DANMARKS NATIONALBANK

DIGITALISERING

ANALYSIS | Payments
29 April 2024 | No. 7

Digital payment fraud in Denmark

Written by

Marcus Clausen Brock
Senior Retail Payments Economist

mcb@nationalbanken.dk
+45 3363 6072

Time to read

22 pages

Digital payment has become widespread, creating new opportunities for criminals to commit fraud. This is also the case in Denmark, which is one of the most digitalised countries in the world when it comes to payments. Danish payment systems are secure and difficult to defraud. Consequently, fraudsters and scammers are increasingly using methods that trick the public and company employees to make and authorise fraudulent payments.

Payment card fraud of Danish payment cards is at a low but increasing level

Payments card fraud had been declining for a number of years, but has increased in the last few years. The increase is partly due to the fact that fraudsters and scammers have found new ways to acquire payment cards. Compared to Europe, payment card fraud in Denmark is low.

Most payment card fraud occurs in foreign e-commerce and increasingly outside of Europe

New security measures and European requirements for two-factor authentication may have contributed to the increase in payment card fraud outside Europe. Wider use of card blocking in geographical areas or payment situations is deemed to be able to limit fraud of Danish payment cards in foreign e-commerce.

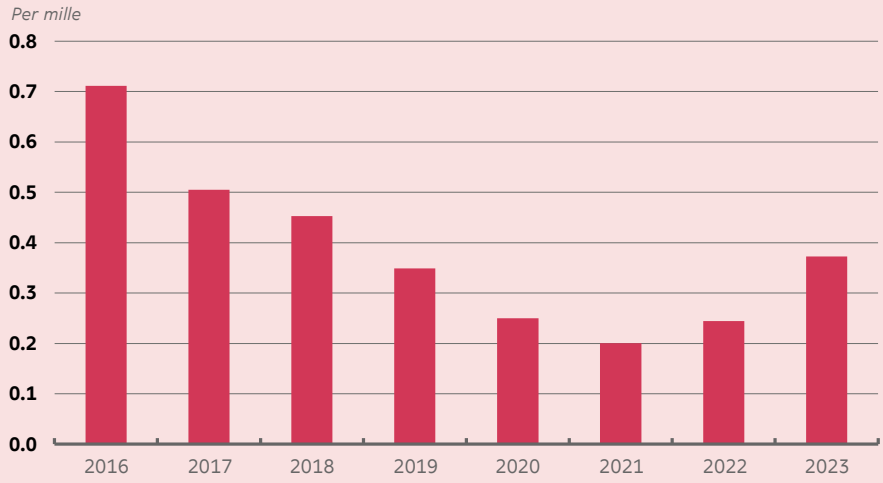
Credit transfer fraud occurs mainly in cases where private citizens transfer money to the fraudster or scammer themselves

Accountholders (the public and company employees) must be aware that they are increasingly at risk of being tricked into authorising fraudulent payments themselves. When accountholders have authorised the payments themselves, they or their employer will be liable for the financial loss in most cases.

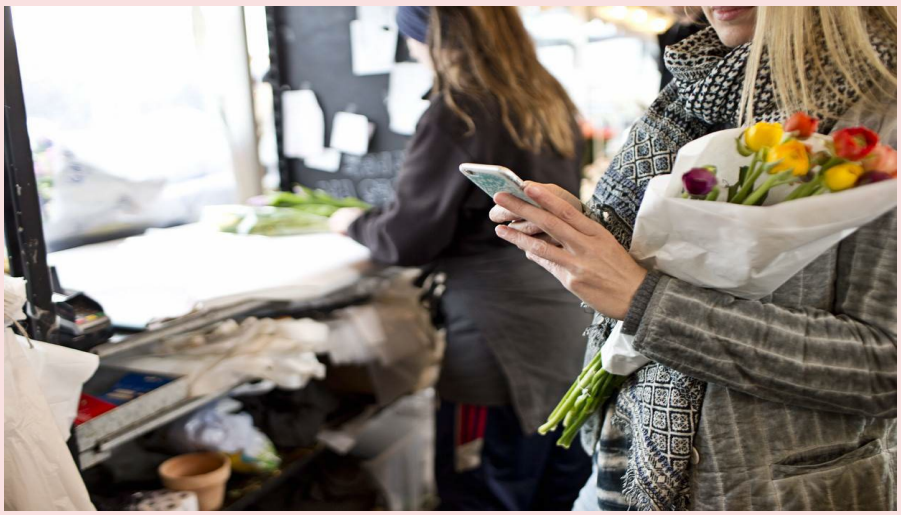
Why is it important?

One of Danmarks Nationalbank's main tasks is to secure safe and efficient payments in Denmark. Fraud can affect anyone in the population and as the use of new digital payment solutions is on the rise, ways for criminals to conduct digital fraud are also increasing. It is therefore important that the public and companies are aware of how they are at risk of being exposed to digital fraud, so they can continue to trust that their payments can be made securely.

Main chart: Payment card fraud is at a low but increasing level



Note: Total Danish-issued payment card fraud in relation to total card turnover.
Source: Danmarks Nationalbank.



Keywords

Payments

Digitalisation

Financial regulation

Statistics

01
Introduction

Digital payment solutions are used for over 92 per cent of the total value of all citizens payments in Denmark. This is largely due to the preference for digital payment solutions and the ongoing digitalisation of Danish society.[1] The digital payments infrastructure is secure and efficient, and digitalisation has made it faster and easier for most people to make payments.

However, the increased use of digital payment solutions also means that the public and businesses are more exposed to digital fraud. In 2023, digital payment fraud in Denmark totalled approximately kr. 627 million. Almost half of this figure related to payment card fraud, where cards were used without the cardholders' authorisation primarily on foreign websites, through payment to a fake online store for example. Bank account transfer fraud, also known as credit transfer scam, has increased in recent years and was on a par with payment card fraud in 2023. In contrast, the number of in-person robberies has more than halved over the last 10 years and no bank robberies were recorded in Denmark in 2022 or 2023.[2] These figures emphasise that criminals have largely gone digital and are following the evolution of society.

New technologies, security measures and European rules for two-factor authentication of digital payments have made it difficult for criminals to make digital payments and credit transfers from online banks without requiring authorisation from the account holder. Digital payment fraud is therefore increasing as criminals succeed in tricking account holders to pay or transfer money to them.

Trends in fraud patterns show that criminals have continuously adapted their methods to new technologies and regulations. It is therefore important that the public and companies in a digital society are aware that they are increasingly at risk of being tricked into authorising fraudulent payments.

