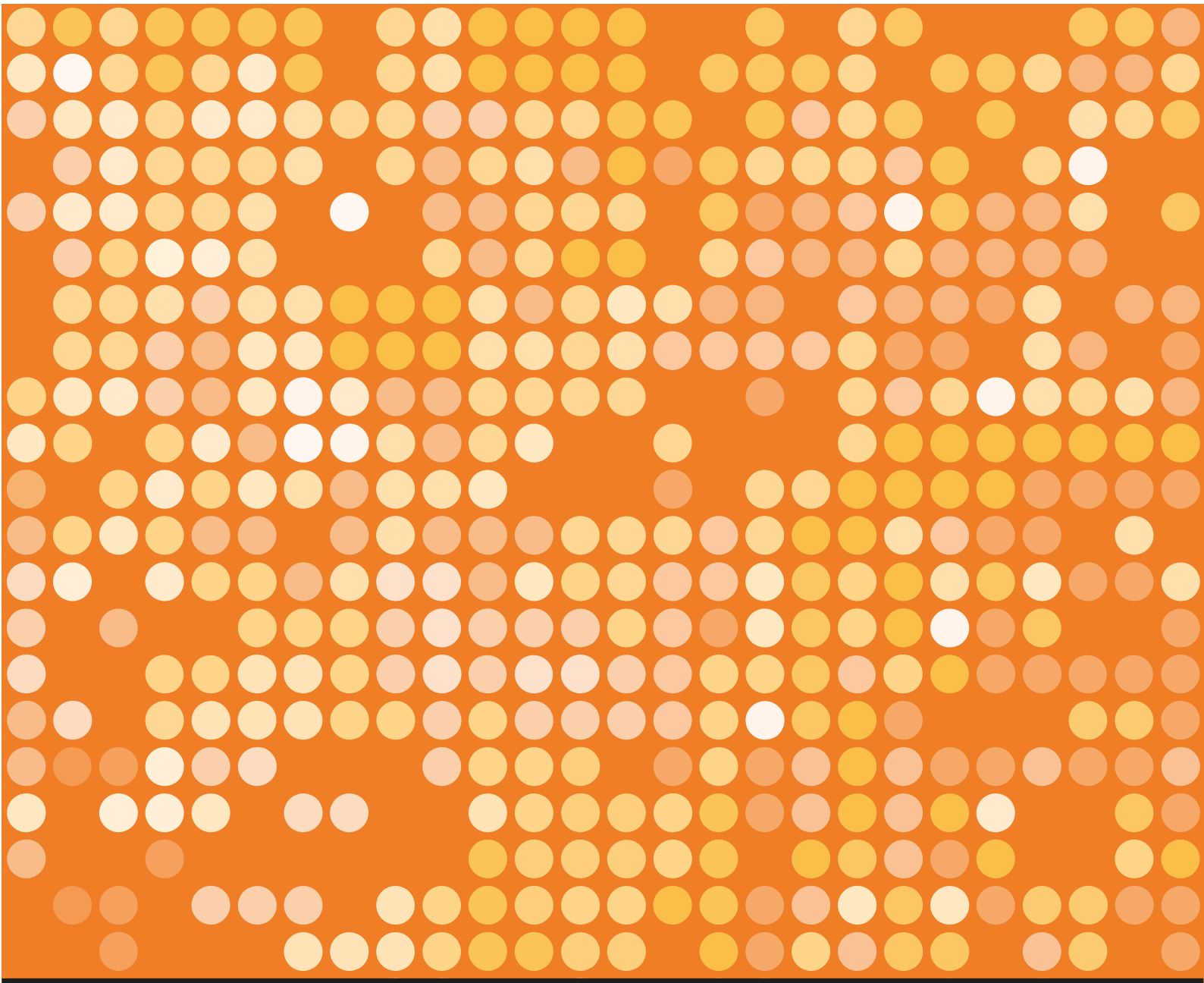
English summary of report 2023:11



Fraud against individuals

The appropriateness of preventive measures

The Swedish National Council for Crime Prevention (Brå) - centre for knowledge about crime and crime prevention measures

The Swedish National Council for Crime Prevention (Brå) works to reduce crime and improve levels of safety in society. We do this by providing factual information and disseminating knowledge on crime and crime prevention work, primarily for the Government and agencies in the criminal justice system.

