Fraud crime in Sweden

Report 2016:9

Authors: David Shannon, Klara Hradilova Selin, Johanna Skinnari and Linda Hörnqvist

urn:nbn:se:bra-887

English summary

In 2014, the Swedish National Council for Crime Prevention (Brå) was instructed by the Government to conduct a study focused on fraud and the work to combat this type of crime. The reason given was that both victim surveys and reported crime statistics indicate that fraud is on the increase. One important factor behind this trend is that technological developments have made it possible both to commit new types of fraud and to engage in fraud offending on a much larger scale. Against this background, the Government's instruction to the National Council stated that new knowledge is required in order to improve the work to combat fraud. The types of knowledge needed include knowledge on the nature of different types of fraud crime, on how the agencies of the justice system work to investigate and prosecute fraud, and on what types of preventive measures might be effective.

Definition of fraud

Stated in somewhat simplified terms, Chapter 9 of the Swedish penal code defines fraud as involving an offender deceiving someone into transferring something of value to the offender. With certain exceptions, benefit fraud is no longer dealt with as a penal code offence in Sweden but is instead regulated in the Benefit Crime Act (Bidragsbrottslagen 2007:612).

Method

The National Council's study is based on an analysis of four principal data sets:

- Statistical data drawn from the Swedish Crime Survey (SCS) and from official crime statistics for the period 2008–2014/2015.[1]

[1] Statistics relating to offences reported to the police are presented for the year 2015. At the time of writing, however, these statistics remain preliminary.

- Cases of fraud reported to the police (a sample of police reports and police investigations into fraud).
- District court judgements.
- Interviews with relevant actors from the justice system, other public sector agencies and the business community, and with offenders.

Fraud levels on the rise according to different sources

During the years since 2008, levels of fraud have increased in terms of both self-reported exposure to fraud (according to the SCS) and the number of fraud offences dealt with by the criminal justice system. In 2015, a total of 170,000 cases of penal-code fraud were reported to the police in Sweden. According to both the SCS and official crime statistics, large increases have been observed in both online fraud and payment card fraud. The SCS, which captures exposure to crime among the public, but not among businesses, shows that it is primarily women who have reported increasing levels of exposure to fraud. In the SCS survey for the year 2014, the proportions reporting exposure to fraud were largely the same among women and men (at approximately three percent).

The number of benefit fraud offences reported to the police has been more stable. A little over 9,300 such offences were reported in 2015, a figure which is largely the same as the number reported in 2008. One important difference by comparison with penal-code fraud is that the number of registered benefit fraud offences is entirely dependent on the level of resources that the relevant agencies and organisations devote to control activities, and on which incidents they themselves choose to report to the police.

Five principal types of reported penal-code fraud

On the basis of a sample of police investigation files from 2013, five principal categories of reported penal-code fraud have been identified. A total of approximately three-quarters of the penal-code fraud offences in the National Council's sample may be said to be part of some kind of purchase or sales process. *Payment card fraud* constitutes the single largest category of offences (22 percent of the sample). Here the offender uses another person's – often stolen – payment card or card-data to make illicit purchases or cash withdrawals.

The second largest category (17 percent) comprises *Credit fraud*, which most commonly involves the offender purchasing goods or services on credit, or taking a loan, in somebody else's name. In most cases, these offences involve identity abuse (e.g. in the form of identity theft), while companies with good credit ratings are used to commit large-scale credit fraud.

A third category, of approximately the same size, is comprised of cases involving *Online auction fraud*. These offences involve the offender using an online auction site to mislead an interested buyer by offering goods or services for sale or rental. Once the payment has been made, however no goods or services are delivered.

A fourth category of penal-code frauds takes the form of *Invoice fraud* (12 percent of the sample). Here the victim is misled into pay-

ing an invoice for goods or services that he or she has not ordered. These offences may involve completely fake invoices, or invoices that have been sent following some form of prior contact (e.g. in the form of telephone sales), in which the recipient of the invoice has been misled into entering into a contract with the sender.

The fifth category of penal-code frauds has been labelled *Other telecom- and internet fraud*. This category includes a range of different types of modus in which fraudsters employ malware or contact their victims by phone or online. These types of fraud do not belong to any of the previous categories, but are sometimes a means of e.g. obtaining the data required to commit another type of fraud. Phishing is often used as a means of obtaining card or account data, for example. Many of the police reports in this category do not relate to completed fraud offences, but rather to attempted or preparatory offences.