In addition to scams that trick cardholders into making payments, digital payments also carry the risk of unauthorised use of payment details to make payments without the cardholder's authorisation. This happens, for example, in the case of payment card fraud, where criminals manage to obtain a payment card and the associated PIN.

In this analysis, *scams* are defined as cases where scammers succeed in deceiving and tricking the account holder into making payments or credit transfers to the criminals themselves. Payment solution *fraud* is defined as the fraudster's use of payment solutions without the direct involvement of the victim.

This is the first time that Danmarks Nationalbank has been able to analyse trends in fraud and scams with both payment cards and credit transfers. This is due to new data on credit transfers.[3] In addition quarterly data from Danmarks Nationalbank on payment card fraud were used.

[1] See Danmarks Nationalbank, The role of cash in a society with low usage of cash, *Danmarks Nationalbank Analysis*, no. 21, November 2023 (*link*).
[2] See Statistics Denmark, *Kriminalitet 2022*, December 2023 (*link*) (in Danish only), and Finance Denmark, *Et år uden bankrøverier – for andet år i træk*, January 2024 (*link*) (in Danish only).
[3] Data on credit transfer fraud and scams are based on reporting by banks to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2*, see appended table. The Danish Financial Supervisory Authority has also contributed valuable comments to the analysis.

02

Payment card fraud is at a low but increasing level

When Danish cardholders buy goods and services in a store or online, they increasingly use digital payment solutions such as payment cards and mobile phones. Paying with a payment card is safe and easy, but sometimes fraudsters manage to make payments without the cardholder's authorisation. This could be because the cardholder's payment card has been stolen after the fraudster has copied the PIN, for example, or because the fraudster has obtained the card details by stealing them from the cardholder via a payment link in a text message or through payment to a fake online store, for example.

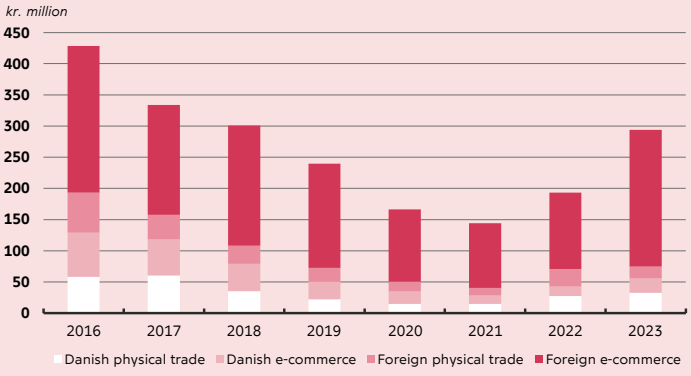
The total recorded fraud of payment cards issued by Danish banks in 2023 was approximately kr. 294 million, see chart 1.[4] Payment card fraud was spread over approximately 232,000 fraud-related card payments. This gives an average fraud value per payment of just under kr. 1,300. Total fraud value should be seen in the context of the fact that total card turnover in 2023 was approximately kr. 800 billion. This means that payment card fraud averaged kr. 369 per million kroner spent.

Payment card fraud has been declining for a number of years. This is largely due to new security measures and new European payment authorisation rules, see box 1. In addition, 2020 and 2021 saw widespread lockdowns due to the

CHART 1

Payment card fraud has increased in recent years

Total value of payment card fraud in physical trade and online

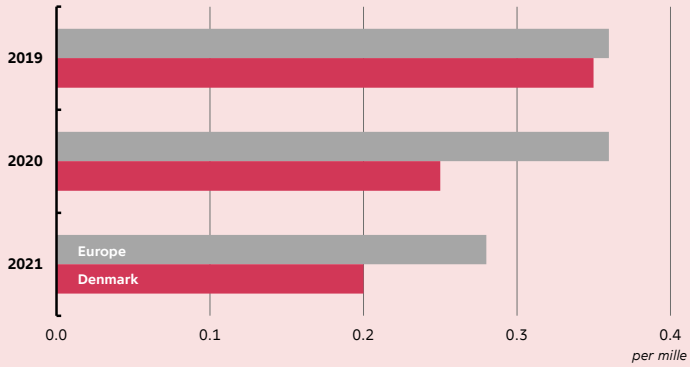


Note: Fraud with Danish-issued payment cards. Physical trade also includes payment card fraud at ATMs.
Source: Danmarks Nationalbank.

CHART 2

Payment card fraud is lower in Denmark compared to the rest of Europe

Total payment card fraud in relation to total card turnover



Note: Data for Europe are only available up to and including 2021. Europe includes the SEPA area, which consists of all EU and EEA countries, Andorra, Monaco, San Marino, Switzerland, the UK and Vatican City.
Source: Danmarks Nationalbank and the European Central Bank (*link*).

[4] Danish-issued payment cards are typically Dankort, Mastercard and Visa cards issued by Danish banks.

coronavirus pandemic, making it difficult for fraudsters to copy PINs and steal physical payment cards. But payment card fraud has increased since 2021, which may be due to increased shopping on foreign websites and fraudsters finding new ways to gain access to payment cards.

In an international context, relative payment card fraud is lower in Denmark than in the rest of Europe. In 2021, when payment card fraud was last calculated across Europe, the Danish fraud rate was 0.20 per cent, while the European average was 0.26 per cent, see chart 2. However, relative card fraud has increased in Denmark since 2021. A similar trend has been observed in Sweden.[5]

BOX 1

European payment authorisation rules

Since January 2021, all digital payments in Europe, including payments with payment cards and mobile payments, have had to be authorised using at least two different factors – 'two-factor authentication'. This applies to physical trade, where the rules came into force on 1 January 2018, and to online payments from 1 January 2021.

The two factors must either be something only the payer knows (e.g. a PIN); something only the payer is (e.g. facial authentication); or something only the payer has (e.g. payment card or mobile phone).

The payment service provider, typically the payer's bank, has the option of exempting certain transactions from two-factor authentication where the risk of fraud is deemed low. For example, contactless payments in physical stores up to kr. 350 and online payments up to kr. 225.[1]

[1] See European Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 (*link*).

Most fraud with Danish payment cards occurs in foreign e-commerce

Danish payment card fraud occurs mainly on foreign websites, see chart 3. In 2023, total fraud with Danish-issued payment cards in foreign e-commerce was kr. 219 million, corresponding to approx. 75 per cent of total card fraud.

