ØKOKRIM

THREAT ASSESSMENT 2020


DIGITAL DECEIVER

Introduction

ØKOKRIM is tasked with protecting values important to Norwegian society by combating financial and environmental crime. Investigating and prosecuting criminal cases is a cornerstone of this work, but ØKOKRIM must also identify and assess relevant threats and trends.

This threat assessment will guide ØKOKRIM's future efforts, both as regards assigning priority to criminal cases and in developing our own prevention efforts. This also applies to our work with the police districts and other actors in the public and private sectors in Norway and abroad.

We hope that our threat assessment will be of interest to other agencies and stakeholders. The world is becoming increasingly complex and constantly changing and we can only protect values important to society – protect our welfare state–through extensive cooperation. We extend our thanks to our partners for providing information used in this assessment.

This year, we have linked the threats to key drivers in the current crime situation: the overall trends globalisation, sustainability, virtualisation and the pandemic. The threat assessment is, however, not intended to provide an exhaustive description, and threats and trends not mentioned here may still be important.

Over the past month, the world has changed in ways we did not predict, and we cannot yet say how the coronavirus pandemic will affect society and crime. However, we believe we can say that the pandemic and other factors impacting the economy will cause a noticeable financial crisis. Experience has told us that such crises bring financial and environmental crime that may test our trust-based welfare state.

In one year, or even sooner, our daily lives may have changed radically, but we still believe our assessment provides a relevant description of recent and expected developments in financial and environmental crime.

Threat assessment 2020, ØKOKRIM
Graphic design: Mona Lisa Iversen, ØKOKRIM
Foto: iStock og Pixabay
Circulation and print (Norwegian version): 1000x, Stapels

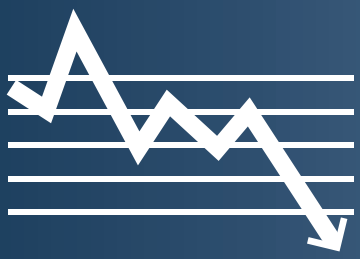
Key findings

1. Globalisation

- Large sums are transferred from Norway every year. Some of that money is likely to be sent to terrorist organisations abroad.
- It is likely that fictitious invoicing, incorrect pricing and use of false and forged documents take place in connection with fish exports, and that these activities facilitate financial crime, including tax fraud, accounting offences and general fraud, and that they camouflages overfishing.
- Increased prosperity globally is presumed to generate increased demand for electronic goods. Illegal export of electronic waste is therefore likely to continue.
- The removal of restrictions on the use of third-country nationals as labour will most likely result in increased exploitation of such workers in the coming years.

2. Sustainability

- The climate changes are escalating faster and impacting us harder than previously expected. Loss of biodiversity is considered one of the largest threats facing the world.
- Increased maritime traffic along our coasts is likely to raise the threat of marine pollution and dumping of plastic in the ocean.
- Tax evasion, work-related crime and abuse of public funding schemes cause large annual losses to the state treasury and threaten the financing of the welfare state.
- Tax havens will continue to be used to evade significant amounts in taxes from Norwegian authorities.



3. Virtualisation

- Financial crime carried out digitally has a global reach, and criminal actors can easily target a large number of victims. Digital financial crime can cause major losses to individuals and enterprises and is difficult to investigate and prosecute.
- Increased use of new, digital payment services and neo-banking, also among criminals, will make it increasingly harder to trace transactions.
- Deepfake technology is expected to be used to defraud Norwegian enterprises, and the number of enterprises suffering losses from such fraud is expected to increase.

4. Pandemic and economic uncertainty

- The coronavirus pandemic and raised economic uncertainty have created opportunities for criminals seeking to exploit the vulnerable situation we are in.
- The pandemic and its economic consequences will be exploited to defraud both individuals and enterprises.
- The compensation schemes aimed at business and industry are likely to attract profit-motivated criminals. The coronavirus pandemic is also likely to result in an increase in unemployment benefit fraud.
- Reduced detection risk in connection with bankruptcy crime, both during and after the coronavirus pandemic, will probably be exploited by criminal actors.

1. Globalisation

National boundaries have become less important in many areas. Norwegians shop online on foreign websites, paying through foreign payment services. Norwegian enterprises are establishing themselves abroad, and foreign enterprises compete for contracts in Norway on the same terms as domestic enterprises. Cross-border activities are becoming increasingly common and financial transactions quicker.

