Annual Fraud Report 2022

DNB Financial Cyber Crime Center (FC3)

Fraud continued to be a threat to DNB and our customers in 2022. The year brought with it a 38% increase in attempted fraud to a total of 1,242 million NOK, cementing the fact that fraud is the crime people are most likely to encounter. Despite the significant increase in fraud, losses remained stable. Put simply, more people have been attacked for more money, but we have also been able to block more fraud.

A change that became apparent in 2022 is that threat actors mix both attack vectors and types of fraud. This makes fraud cases much harder for potential victims to identify.

Phishing has become the main activity for several threat actors, and as criminals focus and specialize on this type of fraud, so do counter fraud professionals. Despite a massive increase in activity in this area there is no indication that other fraud types are declining. Much of the phishing increase can be attributed to automation of parts of phishing attacks misusing familiar brand names and logos to defraud large groups of people at the same time. In turn this pushes the need for automation over on counter fraud environments where a lot of efforts are now being made to automate more of the counter fraud response, allowing us to disrupt and prevent attacks at an earlier stage.

The connection between fraud and organized crime that only a few years ago was in dispute is now quite clear. In addition to this, the connection between criminal groups involved with financial crime and other more classic organized crime activities is becoming more obvious and well documented. Both Swedish and Norwegian police have released several reports highlighting these issues.[i]

Raising awareness of fraud remains an important tool in combating financial crime, and there appears to be an increased focus from police, financial institutions, and the media in this area. Giving advice, keeping the public informed of current threats, and giving insight into the work being done to prevent fraud is a central part of the counter fraud work.

The dramatic increase in cases year on year brings with it another issue, namely that of fraud fatigue. A massive increase in fraud, number of victims and professionalization of criminal actors has quite simply stopped being sensational and has instead become expected. Though this does not affect the counter fraud work in professional environments, it does make efforts to raise awareness and other preventive measures much harder.

Summary of 2022

In 2022 we prevented 1,066 million NOK out of a total attempted 1,242 million NOK. This is an increase of 38% from 898 million NOK attempted in 2021. This increase is matched by improved detection resulting in a fraud loss of 176 million NOK which is comparable to those in previous years. The total amount attempted stolen is slightly lower than in 2020, but this is mainly due to a difference in reporting.

Approximately 60% is card fraud and 40% is digital fraud including the use of payments from DNB accounts initiated outside DNB using PSD2-APIs.

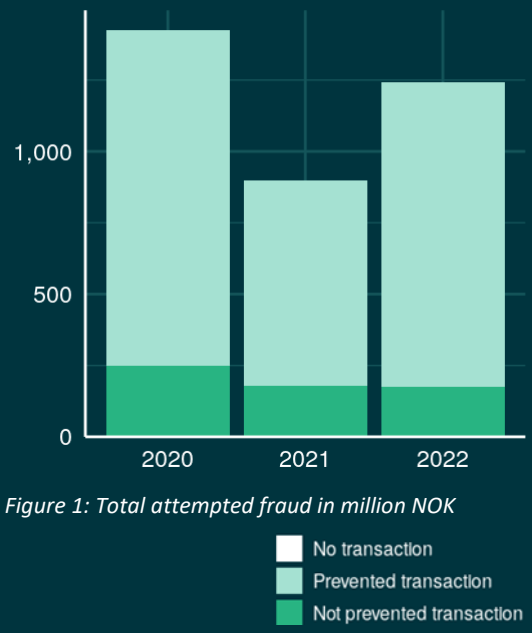

Figure 1: Total attempted fraud in million NOK

Digital fraud summary

In digital channels, we recorded 9,291 cases (for 4,608 customers) which is an increase of 45% from 6,391 cases in 2021. The attempted amount stolen is 496 million NOK which is an increase of 57% compared to last year. Out of this 408 million NOK is prevented which is 82 % of the attempted amount. The large increase in fraud cases is primarily due to a rise in phishing cases which started in 2021 and has continued throughout 2022.