There may be several reasons why payment card fraud on foreign websites is increasing. One of the reasons is that the requirements for two-factor authentication of payments do not apply outside the EEA.[6] This enables fraud with Danish payment cards if the fraudsters have gained knowledge of the payment card details and the foreign website has not implemented similar security measures for authorising the payment.

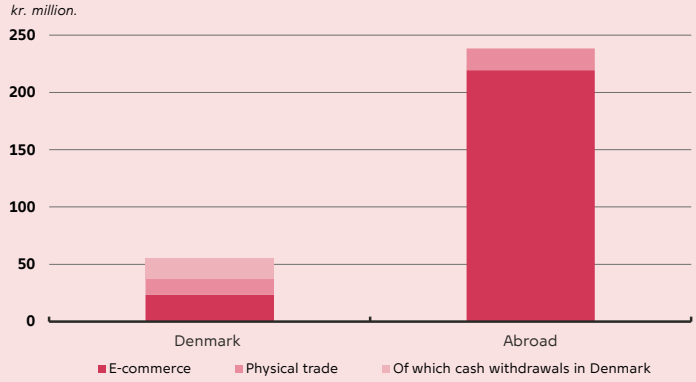
In the first half of 2023, almost half of total payment card fraud took place abroad outside the EEA, even though less than a fifth of total foreign turnover on Danish payment cards was made in the region. Relative Danish payment card fraud is thus significantly higher outside Europe than in Europe and especially in relation to Denmark, see chart 4.

[5] See Sveriges Riksbank: *Payments Report 2024*, March 2024 (*link*).
[6] The European Economic Area, EEA, covers the EU countries, Norway, Iceland and Liechtenstein.

CHART 3

The majority of payment card fraud happens abroad

Breakdown of total payment card fraud in 2023

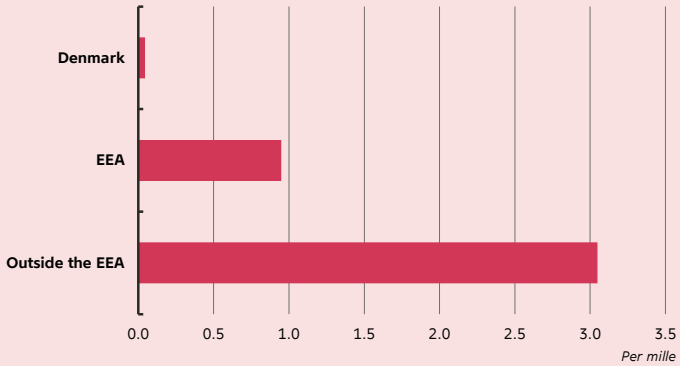


Note: Fraud with Danish-issued payment cards. Physical trade abroad also includes cash withdrawals, making a breakdown impossible.
Source: Danmarks Nationalbank.

CHART 4

Relative card fraud is highest outside of Europe

Total payment card fraud in relation to total card turnover



Note: Fraud with Danish-issued payment cards. The calculation covers the first half of 2023. The European Economic Area, EEA, covers the EU countries, Norway, Iceland and Liechtenstein.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2* and Danmarks Nationalbank.

Methods used by fraudsters and scammers to steal payment card details

Among other things, fraudsters use fake online stores to gain access to cardholder details. This happens, for example, when paying on a fake online store in expectation of receiving a product or when making card payments in connection with fake investment opportunities. See more examples in box 2.

Scammers also make extensive use of phishing and smishing, using email or text messages to steal payment card details and personal data. This is done, for example, by the scammers pretending to be from a bank or Danish authorities.[7]

The methods used by scammers make it difficult to combat fraud and scams, as the cardholders themselves provide the card details and in some cases also authorise the payment. This allows the scammers to receive the original payment and use the card details to make other fraudulent purchases or transactions. However, the two-factor authentication rules do seem to be limiting the ability of scammers to make additional payment demands within the EEA, which may help explain why the relative value of fraud is higher outside the EEA, see chart 4.

[7] See Finance Denmark, *Netbanksvindel* (online banking scams, in Danish only) (*link*).

BOX 2

Examples of fraud and scams with payment cards and credit transfers

Fake online stores: Payment card fraud occurs primarily online. This can be the case, for example, when the payer makes payments in good faith at fake online stores and the card details are subsequently used fraudulently. The Danish Agency for Digital Government and the Centre for Cyber Security, among others, therefore recommend checking the authenticity of an online store if it seems suspicious.[1]

Scams in private trade: According to Finance Denmark, the organisation that represents bank interests, a large proportion of digital scams involve social media and trading platforms such as Facebook Marketplace and DBA.[2] These can include fake ads for concert tickets or home rentals, where there are typically many interested buyers, prompting users to transfer money quickly in the expectation of securing the item. The police therefore encourage buyers to meet the vendor in person to ensure they get the product they pay for.[3] In addition, several ticket agents offer a solution for reselling tickets so that the ticket is verified and guaranteed, which is done against payment through the ticket issuer.

Phishing and smishing: In many cases, scammers try to steal payment card details and personal data, such as MitID, using email (phishing) or text message (smishing). They do so, for example, by pretending to be from a Danish authority or company and convincing the recipient to open a link and subsequently make a payment. The Danish Agency for Digital Government and the Centre for Cyber Security warn that no response should be made to such requests, as no genuine companies or authorities will request payment card details, MitID or other login information via email or text message.[4]

Online banking scams: Online banking scams can be due to criminals successfully hacking the online banking system of the cardholder, for example by stealing user login details. In the vast majority of cases, however, online banking scams are where criminals succeed in tricking cardholders to transfer money to the scammers themselves, known as '*social engineering*'.[5]

Investment scams: By offering attractive returns on fake investment opportunities, such as stocks or crypto-assets, criminals manage to persuade victims to pay or transfer money for a fake investment.

Business scams: One of the ways criminals try to steal money from businesses is by sending invoices for goods or services that the company has not purchased. In other cases, the scammers impersonate an existing supplier and inform the company that they want payments to be made to a different bank account in the future.[6]

Five tips to avoid digital scams
According to the Danish Crime Prevention Council, IT-related crime is one of the most widespread forms of crime and affects all age groups. It is therefore important to be careful and sceptical when using the Internet or if receiving a phone call or text message from an unexpected and unknown sender. The Danish Crime Prevention Council provides five tips for avoiding digital scams.[7]

1) **Stop and take your time** before clicking, paying or sharing personal information. It is important to avoid hasty decisions.
2) **Listen to your gut instinct.** You will often sense that something is wrong.
3) **Be aware of the warning signs** if communication changes suddenly or seems different than usual and if you feel pressured to act quickly.
4) **Verify the identity of the person you are in contact with**. Use the authorities' official channels, such as the main number, and if it is someone you know, call the number they normally use.
5) **Never share personal information** such as MitID or passwords - even with family or friends.