Typical benefit fraud involves providing incorrect information

A typical offence against the Benefit Crime Act involves the offender providing incorrect information, thereby misleading the agency or organisation concerned to issue benefit payments to which the offender is not entitled. These offences may also involve the offenders failing to report relevant changes in circumstances and as a result receiving benefits that they are no longer entitled to. The largest public sector agency in terms of transfers, the Swedish Social Insurance Agency (Försäkringskassan), is also the agency that reports the largest number of offences. Thereafter come the municipalities and the unemployment benefit funds. The Benefit Crime Act only covers benefits paid to individuals, but the actors of the welfare system are also the target of other types of fraud. Fraudulent applications for various types of financial support to businesses, which are primarily paid by the Public Employment Agency, and also certain other types of fraud against the Social Insurance Agency, are dealt with on the basis of the fraud provisions in the penal code.

Internet central to many fraud offences

The National Council's study shows that the internet plays a role in relation to all of the identified fraud categories, either as a facilitator or as the forum in which the offences are committed. The internet is a precondition for *online auction fraud*, and its role in relation to *payment card fraud* and *credit fraud* is clearly visible in the offences that are committed within the framework of e-commerce. However, the internet is also used both prior to and subsequent to these types of fraud crime. Cyber-attacks are employed to steal payment card data, for example, and there is an online black market for stolen information that can be used in both *payment card fraud* and *credit fraud*. Following these types of crime, internet auction sites also provide a forum for the resale of goods that have been purchased fraudulently using stolen data.

The role of the internet in relation to invoice fraud can be seen among other things in the way that some of these fraud schemes employ e-mail contacts to deceive the victims into believing they have entered into a contract with the issuer of the invoice. In addition, many of the police reports on invoice fraud examined by the National Council involved invoices that had been sent to businesses

with demands for payment for various forms of questionable or non-existent internet-related services.

Many of the offence types included in the category *Other telecom and internet fraud* would not be possible without the internet. Examples include fraudsters using various forms of malware or phishing attacks to obtain information that is then used to access bank accounts. Another example involves fraudsters hacking into individuals' e-mail or social media accounts, and then sending messages to these individuals' contacts to deceive them into sending money or revealing sensitive information.

Identitety abuse an important part of many types of fraud

Different forms of identity abuse can be seen in all of the categories of fraud crime identified in the National Council's study. The study shows that some form of identify abuse is used in relation to a large proportion of the penal-code fraud offences that are reported to the police. False identities and other forms of identity abuse may also be employed in the context of benefit and other frauds against the welfare system, e.g. in the form of falsified signatures on medical certificates or certificates of employment, or in the form of applications for subsidies for fictional employees.

Information from a number of private sector actors and from the police shows that the illicit use of others' identities in order to commit fraud is a growing problem. The problem involves not only the use of stolen identities but also entirely falsified identities with no links to real individuals. In both cases, the frauds are committed by offenders pretending to be other people. The objective is usually to conceal possible leads that might lead to the identification of the offender, or to obtain the trust of potential victims, e.g. by pretending to be a friend or acquaintance. The deception may be carried out with the help of fake, stolen or manipulated identity documents (e.g. when collecting or accepting delivery of items purchased online using someone else's identity) but some frauds need not require identity documents (e.g. when fake contact details are used in connection with online auction fraud). In addition to the abuse of private individuals' identities, frauds are also committed via the abuse of the identities of businesses or other organisations.

Younger adults more exposed to fraud, but the elderly a particularly vulnerable group

The victims of fraud include members of the public, businesses and public sector agencies and organisations. According to the Swedish Crime Survey, age and sex differences among those exposed to fraud have become less marked over time. In 2014, women reported the same level of exposure to fraud as men, having previously consistently reported lower levels, and levels of reported exposure have increased among adults aged 45-54, by contrast with earlier years when exposure to fraud was consistently higher among younger adults. Although younger adults appear to experience higher levels of fraud crime than the elderly, the latter group nonetheless constitute a particularly vulnerable group in relation to certain types of fraud. In the National Council's study this was found to be the case

in relation to certain types of invoice fraud and fraud using stolen payment cards.