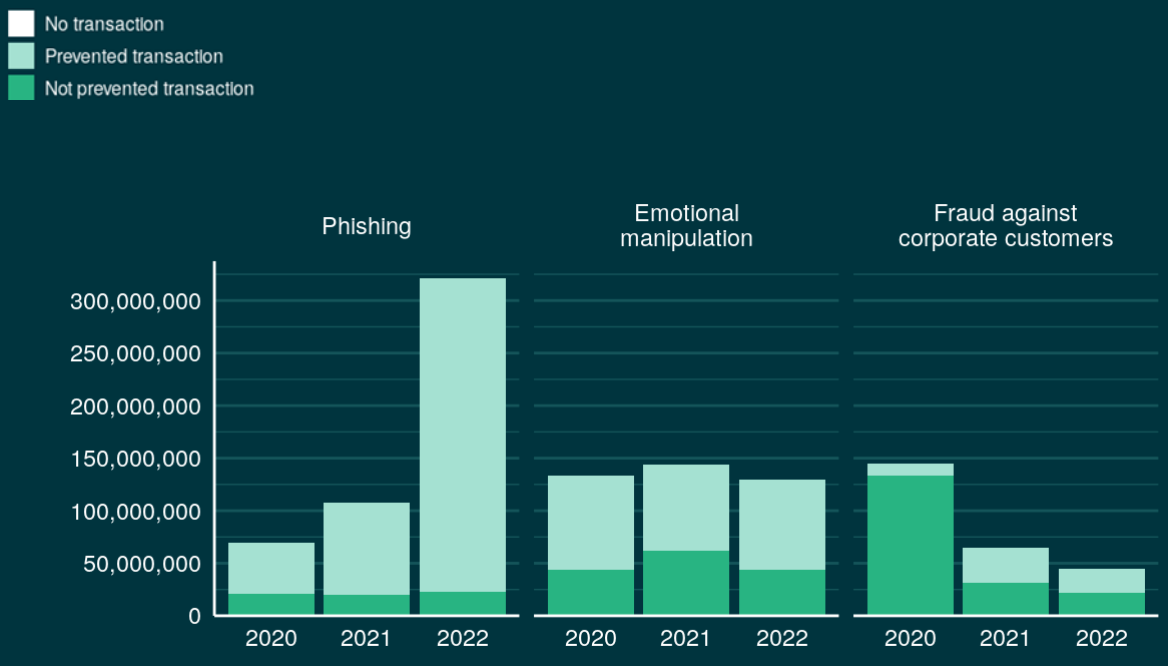

Figure 2: Attempted fraud in digital channels for phishing, emotional manipulation and against corporate customers.

Fraudsters continue to quickly adopt new technology. Since 2021, the number of cases involving payments initiated outside DNB using payment APIs have increased by more than 400% and now accounts for 20% of the digital fraud cases. DNB online banking is still the main channel with over 50% of the cases, probably because this channel is the most used for cross-border payments. Many cases also still involve misuse of legitimate payment service providers, neo banks and crypto trader platforms.

In recent years, we have seen an increase in the use of Norwegian money mules. We see a clear and concerning pattern of fraud victims later becoming involved in money laundering as money mules.