[1] The Danish Agency for Digital Government, the Centre for Cyber Security and others have prepared a guide for detecting digital scams (*link*). A number of companies and organisations have also launched a website where cardholders can check whether a website is trustworthy or an attempt to scam *(link)*.
[2] See Finance Denmark, *Kampen mod digital svindel (report on digital fraud, in Danish only)*, December 2023 *(link)*.
[3] See Danish Police Service, *Undgå at blive snydt, når du handler med andre på nettet* (tips to avoid digital scams, in Danish only) *(link)*.
[4] See the Danish Agency for Digital Government and the Centre for Cyber Security and others, *sikkerdigital.dk* (in Danish only) *(link)*.
[5] See chart 8 and Finance Denmark, *Netbanksvindel* (online banking scams, in Danish only) *(link)*.
[6] See Finance Denmark, *Virksomhedssvindel* (business scams, in Danish only) *(link)*.
[7] See Danish Crime Prevention Council, *Stop op og undgå digital svindel (*tips to avoid digital scams, in Danish only) *(link)*.

Geographical blocking can limit payment card fraud abroad

Some payment cards allow so-called geo-blocking. This means that cardholders can choose not to use a card for payments in specific geographical areas or for certain payment situations, such as online shopping or cash withdrawals. This prevents the possibility of payment card fraud in certain geographical areas or payment situations when cardholders would not typically use the card. This applies, for example, to online shopping outside of Europe. If a cardholder needs to pay in a blocked area or in a blocked payment situation at a later date, the block can usually be lifted temporarily or permanently via online or mobile banking.

However, not all card types support geo-blocking. This is partly due to the fact that several card issuers do not offer the blocking option and that awareness of geo-blocking among the population is limited. Increased use of geo-blocking is believed to reduce payment card fraud but requires a wider roll-out of the solution across card types and card issuers.

Payment card fraud in Denmark is low in physical trade and online

The extent of payment card fraud in Denmark is relatively low. In 2023, the total value of payment card fraud in Denmark was kr. 56 million. Of this figure, approx. 40 per cent took place online, while the remainder was in physical trade and at ATMs, see chart 3. This means that payment card fraud in Denmark differs from payment card fraud abroad in that the value of fraud in Danish e-commerce is just as low as in physical trade. In 2023, the relative proportion of payment card fraud in both online and physical trade was approximately 0.1 per mille. The low proportion emphasises that payments in Denmark are very secure.

The high level of security is due to the fact that payment cards are secure and difficult to counterfeit, and that card schemes and financial institutions have consistently developed and implemented effective real-time mechanisms to identify suspicious transactions. As a result, virtually all fraudulent transactions in physical trade in Denmark are down to lost or stolen payment cards.[8]

Card payments using mobile phones have given fraudsters and scammers new opportunities

Denmark is one of the most digitalised countries in the world when it comes to payments, with around 9 out of 10 payments in physical trade being made digitally.[9] But the high degree of digitalisation also provides fraudsters and scammers with new payment options that are not necessarily as common in other countries. For example, card payments via mobile phones, wallet payments such as Apple Pay or Google Pay, which are widely used in Denmark.

Wallet payments have made it possible for criminals to digitise stolen payment card details on their own mobile phones. In addition, a particular challenge with wallet payments is that if fraudsters manage to digitise a stolen payment card, they can withdraw money from the associated payment account without knowing the PIN. This is because they can authorise payments with their own mobile phone pass code or face recognition rather than the card's PIN.[10]

[8] In 2023, the total value of fraudulent transactions using counterfeit payment cards in Denmark was approx. kr. 124,000 out of total payment card fraud in physical trade in Denmark of approx. kr. 14.3 million.
[9] See Danmarks Nationalbank: Denmark is among the most digitalised countries in terms of payments, *Danmarks Nationalbank Analysis*, no. 2, February 2022 (*link*).
[10] When using wallet payments such as Apple Pay or Google Pay, card issuers use delegated authentication, where two-factor authentication is carried out in the wallet provider's environment. A numeric code or biometric solution can be used, for example, see The Danish Financial Supervisory Authority, *Temaundersøgelse om brugen af stærk kundeautentifikation i e-handlen,* (report on use of strong authentication in e-commerce, in Danish only) 2021 *(link).*

However, digitising a stolen payment card is difficult because it also requires authorisation from the card owner using MitID. Financial institutions and card schemes also prevent a large number of the attempts made by fraudsters and scammers. Wallet payment fraud is therefore usually due to the cardholder having been the victim of identity theft[11], or that the scammer has tricked the cardholder into authorising the digitalisation of the payment card on the scammer's mobile phone.

Since 2021, the value of payment card fraud in Danish physical trade has doubled to just over kr. 14 million, largely due to the fact that the average transaction value has increased and that fraudsters and scammers are increasingly managing to pay without using PINs, e.g. by using wallet payments, see charts 5 and 6.

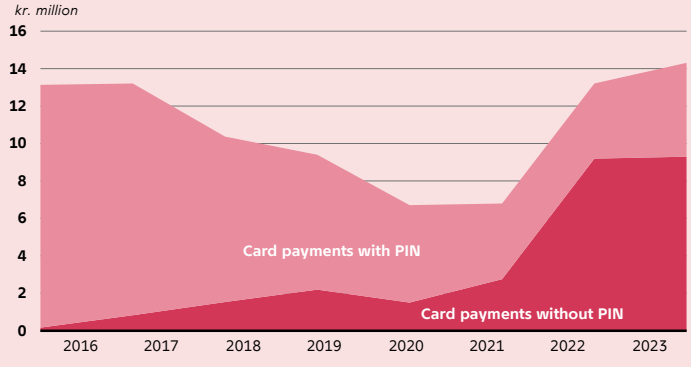
The increase in the value of fraud where a PIN is not used should particularly be seen in light of the fact that before the introduction of mobile wallet payments, it was impossible to make card payments in physical trade of over kr. 350 without using a PIN, see box 1. Viewed in isolation, wallet payments have made it possible for fraudsters and scammers to illegally use stolen payment card details for large transaction values without knowing the PIN if they manage to digitise the payment card.