The publication is available as a pdf at www.bra.se. On request, Brå can develop an alternative format. Please send any enquiry about alternative formats to tillgangligt@bra.se. When material is quoted or tables, figures, and diagrams are used, Brå must be stated as the source. Permission of the copyright holder is necessary for reproduction of images, photographs, and illustrations.

This report is a summary of the Swedish report Bedrägerier mot privatpersoner. De förebyggande åtgärdernas träffsäkerhet. 2022:11

urn:nbn:se:bra-1141
ISSN 1100-6676

Author: Lina Fjelkegård och Anna Horgby

The Swedish National Council for Crime Prevention, Box 1386, 111 93 Stockholm, Sweden
Tel: +46(0)8 527 58 400, E-mail: info@bra.se, www.bra.se

This summary can be downloaded from the Swedish National Council for Crime Prevention's website, www.bra.se/publikationer

Fraud against individuals

The appropriateness of preventive measures

English summary of Brå report 2023:11

Summary

Fraud is a crime that affects many people, and has increased in scope over time. More than 180,000 cases of fraud were reported in 2022, compared to 50,000 in 2000. The Swedish Police Authority also reports significant proceeds of crime from fraud, which have increased over time and are often attributed to organised crime. The high level of crime, combined with the fact that these crimes are generally hard to investigate, means that crime prevention work must be prioritised. Brå therefore initiated a study on fraud against individuals in order to investigate how reliable these crime prevention measures are. The appropriateness of preventive work is being studied through an analysis of how circumstances and situations that make fraud possible are targeted by fraud prevention measures. The report also includes recommendations for different crime prevention actors.

The study is primarily based on interviews with professionals from the Swedish Police Authority, other government agencies, interest groups and businesses. These interviews have been supplemented with written materials and some descriptive statistics.

Telephone fraud is described as the most serious problem

Different sources give different pictures of the scope and structure of fraud crimes. For example, *card fraud* accounted for 40% of all reported crimes in 2022, but only 5% of the estimated proceeds of crime. In the same year, reported instances of *fraud through social engineering* – where the fraudster establishes trust to trick the victim into giving them money or personal information – accounted for 19% of all reported crimes and 46% of the proceeds of crime.

Telephone fraud, in which the victim is contacted by telephone, is the most worrying type of fraud according to most interviewees. The fraudster will usually have carried out research before the call to select suitable victims and to ensure that they sound credible when making contact. This deception often involves the fraudster having manipulated the phone number that the recipient sees. For example, the fraudster may claim to be calling from the police, the bank or a debt collection agency, and pressurises and scares the victim with a made-up story. The fraudster pretends to be

friendly and helpful, and offers a solution to the situation. The money is generally transferred to an intermediary account – often that of a young person – before ultimately ending up with a criminal network. Sender ID manipulation is also used to establish credibility in *social engineering via SMS, email or social media*, where the victim is tricked into carrying out a transaction or providing card details or personal data.

Two types of social engineering fraud for which reports are low but the proceeds of crime are relatively high are *romance fraud* and *investment fraud*. In cases of romance fraud, the fraudster typically initiates a romantic relationship with the victim via social media or dating sites to encourage the victim to transfer money to the fraudster at a later stage. Investment fraud against individuals involves tricking someone into investing money, often in some kind of financial product such as shares, bonds or cryptocurrencies. The contact is usually preceded by fraudulent adverts for these products on social media, which link to companies and websites that appear to be legitimate.

Social media as a platform, as well as links to fraudulent companies, websites and adverts, can also be used in other types of fraud, such as in *card fraud* and *advertising fraud* – in other words, the misleading sale or purchase of advertised goods or services.

Significant harm from fraud – especially through social engineering

Social engineering fraud often results in significant financial losses for victims. Many interviewees describe how victims often feel shame and guilt, and previous studies have shown that falling victim to fraud can cause psychological harm and lead to insecurity. This in turn can affect trust in society's institutions and systems. According to the interviews, social engineering fraud affects older people in particular.