Fraudsters: anyone from individuals in urgent need of money to knowledgeable entrepreneurs

The fraud investigations examined by the National Council contain relatively little information about the offenders. It is only in relation to the reported cases of online auction fraud that an offender had often been identified. One common motive for this type of fraud is an urgent need for money on the part of the offender, which means that the offences themselves are unsophisticated and the risk for detection is relatively high. Official crime statistics show that those convicted of penal-code fraud and benefit fraud are generally somewhat older than those convicted of penal-code offences in general. Among those convicted of benefit fraud, the proportion of women is significantly greater (at over 40 percent) than that found in relation to other types of crime. In addition, those convicted of benefit fraud are less likely to have prior convictions compared to persons convicted of penal-code offences.

The National Council's interview data contain descriptions of a range of different types of fraud offender, including individuals with high levels of legal and business knowledge. These individuals are often involved in more sophisticated types of fraud, and often work in a grey area between legal and illegal activities. In those cases where individuals are convicted of involvement in frauds of this kind, they are usually frontmen or persons who have facilitated the offence in various ways, rather than the principal offenders.

The role of the business community

Businesses play an important role in the context of fraud crime. In addition to being victimised by fraud, businesses are often used as a tool in connection with more organised and systematic fraud activities. The National Council's data include several examples of cases where businesses have been used to commit invoice fraud and credit fraud.

A lack of checks in e.g. payment or delivery systems also means that the business community plays the role of facilitator in relation to frauds committed against others. One central challenge for the business community is that of balancing demands to maximise sales against issues of conducting checks and maintaining high levels of security. The National Council's interviews with representatives from the commercial sector show that many businesses see a clear conflict between these two goals, and some level of fraud appears to be regarded as both inevitable and acceptable. There is also a view that honest customers feel that checks are burdensome and that increased levels of control lead customers to take their business to competitors. Interviews with both representatives of the business community and offenders also suggest that fraudsters direct their activities at companies that are perceived to have poorer security systems than their competitors. The business sector has a clear responsibility to work to prevent fraud crime, and the National Council's interview data suggest that there is considerable potential for improvement in this area.

Limited justice system resources, but positive developments

During the period since 2008, the police have assigned increasing levels of resources to the investigation of fraud crime. According to the National Council's interview participants, however, there remains a clear imbalance between the volume of fraud crime and the resources available for investigating and prosecuting fraud offences. This contributes to long investigation times and to a pressure to quickly discontinue investigations into offences that are unlikely to result in prosecution.

At the same time, the National Council's study shows a number of improvements in the justice system's work to combat fraud. One important development has been the establishment of a National Fraud Centre (Nationellt bedrägericenter) within the police, with the objective of improving the effectiveness of the justice system's work in this area. Interview participants from both the private sector and the justice system have emphasised that there have been substantial improvements in the police's coordination of fraud investigations and there are also clear signs of improvements in the ability of the justice system to investigate and successfully prosecute large scale, complex fraud cases involving several offenders and large numbers of victims. The number of fraud offences that have resulted in prosecution has increased. The official statistics also indicate an increase since 2008 in the number of convictions involving large numbers of fraud offences. The proportion of fraud convictions resulting in a prison sentence has also increased successively.

The district court judgements examined in the study illustrate that prosecuted fraud crime is often focused on serial offending. A little over 40 percent of the judgements related to the prosecution of cases involving at least 20 fraud offences, and just over ten percent of the judgments involved over 100 fraud offences.

Substantial varation in the conditions for successful investigation

At the same time as the number of fraud offences resulting in prosecution has increased, the results of the National Council's study show that this increase is likely to be unevenly distributed across different types of fraud crime. There is a substantial variation in the conditions for successful investigation and prosecution between different types of fraud. These conditions are relatively good in those cases where it is possible to follow transfers of funds to a bank account that can be linked to an offender, which is primarily the case in connection with online auction fraud and invoice fraud.

The conditions for investigating payment card fraud and credit fraud are less positive, however. In these cases, it is rarely possible to follow the money to a bank account, and in the case of many reported offences, investigations are either not initiated or are quickly discontinued because there is no prospect of identifying a suspect. The same is true in relation to the category *other telecom and internet fraud*. These offences are usually committed via the internet either from overseas or via servers located in other countries. In

addition, the offenders often exploit technological opportunities to block the attempts of law enforcement to trace the offenders.

In the case of benefit fraud, the identity of the offender is usually already known when the offence is reported, and the proportion of reported offences that result in prosecution is relatively high. The major challenge for police and prosecutors in these cases is that of proving criminal intent.