Wallet payment fraud can be difficult to detect for the public and financial institutions, as the payments typically look like ordinary everyday transactions when they appear in online banking. Neither is a card actually lost, which means that in some cases it can take a long time before the fraud is detected.

CHART 5

Fraud value of card payments in Denmark in physical trade

Breakdown of value of payment card fraud in Danish physical trade by whether or not the PIN has been used for payment

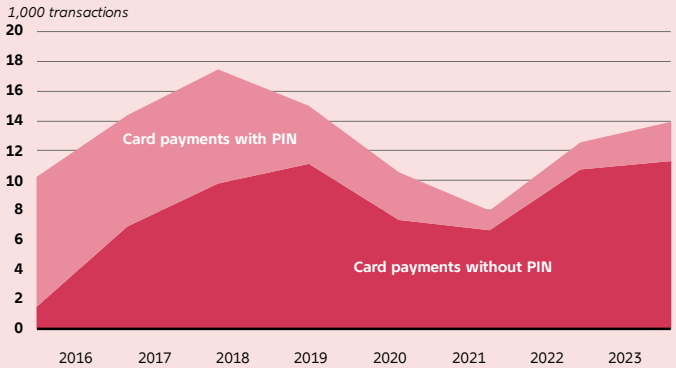


Note: Card payments without a PIN are typically contactless payments or mobile wallet payments. The analysis covers Danish-issued payment cards.
Source: Danmarks Nationalbank.

CHART 6

Number of fraudulent transactions in Denmark in physical trade

Breakdown of fraudulent transactions on payment cards in Danish physical trade by whether or not the PIN code was used for the payment



Note: Card payments without a PIN are typically contactless payments or mobile wallet payments. The analysis covers Danish-issued payment cards.
Source: Danmarks Nationalbank.

[11] Identity theft includes someone illegally obtaining someone else's data, which they can misuse to take out loans or buy things, for example. Such personal data can be a CPR number, password or MitID. It is not identity theft if a fraudster or scammer gains access to credit card information and misuses it, see Borger.dk (*link*).

03
Credit transfer fraud is on the rise

Ways in which fraudsters can commit fraud and misuse bank account details have changed in recent years. This is partly because account holders are increasingly making transfers themselves without the direct involvement of their bank, e.g. using mobile or online banking, and because the population is increasingly using digital payment solutions that use credit transfers to make payments, e.g. MobilePay.

Unlike card payment fraud, financial crime associated with credit transfers is typically related to financial scams where account holders are tricked into making the transfer. It also means that credit transfer fraud is not necessarily linked to a payment situation.

Credit transfer fraud via mobile or online banking also differ from payment card fraud in that payment cards are only linked to one specific account, with cash withdrawals and ongoing spending with payment cards usually limited in amount. However, if the scammer manages to gain access to online banking, perhaps by tricking the victim into providing authorisation, it is possible to make credit transfers from several accounts and simultaneously empty them or create overdrafts if the account allows.

In most cases, banks are successful in preventing scams. Nevertheless, the total value of credit transfer fraud has been increasing and in 2023 was approximately kr. 333 million, see chart 7. This is roughly on a par with the value of payment card fraud, which in the same period was approximately kr. 294 million. However, unlike payment card, significantly fewer, but on average larger fraudulent transactions were recorded. In 2023, approximately 9,400 fraudulent credit transfers were recorded with an average value of approximately kr. 35,300. In comparison, the average value of payment card fraud was just under kr. 1,300 in 2023, see section 2.

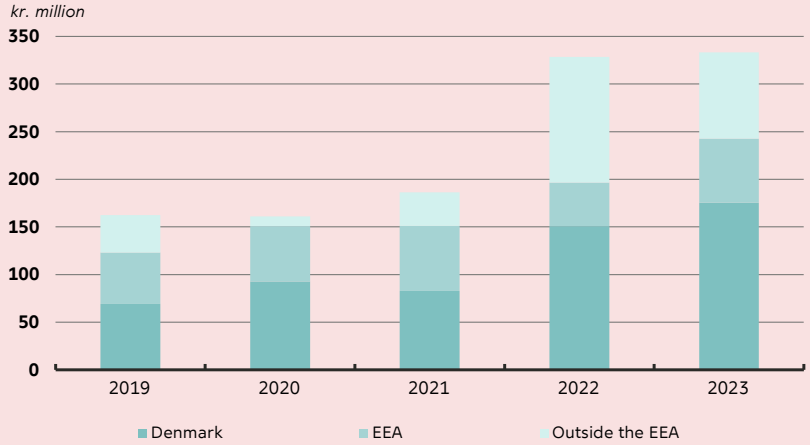
According to figures from the organisation representing the interests of banks, Finance Denmark, members of the public are the main victims of credit transfer fraud: In the first half of 2023, fraud related to the public accounted for approximately 80 per cent of the total fraud value, while business fraud accounted for just under 20 per cent.[12] This has led to several authorities and organisations communicating with cardholders to try and prevent digital scams, see box 2.

[12] See Finance Denmark, *Virksomhedssvindel,* (business scams, in Danish only) (*link*).

CHART 7

Credit transfer fraud is on the rise

Total credit transfer fraud and scams by origin of recipient account



Note: The scope covers the full value of credit transfer fraud and scams. In several cases, the banks succeeded in reversing all or part of a fraudulent transfer, so the total loss is lower, see chart 10. Banks also prevented the majority of fraudulent transfers before they were completed. Data breach between H1 and H2 2020.

Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2,* and Danmarks Nationalbank.

Credit transfer fraud stem particularly from scams where account holders make the payment to the scammer

The rules for two-factor authentication mean that accessing online banking and making payments requires authorisation with MitID, for example. This has increasingly made it necessary for scammers to involve cardholders to complete and authorise fraudulent payments.

Credit transfer fraud therefore increasingly involve account holders being tricked into transferring money to the scammers, for example, under the guise of claiming that their online banking has been hacked and therefore they should transfer their savings to a 'secure account'.