For Norway, globalisation has led to access to cheaper goods and commodities from abroad, contributed to lower inflation, and secured Norwegian industry and Norwegian consumers access to a wide range of components, goods and raw materials. Cheap imports have, on the other side, led to Norwegian businesses going bankrupt and to the loss of Norwegian jobs. Place bound national businesses, who have large parts of their value chain locally, often have larger costs related to labour and taxes than their foreign competitors and are at risk of going bankrupt or being purchased or merged with global groups.

A decreasingly small number of large corporations now dominate entire value chains and sectors. Large companies and funds have become key players in the globalised economy. It is a challenge that international law does not pose the same requirements to companies as it does to states.

In the global business models of multinational corporations, production is often fragmented and moved to areas with low labour costs and low environmental standards. With raw materials being extracted in one location, processed in another and the components assembled in a third, the transport alone has a major impact on the environment.

The practice of beaching highlights one problem of globalisation. 469 out of 674 vessels decommissioned in 2019 were scrapped on the beaches of India, Pakistan or Bangladesh,[1] with poor safety for workers and unsafe handling of hazardous waste. Scrapping vessels sailing under the flag of an EEA member state in those countries is not permitted, and it is not permitted to export decommissioned vessels sailing in EEA waters to those countries, even if the

[1] NGO Shipbreaking platform, «2019 Annual list of ships scrapped worldwide», 2020.

flag state is not European. From a financial perspective, the shipping companies have a strong incentive to scrap decommissioned vessels on the Indian subcontinent, where the price of steel is generally higher. It is therefore likely that illegal scrapping will continue to occur.

A more international business sector also results in increased foreign ownership in Norwegian enterprises and more foreign enterprises with activities in Norway. If foreign enterprises use foreign contractors, weakened domestic expertise and fewer local business development opportunities may result. There is also a risk that foreign acquisitions of Norwegian enterprises will result in lower taxable profits in Norway and jobs and technology moving abroad. It is also a problem that foreign organised criminals can buy up in Norwegian companies, as witnessed in the fisheries sector.

However, a stronger focus on national priorities among several of the larger economies is now challenging the global economy, which is based on low trade barriers, strong global investment and responsible state finances. Sovereign states are to an increasing extent taking a unilateral perspective on opportunities and problems, with trade becoming an instrument of rivalry.[2] Brexit[3] is one example of this, and the coronavirus pandemic is also being handled mainly at a national level.

The international economy and the global community are also changing as a result of the growth of developing economies, while digital technology is redefining what it means to exercise global power. Artificial intelligence, for instance, has become a new arena for competitive geo-politics.

Reduced global efforts and more competitive geo-politics pose problems in a world where societies are increasingly digitalised and virtualised. There is need for a multilateral effort to handle new challenges in digital security and digital financial crime, such as fraud.

---

2 World Economic Forum, «The Global Risk Report», 2020.

3 Great Britain left the EU on January 31th 2020.

Cross-border crime

With increased globalisation and integration of economies follow problems relating to cross-border crime and actors. We know little about what the large amounts transferred out of Norway every year are used for, and it is particularly problematic that many of the major fraud actors targeting both private individuals and enterprises operate from abroad.

In a global economy, professional money launderers with an international scope will also be a problem. These actors range from individuals to loose-knit networks to well-run organisations offering expertise on how to launder money and exploit regulatory loopholes. Such actors are rarely exposed when the primary offences[4] are investigated.[5]

Trade across national borders offers a significant potential for making illicit gains through deliberately declaring false import duty values and miscategorising goods and their origins, as well as declaring lower than actual weights and volumes. Increased online trade also raises the potential for import duty and VAT evasion.

Globalisation also results in more illegal trade, including trading in art, cultural artefacts and endangered species, a market often consisting of international collectors. There is also a major market for export of electronic waste from Norway, as revealed by a TV documentary from state broadcaster NRK.6

It is believed that 20 per cent of all fish sold by retailers and catering in the international seafood market is mislabelled.7 The most common practice is mixing low-quality raw materials into high-quality raw materials and selling them as the latter. This type of fraud is hard to detect and generates significant profits.8

Large percentages of Norwegian exports, also from the petroleum sector, goes to countries with structural corruption problems. This makes the involved industries vulnerable to corruption, for instance when bribes are required to win or bid for contracts.