Other types of fraud, such as card fraud and advertising fraud, mainly affect people of working age instead. The financial losses in these cases are relatively small, and are described as being associated with shame and guilt to a lesser extent than social engineering fraud.

Vulnerabilities that facilitate fraud

Based on our study of fraud crimes, a number of technical and structural vulnerabilities – as well as vulnerabilities of potential victims – have been identified:

- Readily available information such as name, address, age, family situation and vehicle ownership enables fraudsters to identify potential victims and prepare their deception.
- The ability to manipulate who is displayed as the sender of calls, text messages and emails makes the fraudster appear credible in their contact with the victim.
- The ability to publish fraudulent adverts, register fraudulent domains and companies, and use intermediaries to represent them allows fraudsters to establish credibility via seemingly legitimate websites, companies and adverts.
- A digital banking and payment market imply both insufficient transaction monitoring and considerable opportunities for fraudsters to make money untraceable quickly.
- Despite several measures having been taken, there are still opportunities to misuse someone else's identity for banking and card purchases.
- Access to specific skills to prepare and carry out the fraud (e.g. technical know-how) and to people who can be used as money launderers facilitates fraud.
- Digital ignorance and unfamiliarity, stress, a lack of critical thinking, risk tendency, the need for excitement, greed, desperation, loneliness and the need for affirmation, understanding, closeness and love are all vulnerabilities that are associated with potential victims. Digital illiteracy, susceptibility to stress and a lack of critical thinking are vulnerabilities that are particularly associated with older people.
- The lack of accessible alternatives to digital services means that people who lack digital skills, knowledge and perhaps the motivation to learn are forced to use services they do not master.

The identified vulnerabilities largely reflect people's behavioural patterns. What people do, how they do it and which alternatives are available, combined with human capabilities and characteristics, determine how fraud can be carried out and who is affected.

Different types of crime prevention measures

The interviews reveal a number of crime prevention measures that target these different technical and structural vulnerabilities. These include measures that make it harder to prepare for crime, such as checks on domains and user accounts. They also include measures aimed at making it harder to mislead in initial contacts, such as checks on adverts and initiatives against spoofed phone numbers. There are also measures such as transaction monitoring and secure login to stop fraudulent transactions, as well as measures that make it harder for perpetrators to access the proceeds of crime from fraud.

Brå's study also highlights crime prevention measures that involve strengthening individuals' ability to resist fraud attempts. Much of this work is aimed at older people to increase their abilities to protect themselves. These efforts are often focused on telephone fraud and other types of social engineering, to make older people more aware of fraudulent practices and how digital services such as bank ID work.

More needs to be done to ensure that these measures achieve their full effect

Despite a wide range of preventive measures, it is obvious that current crime prevention activities are nowhere near sufficient to address the problem of fraud against individuals.

Some measures have significant preventive potential, but so far only consist of lobbying work or are still being planned. These include a proposal for a state eID system, measures against the fraudulent use of spoofed phone numbers, solutions related to more secure identification when using digital services, and proposals for increased checks on businesses and online content.

There are also several circumstances that affect the opportunities for preventive work against certain vulnerabilities, such as legislation, expectations (e.g. for fast transactions) and the often international nature of these crimes. Interviewees from the banking sector describe challenges in terms of coming up with sufficiently reliable checks that can identify fraudulent transactions while allowing others through.

Measures to improve individuals' resilience to fraud are also associated with a large number of challenges. Interviewees see difficulties with getting

information across, especially for those groups who need it the most, and some are doubtful that these efforts have a crime prevention effect even when the information does get through. There is also research which shows that the impact of information efforts on people's behaviour is not obvious. To have an effect, messages and content need to be adapted according to the target audience and the context.

Brå's assessment

Fraud against individuals is a crime with serious consequences, and affects both individuals and society as a whole. Telephone fraud is of particular concern, as it often results in considerable financial and emotional harm to the victim, risks eroding trust in society's institutions and systems, and provides significant proceeds of crime to criminal networks. Other types of fraud also have serious consequences. Brå therefore believes that it is important to generally prioritise crime prevention work to counter fraud against individuals.