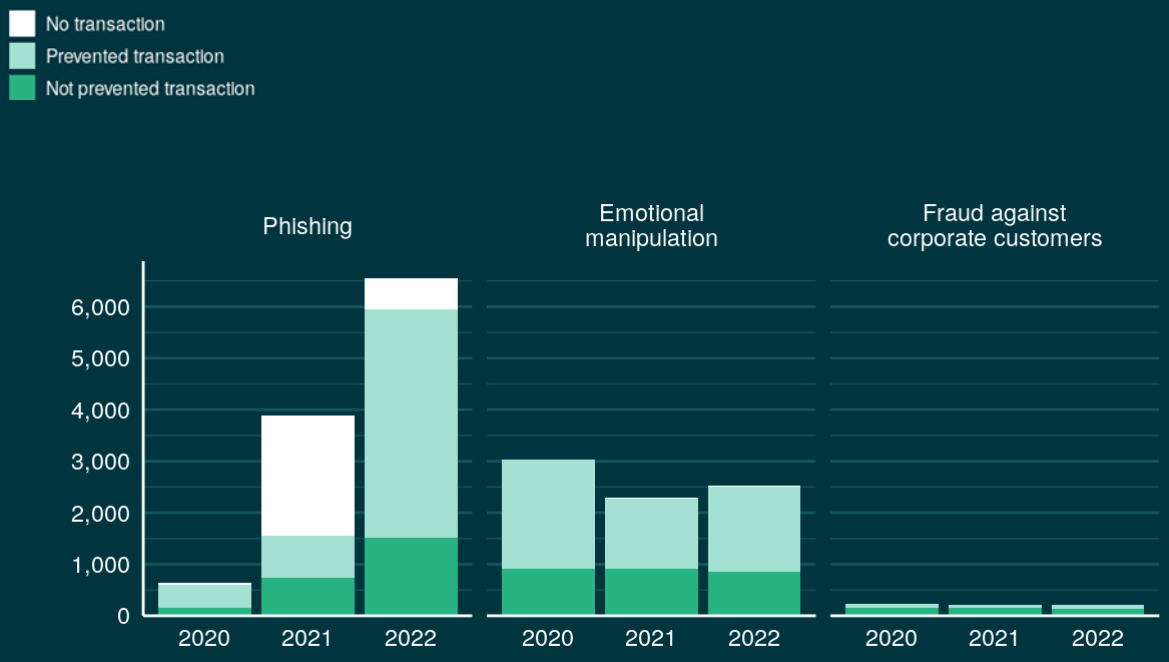

Figure 3: Number of fraud cases in digital channels for phishing, emotional manipulation and against corporate customers

Phishing dominating the fraud threat landscape

In 2022 we investigated 6,550 cases related to phishing, this now accounts for 70% of the fraud cases in digital channels. This is an increase of 69% compared to 3,887 cases in 2021 and 920% from 642 cases in 2020 which makes phishing the main driver for the rise in fraud cases.

With automated systems and monitoring, we often block fraud attempts early in the phishing process. In those cases we use a standard value for potential loss, based on the average loss in similar cases over years. We estimate a potential loss of 120,000 NOK. Including this estimate, the amount attempted stolen in different types of phishing campaigns amount to 321 million NOK. This is only cases registered in our infrastructure and does not include the potential attempts divulged by our customers.

	Fraud cases	Attack sum
Phishing (SMS, email, SEO)	4,413	231,385,000
Vishing	832	35,445,000
SoMe phishing	1,097	29,210,000
Spear phishing	127	19,815,000
Fake support	86	5,525,000

Phishing can take many forms. Traditionally the victim receives an email, but we have seen a clear shift towards use of SMS, social media (especially Messenger/Facebook) phone calls (vishing) and misuse of marketplace apps.

Phishing targeting people advertising on marketplaces such as Tise and Finn has become commonplace. The seller of an item receives an SMS from the buyer after a purchase, telling them to follow a link to receive the payment.

There is still a lot of vishing targeting elderly customers where the victim is called from what appears to be the police or bank and persuaded to give away credentials, resulting in their accounts being emptied. The ability to call from what appears to be a legitimate phone number belonging to someone else is known as spoofing and Telenor reports that they blocked 30 million such attempts in Norway in 2021.[ii] DNB has in cooperation with telecom companies installed countermeasures to avoid spoofing of DNB official phone numbers. This reduces the fraudster's ability to misuse the DNB brand in SMS phishing, but many other brands that normally require BankID to log in or make payments can still be misused.

Many threat actors target the brands of DNB and other financial institutions, but there has been a clear decrease in phishing targeting the DNB brand in 2022.

SoMe phishing (social media phishing) is using a hacked social media account to contact friends of the victim with various scams. Though the stories vary, the result is victims giving away their credentials to the fraudsters. In these cases, publicly available information from social media accounts has been used to manipulate the victims to transfer money.

Spear phishing is a form of phishing targeting specific individuals. In 2022 criminals focused on targeting individuals with a role in a company that newly made changes that have been publicized in The Brønnøysund Register Centre. Typically, this has been companies which have newly changed accountants. The contact person in the firm has received a call from "the new accountant" telling them they need to sign a document regarding the change or authorize something with BankID. This targeted phishing uses real and current information that is specific to the target and is therefore very effective.