Approximately 81 per cent of the total value of credit transfer fraud in 2023 were scams of private or corporate account holders transferring money themselves, see chart 8. This happens, for example, when criminals contact account holders by phone and pretend to be from a bank or Danish authorities or when an account holder sees a fake advert on social media or trading platforms and makes a payment using a mobile phone, for example.[13]

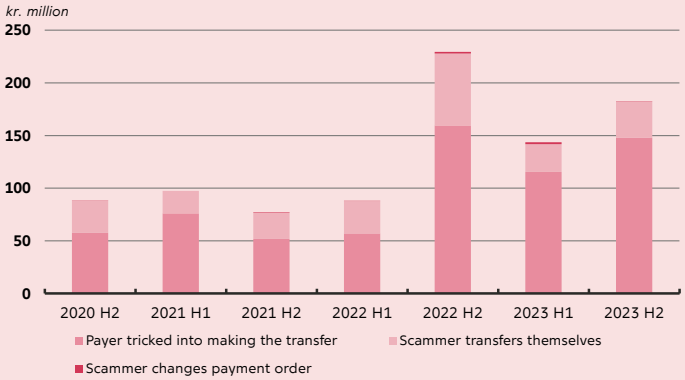
Since the introduction of two-factor authentication, the vast majority of fraudulent credit transfers have been authorised using two-factor authentication, see chart 9. This emphasises that fraudsters and scammers are constantly changing and adapting the methods they use to commit fraud as new security measures are introduced.

[13] See Finance Denmark, *Netbanksvindel* (online banking scams, in Danish only (*link*), and *Kampen mod digital svindel* (report on digital scam, in Danish only) (*link*).

CHART 8

Credit transfer fraud stem particularly from scams where account holders transfer money to the scammer

Total credit transfer fraud broken down by
the party transferring money to the scammer

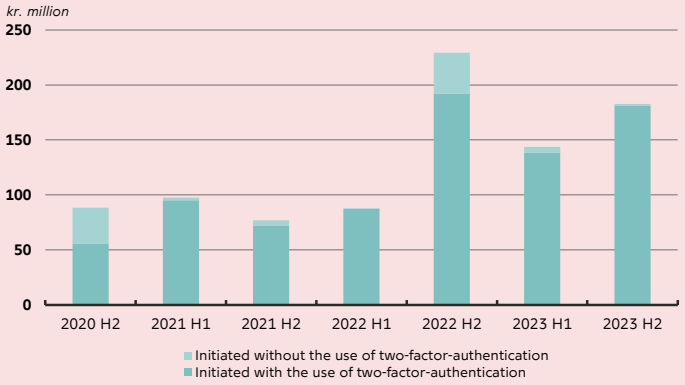


Note: The extent of fraud where scammers change a payment order is limited and can therefore be difficult to see in the chart.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2,* and Danmarks Nationalbank.

CHART 9

Most credit transfer fraud is authorised using two-factor authentication

Total credit transfer fraud by whether
or not two-factor authentication was used in the transfer



Note: The two-factor authentication rules for credit transfers came into effect on 1 January 2018. The high value of credit transfer fraud initiated without two-factor authentication in H2 2022 is down to a few high-value corporate transactions that were exempted from the two-factor authentication requirement under Article 17 of COM/2018/389.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2,* and Danmarks Nationalbank.

The remaining cases of fraud that do not directly involve account holders are primarily cases where the fraudster has gained access to an account holder's online bank and made the transfer themselves. These may be due to phishing, where the fraudster manages to get login details, or the fraudster manages to steal information in some other way, for example by installing malicious software, also known as *malware*. In order for the fraudsters to complete the transfer themselves, they also need to be able to authorise the transfer using MitID.

Only in a few cases do fraudsters manage to modify an existing payment order, which emphasises that the payments infrastructure itself is very secure.

Most attempts at credit transfer scams are stopped by banks

In most cases, banks manage to stop credit transfer scams before it happens. According to figures from Finance Denmark, banks prevented approximately 60 per cent of the total value of attempted scams in 2022.[14]

Banks also manage to recover some of the value of scams that initially flow through the payment systems. Of the total value of credit transfer fraud in 2023 of approx. kr. 333 million, the banks succeeded in reversing approx. kr. 67 million. The total loss in the period was therefore approx. kr. 266 million.

Credit transfer scams, where account holders are tricked into transferring money, can be difficult for banks to prevent as the transactions can look like regular credit transfers made by the account holder. Furthermore, two-factor

[14] See Finance Denmark, *Kampen mod digital svindel* (report on digital fraud, in Danish only), December 2023 *(link)*.

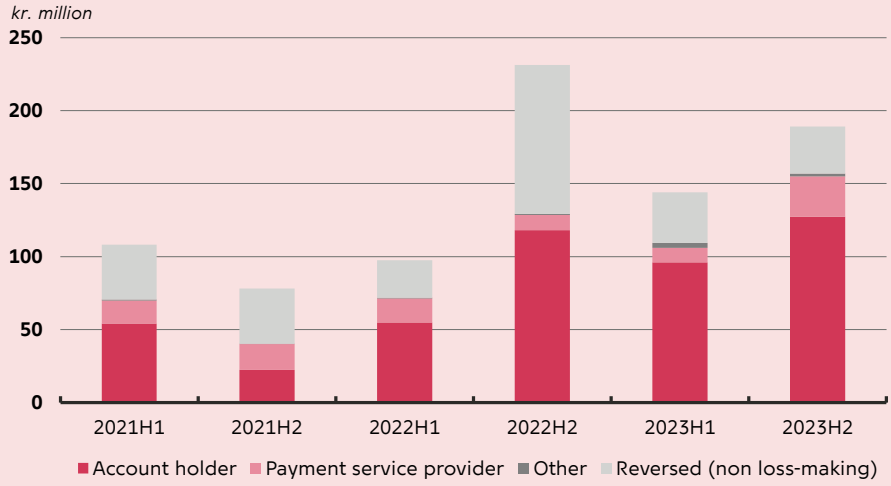
authentication does not prevent payment, as the payer authorises the transaction themselves.

If account holders have been victims of credit transfer scams and have made and authorised the payments themselves, they will be liable for the financial loss in most cases, see box 3. Of the total losses in 2023, payers who were victims were liable for approx. kr. 223 million, corresponding to approx. 84 per cent of the total losses, see chart 10.

CHART 10

Account holders are largely liable for losses from credit transfer fraud

Total credit transfer fraud broken down by the party liable for the loss



Note: The account holder is the private citizen or company that has made the payment.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2* and Danmarks Nationalbank.