---

4 Crime that generate profit.

5 Financial Action Task Force (FATF), «Professional Money Laundering», 2018.

6 NRK, «Brennpunkt: Søppelsmuglerne», 2019.

7 FAO, Overview of food fraud in the fisheries sector, 2018.

8 The European Commission, «Fish substitution», 2015.

Large sums transferred out of Norway

Every year, large sums are transferred out of Norway by money service providers. The money often ends up in or near areas torn by conflict and war. The transfers are often made by persons of foreign origin, and some of them are well known to the police, with connections to drugs, violence and radicalisation.

Although most of the transactions probably involve funds with legitimate origins and are sent to family members, there are several cases of suspicious circumstances surrounding both the person transferring the money and the recipient. It is therefore likely that some of the money goes towards financing terrorist organisations abroad. Terrorist financing can seriously threaten life, health and the feeling of security.

There are few foreign fighters with links to the Nordic countries left in the Middle East, but it is possible that funds will be sent to those left.

Diaspora communities in the EU are financing activities and conflicts in their countries of origin.[9] The money is often transferred via money service providers who use banks to make transfers abroad. Several banks have over time discontinued or limited their customer relationship with a number of these providers.

One money service provider lost its licence with immediate effect in February 2020. According to the Norwegian currency transactions database, this provider had transferred NOK 1.5 billion out of Norway since 2014. The provider was first refused a permit to receive cash deposits and make bank transfers out of Norway but circumvented this by buying cash in Norway and transporting it physically abroad.

As established money service providers lose their bank connections and licences, their customers are presumed to start using other actors. It is therefore likely that other money service providers will transfer large amounts of cash out of Norway.

In addition, there are several actors who engage in illegal payment transfers, so-called Hawala operators.[10] Hawala is still used frequently by persons financing terrorism outside the EU. Many major Hawala operators are based in the United Arab Emirates and provide an international platform for illegal financing.[11]

9 Europol, «Terrorism situation and trend report" (TESAT) », 2018.

10 Hawala is an informal and trust based system for payments and transferral of money between countries that serves as an alternative to banks.

11 Europol, «Terrorism situation and trend report (TESAT) », 2018.

Financing of and support for terrorist organisations and acts of terrorism will often be motivated by political, ideological or religious goals. Unlike money laundering, terrorist financing does not focus on the origin of the money, but what it is intended to be used for. Financial or material support for terrorism is a crime under Norwegian law and defined as a terrorism-related act.

Illegal export of electronic waste

It is estimated that around 400,000 tonnes of illegal obsolete electrical and electronic products (electronic waste) are exported without a licence from Europe each year. [12] In Norway, the amount of electronic waste recorded as collected by return and recycling companies has fallen in recent years, and it is reported that an increasing share of the electronic waste is routed around the established return systems. Some retailers report that up to 50 per cent of their electronic waste is stolen. The Norwegian Environment Agency estimates that between 4000 and 10,000 tonnes of electronic waste disappears from waste reception centres in Norway each year. A significant percentage of the electronic waste that is not handled within the established return schemes is likely to be handled in violation of the regulations.

The reverse logistics system[13] means that failure to comply with the regulations in the further processing of the waste increases the profit significantly. Electronic waste also contains valuable components with a high resale value.

Illegal processing of waste distorts competition as the valuable components are removed before the products reach the recycling centres. Electronics contain heavy metals and organic toxic waste which pose a major environmental problem when they end up in nature. The processing of electronic waste in vulnerable countries is often highly polluting and harmful. Cutting compressors from household appliances is also a significant source of greenhouse gases.

Theft of electronic waste has been linked to Eastern European actors, and the waste is mostly exported in ship containers, first to transit countries such as Germany and the Netherlands, with countries in Africa, such as Ghana and Nigeria, and Asia as the final destination. Actors from African countries also travel to Norway or Europe on tourist visas to organise and load containers for export to Africa.

The export of waste appears to be well organised and some of the organisers of the sites where waste is gathered and loaded into containers likely help with transport, booking and document handling. Some seemingly legal enterprises are linked to export of electronic waste and several of the exporters are recurring offenders. Abuse of ID documents is also taking place when concealing the export.

Increased wealth in parts of the world is likely to result in increased demand for electronic goods. This is likely to generate a profit incentive for illegal trading in electronic waste. Selling electronic waste to recipients abroad via the internet also seems to be a growing trend in the West.

---

[12] CWIT-project, Countering WEEE Illegal Trade Summary Report, 2015. It was estimated that 1.3 million ton of undocumented electronics were exported from Europe each year. 30 percent is assumed to be illegal electronic waste.