Emotional manipulation as a tool to commit fraud

Emotional manipulation includes fraud like romance fraud, investment fraud and advance fee fraud and is based on manipulating the victims' emotions, usually by creating a relationship of trust. This type of fraud previously accounted for most fraud cases and while the volumes are not as high as for phishing, these more traditional fraud scenarios remain at stable levels. In 2022 we registered 2,530 fraud cases of a total of 130 million NOK. This year we have seen a shift towards hybrids of these categories.

	Fraud cases	Attack sum
Investment fraud	1,008	82,384,000
Romance fraud	541	19,609,000
Advance fee fraud	298	9,873,000
Other manipulation of retail customers	683	17,977,000

Criminals have become more willing to combine different types of fraud. A common example of this is where fraud starts out as romance fraud, where criminals attempt to create a close and personal relationship with their victims, and then changes direction into an investment fraud. The criminals use the personal connection to their victims to advise them on how to invest. This has led to a muddying of the waters around advance fee fraud, investment fraud, the recovery phase of investment fraud, and romance fraud. Cases do not need to involve romance but can be based on friendship or a charitable act. For example, the criminals can pretend to be victims of the war in the Ukraine who need financial aid.

Investment fraud is still prevalent and the modus where criminals persuade the victim into making transfers to legitimate crypto trading platforms continues. It can be challenging to distinguish

legitimate cryptocurrency investments from fraud. Fraudsters take advantage of the hype and less regulated environment surrounding crypto currency to pressure victims to let them invest on their behalf. These fraudsters in some cases also use remote access tools to control the victim's computer and online bank accounts

Fraud against corporate customers remains stable

There are mainly three types of fraud targeting corporate customers specifically: Fake invoices, CEO Fraud and Beneficiary Account Change Fraud (BAC).

	Fraud cases	Attack sum
BAC	87	33,284,000
CEO fraud	40	4,030,000
Fake invoice fraud	16	3,155,000
Other manipulation of corporate customers	63	4,597,000

Fake invoices are generally mass produced and are often sent to smaller organisations like sports clubs who may have a lower level of security or public information which can be misused by fraudsters to gain trust.

CEO fraud is usually perpetrated by email and the criminals pretend to be from another person in the firm, often CEO or CFO to an accountant in the firm, telling them to make a payment. CEO fraud is not only directed at large companies, but also smaller volunteer organization such as sports teams, local political groups, and dog clubs.

Beneficiary Account Change fraud is more sophisticated as the fraudsters in these cases have access to email accounts or other systems allowing them to send emails from legitimate addresses, negating the need for spoofing. This allows them to have access over time and through observation of routines and normal payments, change relevant payment information at the most crucial time.

In 2022 we had a similar level of fraud cases targeting corporate customers as in 2021, with 206 cases. These cases are generally larger with 219,000 NOK per case totalling 45 million NOK. However, we believe that the actual amount is higher due to fewer cases being reported by corporate customers. There are potentially several reasons for this, for example companies keeping losses secret to avoid reputational damage. But if more fraud was reported, it would improve both fraud prevention and prosecution.

Credit fraud and organised crime

As fraud becomes one of the most lucrative activities for organised criminal groups, credit fraud remains a low risk, high reward criminal activity. One of the reasons for this is the fairly low chance of being caught and successfully prosecuted.

As previously reported in last year's annual fraud report, there are criminal elements in Norway with a connection to organised crime abroad behind many of these cases, and particularly criminal groups in Sweden and Norway cooperate closely. Fraud connected to the financing of vehicles is well organised and the vehicles are quickly moved abroad where foreign criminal networks are waiting to receive them. The vehicles are then swiftly registered to new owners, often via car dealerships.

We are seeing more examples of criminals taking control over companies to commit fraud and there are clear connections to bankruptcy crime and labour crime. The criminals will often put their own people inn as managers or board members and drain a company for assets at the same time as they take up and move loans and credit. These criminal activities in turn finance other forms of crime and there are clear connections to money laundering, narcotics, and human trafficking.