To curb digital scams, the Danish Ministry of Industry, Business and Financial Affairs in collaboration with Finance Denmark, Forbrugerrådet Tænk (Danish Consumer Council), the telecoms industry and Ældre Sagen (DaneAge Association) launched four initiatives in the autumn of 2023. They include a reduced daily limit for instant payments of kr. 50,000 without first contacting the bank and awareness campaigns on digital scams. A solution has also been implemented enabling senders of text messages to have their sender name protected so that scammers cannot impersonate a bank or government agency.[15] More recently, Finance Denmark launched the campaign *Sikker bank - sammen (Safe banking - together*) and set up a fraud task force to identify new initiatives and recommendations to reduce digital scams in December 2023.[16]

[15] See Ministry of Industry, Business and Financial Affairs, *Kampen mod digital svindel styrkes,* November 2023 (*link*).
[16] See Finance Denmark, *Sikker bank – sammen* (safe banking – together, in Danish only) (*link*), and *Ny Svindel Task Force tager kampen op mod de kriminelle* (new fraud task to reduce digital scams, in Danish only), December 2023 (*link*).

BOX 3

Legislation regarding digital payment fraud

The payment service provider, usually the payer's bank, is generally liable for digital payment fraud, such as payment card fraud, but the type of fraud and lack of caution can increase the payer's degree of liability.

The payment service provider is liable for the payer's loss if the payment service provider has chosen to exempt the specific payment from the requirement for two-factor authentication, see box 1. This applies to contactless card payments, for example, where the payer does not use a PIN. On the other hand, the payer must cover kr. 375 of the total fraud if the payment service provider can prove that a personal security measure, such as a PIN or the MitID app, has been used to authorise the payment. This applies even if the payer has not provided their PIN or MitID details to anyone.

The payer is liable for up to kr. 8,000 in cases where the payment service provider can prove that a personal security measure has been used and the payer has otherwise behaved irresponsibly, for example by disclosing their PIN or granting access to MitID. The same rules apply if the payer has not notified the bank as soon as possible after realising that they have lost their payment card or their mobile phone if it can make mobile payments.

The payer will have unlimited liability if the payment service provider can prove that the payer has given a personal security measure to the scammer and that the payer knew or should have known that it would involve a risk of being scammed.

The payer's liability is also generally unlimited if the payer completes the payment using two-factor authentication. This applies, for example, when making payments at fake online stores or when scammers manage to persuade the payer to transfer money. In some cases, however, the bank has the option to stop the payment and possibly reverse all or part of the payment.

In several cases, payment card and credit transfer scams are punishable under the clause relating to fraud in the Danish Criminal Code.[1] Violation of this clause is generally punishable by imprisonment of up to one year and six months, but in particularly serious cases the penalty can increase to imprisonment of up to eight years.

Source: Danish Payment Services Act (*link*) and the Danish Criminal Code, Chapter 28 (*link*).

[1] See, for example, South Jutland Police, June 2020 (in Danish only) (*link*).

A large proportion of credit transfer fraud is to Danish accounts

In contrast to payment card fraud, a large proportion of the total credit transfer scams occurs through Danish accounts, see chart 7.

As part of uncovering digital payment fraud in Denmark, Danmarks Nationalbank has been in dialogue with some of the largest payment and financial institutions in Denmark to gain insight into the fraud patterns that typically affect their customers and why fraudulent credit transfers are made to Danish accounts in particular.

Those institutions cite several possible explanations. One reason is that the payments infrastructure for domestic credit transfers is better connected than for foreign accounts. This is because most credit transfers abroad require more information in order for the transfer to be completed. In addition, credit transfers abroad typically take longer, giving institutions and account holders more time to prevent fraudulent transfers.

Another reason, according to the institutions, is that credit transfer fraud often occurs when scammers trick account holders into transferring money to the scammers: In this case, payers will probably perceive a transfer to a foreign account as more suspicious than to a Danish bank account.

Finally, according to the financial institutions, the fraud pattern should be seen in the context of the fact that scammers often use a combination of payment card fraud and credit transfer scams. This means that scammers use a stolen recipient account for which they also have access to payment card details. This enables credit transfers from other victims, after which the scammers can pay, withdraw, obscure, or transfer the money abroad.

04
Digital fraud affects all cohorts of the population

In the spring of 2023, Danmarks Nationalbank used a questionnaire to survey public payment habits. Among other things, the survey provided insight into the types of fraud the public is exposed to and whether digital fraud is more prevalent in certain cohorts of the population. Respondents were asked if they had made a payment in the past year in connection with a purchase or investment opportunity that turned out to be a scam.[17]

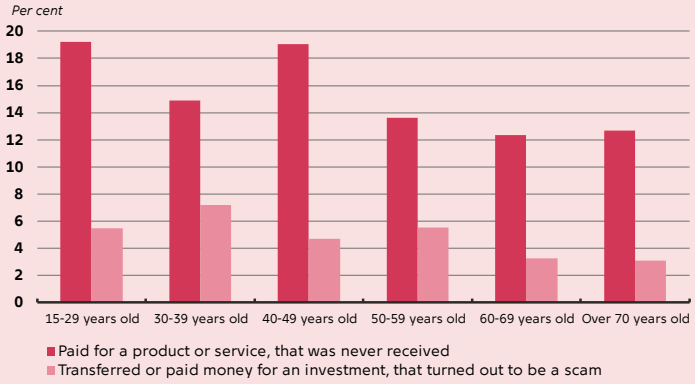
According to the survey, 16 per cent of respondents had paid for a product or service that they never received. Similarly, just under 5 per cent of respondents indicated that they had paid money for an investment that turned out to be a scam.[18] The results therefore indicate that a larger proportion of the population has experienced payment situations that involved a potential scam, but this does not necessarily mean that financial loss was experienced.[19]

Across the population, it was especially those under the age of 50 who experienced paying for a product or service that they never received. However, the results should be seen in light of the fact that the same population cohort often shops more online. Similarly, the study showed that it was typically citizens under the age of 60 who transferred or paid money for an investment that turned out to be a scam. The results therefore indicate that digital scams affect all cohorts of the population, see chart 11.[20]

[17] The data were collected by the analysis institute Epinion and were based on responses from a representative selection of 2,737 citizens over the age of 15.
[18] Survey uncertainty is +/- 1.3 percentage points for the question on the purchase of goods or services not received and +/- 0.8 percentage points for the question on investment. The scope of Danmarks Nationalbank's survey indicates that the *recorded* cases of payment card fraud and credit transfer fraud are likely to not represent true figures. This should be seen in light of the fact that in some cases the payer is fully or partially liable for the total amount of the scam, see box 3. In such cases, cardholders have no financial incentive to report the loss.
[19] In online shopping, for example, special 'charge back rules' apply, which ensure a refund in situations where the payer does not receive the goods or services they have ordered, see Article 112 of the Danish Payment Services Act (*link*).
[20] Similar results are found in the latest report on IT use in the population, which concludes that the younger cohort of the population in particular has suffered financial losses as a result of an online scam. See Statistics Denmark: *IT-anvendelse i befolkningen 2023* (in Danish only) *(link)*.