A rapidly changing field of criminal activity

The field of fraud crime is constantly changing, with the continuous emergence of new means of deceiving individuals, businesses and public sector agencies for personal gain. According to the National Council's interview participants, the electronic use of payment card data to commit fraud is currently the fastest growing area of fraud crime. According to information provided by the police, recent years have witnessed a number of large-scale data breaches, which have led to substantial amounts of payment card data being made available to fraudsters. This type of fraud is particularly difficult to prevent, since doing so requires international collaboration, expertise in the field of IT, and a greater desire on the part of the actors affected to improve levels of security. Another clear trend, according to interviewed experts, is that fraudsters are increasingly analysing data from social media profiles and using this information to more effectively target potential fraud victims.

The National Council's assessment

Areas for improvement in the justice system: more efficient handling of complex investigations

As has been noted above, recent years have witnessed improvements in the justice system's work in dealing with fraud. At the same time, the National Council would like to draw attention to a number of areas where there is a potential for further positive developments.

Some frauds result in extensive investigations that place substantial demands on the agencies of the justice system. This is particularly the case in relation to cases of large-scale invoice fraud and personal assistance benefit fraud. In the case of invoice fraud, the introduction of a new penal code offence, *gross invoice fraud*, specifically focused on this type of crime should improve the ability of the police and prosecutors to investigate these offences more efficiently.

A number of measures to improve the efficiency of investigations into cases of large-scale personal assistance benefit fraud have been proposed by the Swedish Prosecution Authority (Åklagarmyndigheten 2015). It is important that knowledge of these proposed measures is disseminated within the justice system and that the measures are also implemented in relation to the investigation of other types of fraud. It is also important to continue the work to identify further measures that may facilitate the justice system's work with complex fraud investigations. One important factor noted by the National Council's interview participants was a need for the police to improve processing times in connection with IT forensic analyses.

Improving competence, knowledge exchange and investigatory methods

The National Council's study found a widespread perception among interview participants that there was a lack of individuals with important types of expertise among police fraud investigation staff. These include individuals with expertise in the field of benefit fraud, and also individuals with the expertise required to analyse various types of evidence, including professional auditors. A general conclusion based on the National Council's findings is that there may be a need to review the nature the skill sets required for the effective investigation of fraud crime.

Frauds that are committed with the help of businesses may present special difficulties with regard to efforts to identify those responsible for the offences. This is because the principal offenders are often able to conceal themselves behind frontmen. Here the National Council's interviews indicate the need for a knowledge exchange between the police, who are relatively unused to investigating offences committed by businesses, the Swedish Economic Crime Authority and the Swedish Tax Agency, who have more experience of mapping the activities of companies used to commit crime. These agencies need to work together in order to obtain an overview of these types of fraud crime. For the same reasons, it is important for the work to combat fraud to become more intelligence-based in order to identify particularly active offenders, new types of fraud and also the types of businesses that are often used. In this regard, the private sector also has important knowledge to contribute to law enforcement efforts. Improvements to the justice system's ability to investigate benefit fraud can also be achieved by improving the quality of the reports submitted to the police by the relevant welfare agencies and organisations.

When certain types of fraud investigation, such as investigations into payment card fraud and credit fraud, are consistently discontinued quickly as a result of investigatory problems, it becomes difficult to identify opportunities for improving investigative strategies and techniques. Work to improve the investigation of these types of fraud offences should therefore be a priority, not least in order to identify new ways of identifying unknown offenders. The use of more detailed crime codes when registering offences would also make it easier for justice system actors to follow trends in important types of fraud, and also to identify areas that may need to be prioritised.

Improved prevention more important than better prosecution rates

Although there are opportunities for further improvements to the work conducted by the justice system, it is important to be aware that the problems associated with fraud crime cannot be resolved exclusively through the investigation and prosecution of these offences. The volume of fraud crime is so great that it cannot reasonably be matched by sufficient investigative resources. The most important efforts to reduce fraud crime must therefore be focused on prevention work in society at large.

Fraud crime affects a large number of different actors, who all have substantial opportunities to work to prevent fraud, but at present other interests appear to be viewed as more important. This is the case in both the private and the public sector.

Easy sales and good service versus control and security

Both welfare agencies and businesses face the same dilemma of balancing the desire to provide a quick and efficient service or sales with the goal of ensuring security and reducing levels of fraud.