There is an increase in the use of violence and threats of violence with these fraud types, often in combination with ID theft. They often take advantage of the lack of computer literacy, resources, and the lack of cooperation across borders.

Future developments

While it is certain that we will continue to see new developments in the fraud landscape in the coming year, it is uncertain exactly what should be expected. It is highly likely that threat actors will continue to exploit digital innovations to their own advantage. With the introduction of advanced artificial intelligence, machine learning, and deepfake technology, it is just a matter of time before more and more threat actors embrace the technologies.

Although limited, organized criminals have for some time been experimenting with the use of deepfake technology not only towards individuals, but also companies. In romance fraud and investment fraud, deepfakes are used to represent a fake persona through video communication, images, or voice calls. By using such technology, it is possible for the criminals to completely alter their voice, face, and behaviour. This inherently contribute to building trust with the victim. For fraud targeting companies, the same technology has previously been used to represent a business partner, a superior, or the company's executive management. All with the intent of building trust and deceiving the recipient with the intention of defrauding them or making them conduct seemingly harmless actions. Even though these techniques have only been used in some cases until now, it is likely that an increasing number of threat actors will use them on a regular basis as the technology becomes more readily available.

With the introduction of ChatGPT, advanced language models are intertwined with artificial intelligence to produce seemingly flawless messages without human input. If desired, one could ask a robot to create efficient and correct phishing messages or to set it up to chat with unsuspecting victims of for instance romance fraud. For the victim, it would be extremely challenging to understand that something unpleasant is going on in the background. The robot does after all answer seemingly correct and sophisticated to each question or topic introduced by the victim.

Some threat actors have already started discussing how to best use this new technology with criminal intent, and it is likely that some will apply it in fraud cases in near future.

At the same time, the simplest solutions are often most efficient. This also applies within criminal communities. It is highly likely that threat actors will continue to use similar tactics, techniques, and procedures as those seen throughout 2022. This means that less sophisticated and mass-produced phishing attempts, email distribution techniques, or social media-based approaches are likely to remain relevant.

Based on global tendencies, it is nevertheless easy to assume that we will continue to see high levels of fraud targeting both DNB and our customers in the coming year. We also know that whenever new global events arise or whenever there is a surge of uncertainty or instability, threat actors are among the first to adapt. While it is impossible to always be one step ahead, this highlights the importance of staying updated and being ready for changes that could arise at short notice.

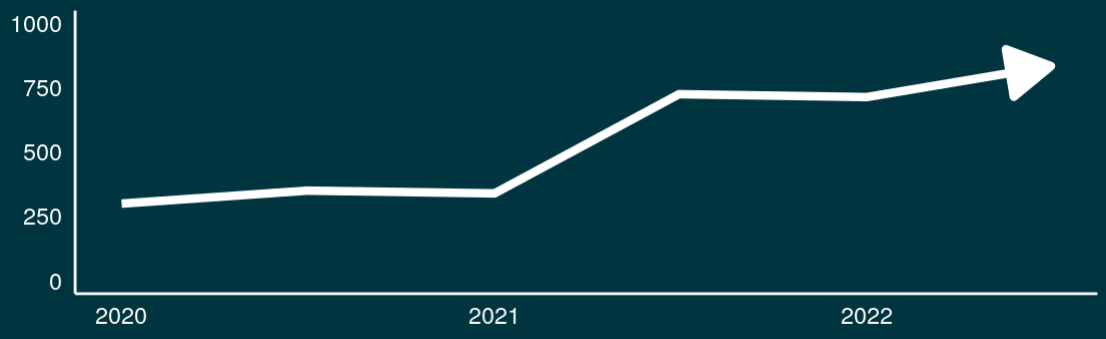

Figure 4: Over the years the number of fraud cases are steadily rising.

[i] https://polisen.se/aktuellt/nyheter/2022/december/narmare-halften-av-de-inblandade-i-det-dodliga-skjutvapenvaldet-kopplas-till-bedrageribrott/

[ii] https://www.dagsavisen.no/nyheter/innenriks/2023/01/18/telenor-advarer-mot-mer-proffe-svindlere/