[13] This means that the businesses are payed fully as they receive the waste, and before processing it.

Cross-border fisheries crime

The value of a sustainable and competitive industry serving as a cornerstone in many Norwegian coastal communities is important to maintain in order to benefit from positive effects in a globalised market. Fisheries are globalised with a complex and opaque value chain. Goods, labour and money cross Norway's borders in increasing volumes. Fish and fish-related products make up Norway's second largest export industry, with a total value of NOK 104 billion in 2019.[14] The fisheries actors range from small one-person businesses to large, global corporations that control several links in the value chain and have a significant geographic distribution.

It is likely that fictitious invoicing, quoting of incorrect prices and use of incorrect documents take place when fish is exported from Norway. These are actions that facilitate and conceal financial crimes, including tax evasion, accounting offences, fraud and overfishing.

Norwegian fisheries resources also attract roughe actors with links abroad. These actors acquire Norwegian resources illegally, as seen when tourists exceed their fishing quotas, or by challenging Norwegian jurisdiction over Norwegian resources, as seen in crab fishing.[15] There is reason to believe that the industry is vulnerable to laundering of proceeds both from illegal fisheries and other crime.

A recurring phenomenon in recent years has been the theft of whole lorry loads of frozen salmon by criminal actors with links abroad.[16] Norwegian authorities also receive requests from foreign authorities for verification of forged documents appearing to have been issued by Norwegian fisheries enterprises or fisheries management authorities. Exploitation of vulnerable foreign workers is also a problem.

Fisheries crime distorts competition and impacts negatively on management of resources and tax incomes. Rogue actors who create the impression of wanting to invest in jobs and infrastructure, but engage in crime instead, may harm the industry. Ultimately, cross-border fisheries crime can harm the reputation of Norwegian fisheries and fisheries management and threaten the livelihood of coastal communities.

14 Statistics Norway, «Fiskeeksporten passerte 100 milliard kroner i 2019», 2020.

15 Store norske leksikon, «Senatorsaken», 30. april 2019.

16 Helgelands blad, «Kripos etterforsker forsvunnet last med laks», 25. september 2019.

Fish welfare in fish farming

Fish farming has become important to coastal Norway and is now producing far more fish than traditional fisheries. However, the industry is facing problems relating to fish welfare.

The Animal Welfare Act applies both to the welfare of fish produced for food and cleaner fish – fish used to remove lice from the fish produced for food. The attention to and awareness of farm fish welfare has been raised, but the Norwegian Food Safety Authority still believe that welfare for the fish produced for food has declined in recent years.[17] 59 million farmed salmon died in the sea in 2019.[18] Increased mortality can to a large extent be linked to treatments for combating salmon lice. Higher-than permitted salmon lice levels can cause deep wounds. The measures taken to remove the salmon lice can, however, cause poor fish welfare and high mortality.[19]

Most of the enterprises now use non-medication methods against lice, which mean that the fish is deloused frequently. Estimates show that more than 311 million fish may have undergone thermal delousing[20] in 2017. Use of thermal delousing puts severe strain on the fish and mortality rises after such delousing.[21]

Use of cleaner fish is gentler on the fish produced for food and is permitted. However, cleaner fish are severely subjected to transport stress and illness[22] and is used as an input factor with a mortality of up to 100 per cent. Many cleaner fish also die because they end up in the delousing process.[23] Between 50 and 60 million cleaner fish die annually.[24]

The Food Safety Authority has increased its focus on cleaner fish welfare. However, fish farming is an industry where exceptionally large numbers of fish are involved in industrialised and capital-intensive food production. Actors who violate the regulations by e.g. not reporting high lice numbers to avoid early slaughtering, can make a big profit. Safeguarding fish welfare will therefore probably continue to be challenging.

17 The Norwegian Food Safety Authority, «Mattilsynets arbeid med dyrevelferd, Årsrapport 2017».

18 Norwegian Veterinary Institute, «Fiskehelserapporten 2019», Rapport 5a-2020.

19 The Norwegian Food Safety Authority, «Sluttrapport etter Mattilsynets tilsynskampanje på legemiddelbruk i oppdrettsnæringen», 2018.

20 The use of hot water.

21 Poppe, Trygve T.; Dalum, Alf S.; Røyslien, Eline; Nordgreen, Janiiscke & Helgesen, Kari Olli, «Termisk behandling av laks», Norsk veterinærtidsskrift nr. 3/2018.

