the measures required by law for preventing financial fraud and to protect their clients, but people themselves have a vital role to play in preventing fraud by being attentive and cautious. The banks have stated that they are currently unable to block more than half of attempted frauds.

Information campaigns

- The police work every day on spreading information and compile statistics on individual fraud cases, and they have produced guidelines that are published on the police website on how people can protect themselves against scammers.
- The Ministry of Finance is working with a partner that won a procurement on running an information campaign about stopping financial fraud that started in summer 2026 and will last for 18 months. The campaign will try to reach as many people as possible in Estonia, including those who do not pay attention to the mainstream media. Outdoor billboard advertising and social media will be used among other channels.
- The state communication strategy on preventing financial fraud was recently completed and its main aim is to make people more confident in their ability to recognise scams and to resist them. The strategy gives guidelines for how to shape messaging so that it does not create excessive anxiety or undermine a reasonable sense of caution. The messaging and the activities of the state, and also of partners in the private sector, should help reduce the sense of shame that

victims feel when they are scammed, support a sense of caution within society, and set out practical ways for people to act when faced with a scam. The main state institutions involved in preventing and tackling fraud are the Ministry of Finance, the Ministry of Justice and Digital Affairs, the Ministry of the Interior, the Police and Border Guard Board, the Information System Authority, the Consumer Protection and Technical Regulatory Authority, the Prosecutor's Office, and Eesti Pank.

- The Information System Authority is preparing its own campaign, which it has further details about [on its website](#).
- The Estonian Banking Association and the telecommunications companies are also working constantly on campaigns to warn about scams, and information about this can be found on the website of the Estonian Banking Association.

The Estonian Banking Association has set up a separate operation for combating fraud. It also started a fraud prevention campaign in 2025 titled *Scammers have many faces*, which was partly financed by the communications companies Telia, Elisa and Tele2. The wide-ranging advertising campaign was designed to make people more aware of scams and frauds. Victims have different levels of education, incomes and ages and can be found all across Estonia, and the campaign promoted the following messages:

- Make sure who you are talking to and who you are sharing information with.
- Don't let yourself be put under pressure or rushed.
- Concentrate! Don't just absent-mindedly click on a link.
- The call seems suspicious? Hang up. You don't have to give any reason for doing so.
- Make sure that you know what you are signing with your PIN code.
- Keep your personal data to yourself.
- Don't hesitate to ask somebody else's opinion.
- If you spot a scam, call the police.
- If you have been scammed, inform your bank and the police.

The Estonian Banking Association is continuing to run various information campaigns in 2026, joining forces to do so with the Ministry of Finance and the Police and Border Guard Board.

The wider use of the Malware Information Sharing Platform (MISP) set up by the Information System Authority should also be noted. The platform can now also be accessed by telecommunications companies, allowing information on the websites of fraudsters to be shared more quickly and access to them to be blocked.

Information about adverts on Facebook for fake investment schemes and other scams and the websites they link to can be passed on to the Consumer Protection and Technical Regulatory Authority, which then works to take them down.

SK ID Solutions has made a change so that Smart ID cannot be accessed by a device that is in a different location. Smart ID+ has also been developed and is now available for the banks and other providers of e-services to use. Smart ID+ connects authentication more securely with transactions initiated by the user.

The SALV Bridge platform is important for the rapid exchange of information between banks, as it allows them and other financial institutions to exchange information about suspicious transactions and accounts. This allows rapid confirmation of whether a fraud also affects other financial institutions.

These measures cover only some of the participants, actions and measures involved in the fight against fraud. Eesti Pank and the Ministry of Finance have set a target of maintaining a constant focus at the state level on fighting financial fraud and of supporting all parties that want to work together to tackle the problem.

Individuals as the first line of defence against fraud – how you can help stop scams

All these measures are effective, but the key element in stopping fraud is still you as the individual person. Most payment fraud and card fraud can be prevented if you make sure first of all who you are

making a payment to and where you are entering your data. If at all possible, you should always use strong two-factor authentication. Remember that you must never share your PIN codes, passwords and other sensitive data with anybody. This applies even when you are talking with bank staff, police officers or other official people, as a real official would never ask you for such data. If you receive a phone call, email or message saying that your bank account is in danger, then you should stop the conversation immediately and call the official telephone number of your bank, which you can find on your bank's website. A big red flag is any request to download an app that allows remote access to your computer such as TeamViewer or AnyDesk, as these can give the fraudsters complete control over your computer. You should also be very cautious if somebody is pressing you to complete a transaction quickly, as rushing can distract your attention and make you miss suspicious signs. Rushing also mean that you have no time to ask anybody else for advice or help.

Remember when shopping online or speaking on the telephone that if an offer of a product or service seems too good to be true, then it almost certainly is. Typical examples are massive discounts or a promise of outsized returns on an investment. Check carefully before entering data into a website whether the address of the site begins <https://> and whether it contains the correct name of the service provider without any spelling mistakes or unknown symbols. If you get a phone call from an unknown number, especially a foreign one, you do not need to answer it, and you should look on the internet to see whether warnings have previously been given about that number. It is generally not worth answering phone calls from foreign countries if you do not know anybody who lives there, as it is very probable that the caller is a scammer.

If you suspect that you have fallen victim to a scam, you must act straight away. Close your card or your account, save any evidence such as SMSs or screenshots, and inform your bank and the police. Acting quickly makes it more likely that you will get your money back and the scammers will get caught. If you think you might be talking to a scammer and not an official employee, you should call the official number of the bank, the police, the delivery firm or other institution to ask for advice. This can help you avoid the most common scams and reduce the risk of your personal data falling into the hands of criminals and of you losing your money.

The public messages from Eesti Pank about avoiding scams and frauds are:

- If you are contacted about a financial matter, do not react immediately. Take your time and consider whether this might be a scam.
- Remember that banks and officials will never ask you to give them your PIN code or share your screen, and will not contact you using WhatsApp or Viber.
- Do not open suspicious links or files sent to you by SMS or email.
- Do not give your bank card, PIN codes or cash to strangers, even if they claim to be a courier or an official.
- If you are told that your account is in danger, hang up immediately and call the bank or the police yourself to confirm the information.
- Only enter your PIN code when you have initiated a transaction yourself and know exactly what it is that you are confirming. Be especially careful with calls that say you have a delivery from a courier, offer to change your electricity or water meter, or invite you to the healthcare centre, as such calls often try to trick people into entering their PIN codes.
- If somebody calls you and asks you to enter your PIN code, it is always a scam.