In order to avoid losing customers to competitors, security issues are not given a sufficiently high priority in the commercial sector. One of the most important fraud prevention measures in the private sector would thus be the development of sector-wide solutions that avoid customers moving to businesses with lower levels of security. This also requires a greater awareness that businesses also have a social and ethical responsibility in relation to fraud crime, not least since there are indications that the some of the proceeds are employed to finance continued criminal activities. There is thus a need to review possible ways to address the balance between security and other, conflicting interests; the increased use of biometric data in connection with payments constitutes one example.

As regards welfare fraud, the National Council suggests expanding, and an increased use of, the opportunities that exist for information sharing among the agencies of the welfare system. Some of the interviewed representatives of government agencies and the private sector felt that it was problematic that their primary work descriptions did not include a focus on preventing and combating fraud, even though their work included a certain level of control activities. Their everyday tasks gave them insights into a range of vulnerabilities that could be exploited for the purposes of fraud, and they felt that more measures could be taken.

Improving the security of the sales and delivery process

A large proportion of the reported penal-code fraud offences examined by the National Council, approximately three-quarters, were found to take place in the context of some kind of sales or purchase process. An increasing proportion of retail sales are taking place online, which means that the goods must be delivered to or collected by the buyers. At all stages of this process, from the order being placed, possible credit checks, to delivery and collection, there are security vulnerabilities that may be exploited by fraudsters. Interviews with representatives of both the justice system and the business community indicate that the principal focus for preventive work is currently being directed at the point at which goods are finally delivered to or collected by the customer, primarily because this is the point at which it becomes possible to conduct a physical identity check.

It is important, however, to work to prevent fraud at as early a stage of this process as possible. The work to prevent fraudulent purchases should therefore direct a greater focus at measures to ensure secure online ordering. A number of the interviewed representatives of the business community advocated an increase in the use of digital identity controls. At the same time, it will continue to

be essential to ensure that the person who collects the purchased item, or to whom it is delivered, in fact represents the individual who has supposedly ordered and paid for the items. Thus security measures at collection points also need to be given a higher priority. One key factor in creating better incentives for different actors to improve their security checks is to introduce greater clarity regarding who is responsible for ensuring the security of different phases of the sales and delivery process.

A parallel may also be drawn to agencies and organisations working in the benefits system. Some of these agencies, such as the Social Insurance Agency, have come a long way in developing methods for checking welfare payments, with a focus not only on payments that have already been made, but also on working to identify suspected benefit fraud prior to any money being transferred. Continued efforts towards this end are also essential.

A joined-up approach required in relation to secure identification

Most types of fraud involve the use of a false or stolen identity to some degree, including benefit fraud. Pretending to be someone else is a common strategy. In Sweden, factors that facilitate the use of false or stolen identities include the high number of acceptable forms of confirming one's identity, something which makes identity checks difficult, as well as the fact that it is relatively easy in Sweden to obtain personal information relating to others from public agencies such as the Swedish Tax Agency. The assessment of the Swedish National Council for Crime Prevention is the same as that of many representatives from the business community, namely that a single central actor should be given overall responsibility for all phases of the issue and control of personal identity documents, including the application process, background checks of applicants, the production of identity documents, the issuance of these documents and also the process of subsequently verifying the authenticity of such documents. Individuals should be required to both apply for and collect identity documents in person. Interview subjects in the National Council's study also advocated the importance of reviewing the regulations regarding the ease with which it is possible to obtain personal information relating to others as a result of the way the principle of public access to official records is implemented in Sweden.

New legislation on the unlawful use of another's identity will cover some of the acts that constitute important elements in fraud offences, but the use of completely false identities (with no connection to existing individuals) is not covered by the new legislation. The National Council's study shows that some individuals are currently able to register and make use of multiple identities in Sweden; it is therefore essential to guarantee that the initial registration of an identity at the National Tax Agency or the Swedish Migration Agency is secure, i.e. that a single person can only be registered in connection with a single identity, and vice versa.

Payment card fraud a particularly serious problem

According to a number of different sources, there has recently been a rapid increase in the number of frauds being committed using stolen

payment card data. As with many forms of internet-related crime, preventing these offences poses major challenges. The offenders often have access to technical expertise, and the data are often stolen by means of advanced data breach offences. Representatives of the justice system emphasised that banks and online retail businesses need to assume more responsibility in this area. Important developments include the use of secure electronic identification and the default restriction of card payments to the cardholder's country of residence. Members of the public also need to be informed about how to protect themselves against data breach and how to make secure online purchases, even if it may take a few seconds longer. There is much to suggest that substantial long-term efforts will be required to improve the prevention of fraud based on stolen payment card data and that international cooperation will be essential.