22 Nilsen, Arve; Viljugrein, Hildegunn; Røsæg, Magnus Vikan & Colquhoun, Duncan, «Rensefiskhelse – kartlegging av dødelighet og dødelighetsårsaker», Veterinærinstituttets rapportserie nr. 12/ 2014.

23 The Norwegian Food Safety Authority, «Nasjonal tilsynskampanje 2018/2019 - Velferd hos rensefisk».

24 Dagens Næringsliv, « Mener laksenæringen ikke er bærekraftig: - Må si klarere ifra», 2020.

Work-related crime

Organised criminals are to an increasing degree infiltrating legal business sectors to maximise their profits, erasing the lines between organised crime, financial crime and work-related crime.[25]The support schemes aimed at private enterprise in connection with the coronavirus pandemic and the unemployment benefits scheme are expected to be attractive to such actors.

Work-related crime is profit-motivated crime at the expense of the employees' working conditions and rights. The term covers a wide range of criminal offences and actors. VAT and benefit fraud are, in addition to undeclared labour, among the chief sources of profit. Criminal actors will also attempt to minimise wage costs and avoid mandatory costs in connection with the employees' health, working environment and safety.

In Norway, work-related crime and organised crime is now being committed in some networks by legal import channels being used to smuggle drugs, and by enterprises being used for drug distribution. There are also links to illegal gambling, firearms sales and prostitution.[26]

Proceeds from other criminal activities are laundered by investing or routing them through enterprises linked to work-related crime. Proceeds are also invested in real estate, which is in turn often rented to legal entities.

Use of fictitious and false documents remains a major problem. False ID is used for e.g. VAT fraud, to conceal undeclared labour and to strip companies of assets. ID documents are also used to register unaware or exploited persons as managers of enterprises.

Enterprises trying to evade their employer responsibility and criminals adapting to control efforts and regulations are on the increase. Illegal activities are moved between enterprises and planned bankruptcies are used to evade authority requirements. The National Joint Analysis and Intelligence Centre (NTAES) uncovered that 45 per cent of threat actors in work-related crime had held a leading role in an enterprise that had declared bankruptcy.[27]

---

25 Transcrime, « Mapping the risk of serious and organised crime infiltration in Europe», Final report of the MORE project, 2018.

26 NTAES, «Situasjonsbeskrivelse arbeidslivskriminalitet» 2020.

27 Ibid.

Exploitation of foreign workers

Norway has a good economy, high standard of living and high demand for labour. These are pull factors for foreign workers, people fleeing wars and poverty and those who want to make a profit on these people.

There is more to gain by using cheap foreign labour in large, labour-intensive projects. In the construction industry even a small difference in the hourly wage can cut significant costs for the employer and enable competitive tenders. Exploitation also takes place in labour-intensive professions with a high percentage of untrained workers, such as car valeting, seasonal farm work and fish processing.[28]

So-called payback is a common method when underpaying workers. The employer demands to have wages paid back, does not disburse holiday pay and demands higher housing rent than the market dictates. There are also several examples of enterprises failing to ensure proper health, environment and safety solutions. It is not uncommon for foreign workers to be quartered in housing intended for fewer people, with faulty electrical wiring and deficient or lacking smoke detectors, fire extinguishers and escape routes.

To avoid paying taxes, foreign enterprises state that they pay tax to the EU or EEA state in which they are registered, and that the workers will only stay in Norway for brief periods. Wages are often paid into accounts abroad, making it difficult for Norwegian authorities to check whether the wages comply with Norwegian regulations.[29] Underpaying workers distorts competition and may, over time, undermine the faith in a fair market, the welfare state and the police and supervision agencies.

The majority of workers involved in worked-related crime are from Eastern Europe, and there has been an increase in the number of third-country nationals, some of whom commit profit-motivated crime while in Norway. Foreign enterprises performing contract work in Norway can now use third-country nationals without there being any requirement for the employer to also use the same worker on assignments in the EEA/EU country the enterprise is registered in. [30] This will most likely result in an increase in workers from third countries in the coming years. Working on assignment for a foreign employer raises the risk of exploitation in the form of underpayment, poor living quarters and unsafe conditions, in particular if the worker is from a poor country. It is likely that such exploitation will become more serious.