CHART 11

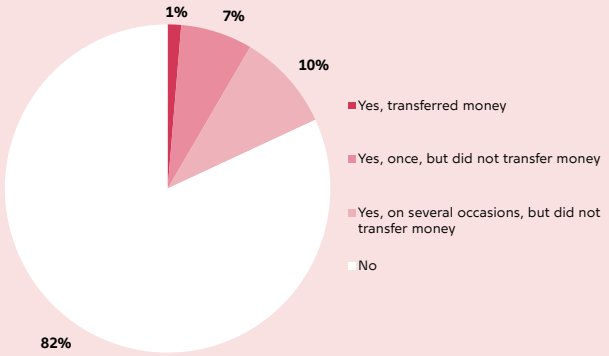
Digital fraud affects all cohorts of the population



Note: Based on 2,737 responses. Respondents were asked if they had paid for a product or service in the past year that they never received, or if they had been the victim of an investment scam.
Source: Danmarks Nationalbank, *Household survey 2023*.

CHART 12

Approximately 1 per cent of the population have transferred money to a scammer who contacted them by phone



Note: Based on 2,737 responses. Respondents were asked if they had been contacted by a scammer over the phone within the past year and had subsequently transferred money.
Source: Danmarks Nationalbank, *Household survey 2023*.

In Danmarks Nationalbank's survey, respondents were also asked whether they had been contacted by telephone within the past year by a person who pretended to be from a bank or authority, for example, but turned out to be a scammer. According to the survey, approximately 18 per cent of the population had received a phone call or text message from a scammer at least once in the past year. However, the vast majority of respondents contacted recognised the scam and therefore did not transfer any money. But scammers still managed to trick around 1 per cent of the population into transferring money, see chart 12.[21]

[21] Survey uncertainty is +/- 0.4 percentage points for the question on phone scams. The Danish Agency for Digital Government also finds that approx. 1 per cent of citizens provide the information requested by scammers, see Danish Agency for Digital Government, *Danskernes informationssikkerhed 2022* (in Danish only) *(link)*.

05
Appendix table

Credit transfer fraud and scams by origin of recipient account

Table A1

kr. million	2019	2020	2021	2022	2023*
Total value of credit transfer fraud and scams	162.3	161.2	186.2	328.6	333.2
Denmark	69.1	92.8	82.9	150.7	175.5
EEA	53.8	58.0	68.1	45.8	67.3
Outside the EEA	39.3	10.3	35.2	132.1	90.4

Note: Data breach between H1 and H2 2020. *Data for 2023 are preliminary figures.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2,* and Danmarks Nationalbank.

Credit transfer fraud and scams by type

Table A2

kr. million	2020H2	2021H1	2021H2	2022H1	2022H2	2023H1	2023H2*
Scammer transfers themselves	30.6	21.4	24.8	30.9	68.2	26.5	34.7
Payer tricked	57.6	76.0	51.9	56.9	159.6	115.4	149.5
Scammer changes payment order	0.2	0.0	0.4	0.0	1.5	1.7	0.3
Initiated with two-factor authentication	55.7	95.1	72.2	87.3	191.9	138.4	182.9
Initiated without two-factor authentication	32.7	2.3	4.8	0.6	37.4	5.2	1.7

Note: *Data for H2 2023 are preliminary figures.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2* and Danmarks Nationalbank.

Credit transfer fraud and scams broken down by liability

Table A3

kr. million	2021H1	2021H2	2022H1	2022H2	2023H1	2023H2*
Payer	54.1	22.4	54.7	118.0	96.1	127.2
Bank	15.8	17.5	16.5	10.4	9.8	27.8
Other	0.6	0.4	0.6	0.8	3.3	1.8
Reversed (non loss-making)	37.6	37.7	25.6	101.9	34.8	32.4
Total	108.2	78.0	97.4	231.1	144.0	189.2

Note: 'Payer' is the citizen or business that has made the payment. *Data for H2 2023 are preliminary figures.
Source: Reporting by financial institutions to the Danish Financial Supervisory Authority under the European Banking Authority, *EBA guidelines on fraud reporting under PSD2* and Danmarks Nationalbank.

Like to receive *updates* from Danmarks Nationalbank?

Get the latest news on our publications sent straight to your inbox.

To learn more about our news service,
and to sign up, visit *nationalbanken.dk/en/news-service,*
or *scan the QR code.*

You can also receive our news as RSS feeds.
For details, visit nationalbanken.dk/en/rss-feeds.

Publications

NEWS

News is an appetiser offering quick insight into one of Danmarks Nationalbank's more extensive publications. News is targeted at people who need an easy overview and like a clear angle.

STATISTICAL NEWS

Statistical news focuses on the latest figures and trends in Danmarks Nationalbank's statistics. Statistical news is targeted at people who want quick insight into current financial data.

REPORT

Reports consist of recurring reports on Danmarks Nationalbank's areas of work and activities. Here you will find Danmarks Nationalbank's annual report, among other documents. Reports are targeted at people who need a status and update on the past period.

ANALYSIS

Analyses focus on current issues of particular relevance to Danmarks Nationalbank's objectives. Analyses may also contain Danmarks Nationalbank's recommendations. They include our projections for the Danish economy and our assessment of financial stability. Analyses are targeted at people with a broad interest in economic and financial matters.

ECONOMIC MEMO

Economic Memo provides insight into the analysis work being performed by Danmarks Nationalbank's employees. For example, Economic Memo contains background analyses and method descriptions. Economic Memos are primarily targeted at people who already have a knowledge of economic and financial analyses.

WORKING PAPER

Working Paper presents research work by both Danmarks Nationalbank's employees and our partners. Working Paper is primarily targeted at professionals and people with an interest in central banking research as well as economics and finance in a broader sense.

The analysis consists of a Danish and an English version. In case of doubt as to the correctness of the translation, the Danish version will prevail.

Danmarks Nationalbank
Langelinie Allé 47
DK-2100 Copenhagen Ø
+45 3363 6363

Editing completed on 22 April 2024

DANMARKS
NATIONALBANK