Brå has identified a large number of vulnerabilities that facilitate crime, both among potential victims and in the technical and structural circumstances. The overall assessment is that, with a few exceptions, these vulnerabilities are addressed by some form of preventive measure. However, it is clear that fraudsters are constantly developing their methods and strategies, and are identifying new vulnerabilities in technology, structures and individuals. The continued high – and, in many respects, rising – levels of crime also show that the preventive work being carried out is not sufficient, and that there is a need for further development and improvement.

Fraud involves deceiving people, and as technology becomes more secure, fraudsters are increasingly targeting the individual. Measures to make potential victims less likely to be deceived are therefore essential. However, these measures need to be designed to make them even more relevant to the target groups, including more practical elements. At the same time, digitalisation means that individuals have been given greater responsibility for protecting their banking assets, and are now reliant on digital solutions that they do not always master. Banks and other actors – within both the private sector and the public sector – who develop and provide the services and systems used in fraud therefore need to take back some of the responsibility and protect the individual better through more secure solutions.

Brå also sees a need for a clearer overall perspective within fraud prevention work, where technology and information are used in partnership to respond better to fraudsters' rapid adaptations. Technology can be used to make the information more accurate, relevant and clear. This information is, in turn, needed to ensure the correct use of the technology.

Brå's recommendations:

- The police should take a leading role in fraud prevention work. Increased support is needed for the police regions and local police districts in terms of how the local levels can include fraud in their status reports and action plans. To ensure that the problem descriptions drawn up by the police are relevant for fraud prevention work, they should also include attempted crimes and reports that are dismissed immediately. The police also need to update and improve the relevance of existing information and training materials on fraud by further enhancing target group adaptation and adding more and better adapted practical elements. In addition, broad implementation of the crime prevention strategy within the authority is required.
- The Swedish Police Authority, in collaboration with agencies such as the Swedish Association of Local Authorities and Regions, the Swedish Theft Protection Association, the Swedish Internet Foundation and the Swedish Civil Contingencies Agency, should develop and systematise targeted information initiatives for children and young people who risk being used to launder money.
- To make it harder to prepare for fraud and to launder the proceeds of crime, the Swedish Companies Registration Office, the Swedish Internet Foundation, online platforms and search engines should increase their checks on company and domain representatives, websites, user accounts and adverts. In particular, Brå has identified a need for the Swedish Companies Registration Office – in accordance with the proposals contained in SOU 2023:34 – to expand its checks on company representatives.
- The Government should review the opportunities for limiting the publication of personal data that can be used to identify potential victims of fraud.
- The Swedish Post and Telecom Authority, telephone operators and the Swedish Telecom Advisors should continue and accelerate their work to combat spoofed phone numbers, and should extend this work to other areas, such as the fraudulent use of text messages and mobile

phone numbers.

- The Government should move forward with the proposal for a state eID. This eID needs to be implemented and ultimately developed.
- All banks should ensure that BankID's solutions for secure identification and signing are fully implemented. At the same time, non-secure options should be phased out. Banks should also continue to develop more secure digital banking, particularly in connection with authorised transactions.[1] Areas where Brå has identified particular opportunities for development include banking products with voluntary restrictions and individual-based transaction monitoring.
- Different actors within society should develop the use of push notifications and alerts that relate to an individual's activity. Brå has also identified an opportunity to make greater use of measures that push people towards the secure alternative, known as nudging.
- Public actors at all levels should increase their support for people who need help using digital services, such as digital banking, digital social services and digital commerce. This applies in particular to municipalities, which have had a responsibility for crime prevention work since 1 July 2023 (in accordance with Act 2023:196).
- The anticipated effects of both technical and structural measures, as well as measures to strengthen potential victims, need to be evaluated and followed up on. Technical and structural measures should also be preceded by risk or vulnerability assessments. These assessments and evaluations should include analyses of any displacement of crime, as well as whether the measures involve any undesirable consequences, such as for groups who do not make use of new solutions or procedures.

[1] An authorised transaction is when the victim is tricked into carrying out a transaction themselves.