28 NTAES, «Situasjonsbeskrivelse 2020 - Arbeidslivskriminalitet», 2020.

29 A-krimsenteret i Oslo, «Årsrapportering», 2019.

30 Frifagbevegelse, «UDI og tredjelandsborgere: Nå blir det lettere for utenlandske firmaer å ta med seg billig arbeidskraft fra land utenfor EØS til Norge», 2020.

VAT fraud in work-related crime

Value-added tax (VAT) is a tax on domestic sales of goods and services. Value-added tax yielded an estimated NOK 310 billion to the Norwegian state in 2019 and makes up one-fifth of the total tax income.[31] The tax is collected by Norwegian enterprises on behalf of the state. Excess value-added tax payments are refunded by the state.

VAT fraud is one of the main sources of profit in work-related crime. The fraud is often carried out through fictitious invoicing or undeclared revenues. Fictitious invoicing is the organised production of incorrect documents in an enterprise structure to make fictitious purchases and sales appear real. Undeclared revenue, however, may involve real payments, but these are deliberately not reported to the authorities. The objective of both methods is to evade taxes and free up cash for undeclared wages off the books.

An audit of the delivery van sector in Oslo in 2019 showed that 20 per cent of audited enterprises had failed to declare revenues for that period. 22 per cent of employed drivers and 60 per cent of driver's assistants were not registered to have received any wages, and a selection of 25 contractors owed a total of NOK 21 million to the public purse, mainly VAT. Common denominators for these enterprises are that they have few or no registered employees and they receive large transfers from the enterprises who use their services. Labour-intensive sectors subject to few regulations and with low start-up costs and extensive use of contractors have a higher risk of work-related crime.[32]

In addition to the loss of revenue for the state from VAT fraud, the practice also distorts competition. In 2018, 31 per cent of enterprises stated that they often had to compete with other enterprises which had a lower cost level due to operating off the books or otherwise evading taxes. For painters and floorers, as well as passenger and goods transport, this figure is above 70 per cent.

Fewer audits can result in lower detection risk during the coronavirus pandemic. There is an even chance that criminals will exploit this situation to receive disbursements through fictitious VAT reports or transactions.

31 The Norwegian Treasury, «Prop. 1 LS (2018-2019)», 2018.

32 A-krimsenteret i Oslo og Akershus, «Arbeidslivskriminalitet i transportbransjen – varebilsegmentet», 2019.

Money laundering in the property market

The property market is a capital-intensive market involving movement of large amounts, making it suitable for laundering the proceeds of crime.[33] The property market is used by work-related crime actors to launder money, investing in both homes and commercial properties in Norway and abroad. The invested proceeds may be from tax evasion, undeclared wages from undeclared workers or revenues that are kept off the books.[34] The property is used, rented out (also to public agencies etc.) or renovated and sold at a profit.

The methods for laundering proceeds in the property market include paying for improvements and renovation with cash generated by criminal activities. Such work is often undeclared.

Another method involves manipulating the value of the properties. Properties are quickly resold at a much higher value without ever being put on the open market, often shortly after being bought. We have also seen professional actors, such as realtors and lawyers, help provide fictitious valuations and facilitate so-called revolving-door sales, i.e. the same property being sold frequently, often at abnormal prices. Some of the actors involved in such sales are known to the police in connection with organised crime.

Selling and buying contracts for the purchase of housing units in future construction projects are also suited to money laundering. Selling such contracts at a large profit before the construction work starts enables tax evasion as the increase in value does not appear in any public databases and is therefore not available to the tax authorities unless declared by one of the involved parties. It is likely that turnover of contracts for purchase of units in future projects is used to launder funds and evade taxes.

The number of suspicious transactions reported from realtors increased from 45 in 2015 to 886 in 2019. There is an even chance that the increase in suspicious transactions reports from realtors is due to raised awareness about compliance with the money-laundering provisions, but the increase may also reflect a real development as this is a sector in which it is attractive to invest the proceeds of crime.

33 Financial Supervisory Authority of Norway, «Risikovurdering – Hvitvasking og terrorfinansiering», 2019.

34 NTAES, «Situasjonsbeskrivelse - Arbeidslivskriminalitet 2019», 2020.

2. Sustainability

A sustainable development meets the needs of the current population without destroying the opportunities of future generations. Sustainable development requires that the basis for our existence, planet earth and its climate, environment and natural diversity, is maintained. The economy should be developed in a manner ensuring good living conditions, including education, decent work, equality, cultural diversity and good health services, for all.

The World Economic Forum has identified climate change and its harmful effects to be among the greatest risks in the coming decade. Climate change is escalating quicker and impacting the world harder than previously assumed. The short-term consequences include loss of life, higher socio-economic and geopolitical tension and negative economic consequences. Climate-related natural disasters such as hurricanes, drought and large-scale fires have already become more intense and frequent.[35] The polar ice caps are melting faster, and heat waves have become more common. The climate in Norway has changed over the last hundred years, and weather conditions are expected to grow warmer and sea levels are expected to keep rising.

Researchers fear the collapse of ecosystems, and loss of biological diversity is one of greatest threats facing the world, potentially causing food production and health services to collapse, increased water shortages and interrupted supply chains. Humans have exterminated 83 per cent of all wild animals and half of all wild plants.[36]

Climate change is expected to cause more migration and general shortages can trigger wars and conflicts. This may curb the world economy, cause food price instability, interrupt supplies, change production and consumption patterns and impact the value of the oil revenue investments.[37] The Arctic shipping lane presents a potential new transport route

35 World Economic Forum, «The Global Risk Report», 2020.
36 World Economic Forum, «The Global Risk Report», 2020.
37 Norway's public investigations (NOU) 2018:17, «Klimarisiko og norsk økonomi», 2018.

as the Arctic ice retreats and may cause more traffic in a vulnerable area far from established emergency response systems. Central banks are increasingly viewing climate change as a significant risk to global capital markets.

The coronavirus outbreak has resulted in countries diverting resources to handle the pandemic, causing postponement of some measures to save the climate.

A sustainable economic development requires funding. The global business model results in incomes being routed to where taxes are low, often tax havens.[38] This lowers the tax incomes of many countries and thereby their ability to provide education, welfare and health services.

The pressure on wages, pensions and benefits also lowers the purchasing power of most people. Increasing social inequality has caused social rebellion in many countries, and inequality in Norway is also increasing due to less redistribution.[39] Housing market developments, with rising house prices over an extended period of time, have caused an increase in the structural differences between cities and rural areas.[40] Extreme weather raises insurance premiums and may at worst result in insurance becoming too expensive for average Norwegian citizens and enterprises, resulting in increased social inequality.[41]

38 Fair Tax, «Tax gap of Silicon Six over $100 billion so far this decade», 2019.

39 Statistics Norway, «Økt ulikhet som følge av skatteendringer de siste årene», 2019.

40 NRK, «Regjeringen varsler ytterligere kutt i eiendomsskatten», 2019.

41 World Economic Forum, «The Global Risk Report», 2020.

Climate and nature crime

Damage to the world's natural resources impacts everything from the air we breathe to the food we eat. Climate and nature crime have a broad impact, with often irreversible effects and damage is caused to humans, animals, nature and the environment. The climate crisis and stronger focus on the environment will change our perception of what constitutes serious crime.

Emissions and discharges that have previously not been sanctioned will probably be considered serious environmental crime in the future.

Along the coast, the ever-growing aquaculture industry has major consequences for nature. Fish farming causes discharge of nutrient salts, medicines and organic material to the sea, impacting marine flora and fauna. Escaped fish also have an impact on biological diversity and ecosystems.

Vulnerable nature areas and animal species are under pressure from multiple directions. Illegal motorised traffic off road is a major problem in several parts of Norway and has particularly serious consequences for fauna and flora when taking place on dryland. The number of motorised vehicles, both snowmobiles and ATVs, is on the increase,[42] and many use their vehicle mostly for recreational driving and thrill-seeking. Illegal motorised traffic is therefore highly likely to remain a problem in several parts of Norway.

The focus on negative environmental consequences and environmental crime is also growing stronger in the tourist industry. Several tour operators have been reported for disturbing animals and birds, and the illegal export of fish from tourist fishing is on the increase. On Svalbard, more tourism, combined with fewer ice-covered fjords, puts pressure on the polar bear population.

The interventions, emissions and discharges that threaten Norwegian nature and biodiversity mostly have one common denominator: they are not individually large, but their overall impact can cause significant damage. In addition, the consequences are often irreversible to humans, biodiversity, nature and the environment. Climate change also makes nature more vulnerable to interventions, meaning that it takes less to damage it.

42 Bjørnskau, Torkel & Ciccione, Alice, «Bruk av snøscooter i Norge», TØI rapport 1564/2017.

Illegal emissions and discharges

Illegal emissions and discharges can have serious consequences to nature and the ecosystem. The largest emissions and discharges are from enterprises with permits to use, handle and release hazardous substances. Violations of the emissions and discharge limits set in permits, resulting from lack of maintenance, accidents or deliberate actions to increase earnings, constitute serious pollution crimes.

In 2019, 269 violations of the Pollution Control Act were reported to the police, on par with the number of cases in each of the four preceding years. There were also several cases of acute pollution. The Norwegian Coastal Administration reported 607 incidents causing acute pollution in 2019.[43]

Norwegian waters include busy shipping lanes. The discharge and emission limits for sea vessels were lowered effective 1 January 2020, and they are now required to use fuel with lower sulphur content.[44] The change entails higher costs,[45] which means that some ship owners may continue to use fuel with illegally high sulphur content.

Maritime transport can also cause discharges when running aground or sinking. There were 52 instances of vessels running aground on the Norwegian coast in 2019, a decline compared with 2018 and 2017. Whether or not a major discharge results when a vessel runs aground is often due to random chance. The consequences of a major discharge from a vessel can be catastrophic to some species and the ecosystem. More maritime traffic in the Arctic as a result of less ice may raise the risk of vessels running aground and subsequent discharges. More frequent extreme weather may also cause more vessels to run aground and create new problems for maritime safety and oil spill preparedness.

The oil industry is another sector with a major emission and discharge potential. The largest discharge since the start of the oil industry in Norway took place in 2007 when an oil hose leak discharged almost 4000 tonnes of oil into the sea. However, most illegal discharges in Norway are violations of set limits for the discharge of oily waters or chemicals.

In the onshore industry, tank facilities and waste management have proven particularly vulnerable to illegal discharges and emissions. Audits have proven that internal checks and controls are often deficient and that knowledge of and compliance with the regulations is poorer at smaller tank facilities.

Legal amendments aiming to reduce emissions and discharges harmful to the climate may cause more pollution crime in the coming years.

43 Norwegian Coastal Administration, «Hendelser håndtert i 2019», 2020.

44 Norwegian Maritime Authority, «Nye svovelkrav fra IMO» 2016.

45 E24, «Skipsfarten stålsetter seg for svovelkrav: - En enorm endring», 2018.

» Marine waste is defined as all solids from human activity that are abandoned in or otherwise transported to the marine environment. Marine waste includes waste from land-based sources transported to the sea by waterways, discharge pipes and wind. Marine waste includes plastic, wood, metals, glass, rubber, textiles, paper etc. (Lozano et al. 2009).

Marine pollution

Marine waste is one of the greatest environmental challenges we face, and it is an increasing problem.[46] Climate change and stronger focus on environmental issues have given a better understanding of the consequences of marine waste, and even minor discharges are now considered to have major environmental consequences because they add to the overall strain on the environment. Marine waste causes great damage to and suffering for many organisms. The costs of plastic waste have been estimated by the United Nations' Environmental Programme (UNEP) at USD 40 billion per year.[47]

Plastics make up around 80 per cent of the waste in the sea. Over time, this plastic disintegrates into microplastics, which can impact the entire marine ecosystem. Globally, most of the waste in the sea comes from land.

Most of the plastic waste in the seas around Norway and Svalbard, however, has local origins – almost 50 per cent of the waste found on Norwegian beaches stems from Norwegian vessels and fisheries.[48] A new study has shown that commercial fisheries in Norway put 400 tonnes of plastic waste in the sea every year.[49]

Active dumping of old fishing equipment is less common than previously. However, lost fishing equipment and large amounts of cut ropes and nets are still observed, probably stemming from minor repairs to fishing equipment that are not sufficiently well handled.[50] Ship traffic is also a source of marine waste. Such violations are hard to uncover, but Coastal Administration aircraft have recorded vessels dumping waste in the sea illegally.[51] Many ship containers are also lost overboard, causing pollution. More traffic along the coast will probably raise the threat of marine pollution and dumping of plastic.

There is a ban on discharging waste from vessels in the North Sea area, and it is forbidden to unnecessarily throw away or leave equipment or moorings at sea or on the seabed.[52] Vessels have a duty to deliver the waste in port.[53] It is therefore likely that a considerable percentage of marine waste in Norway is the result of Pollution Control Act violations and should be treated as serious environmental crime.

---

46 The Norwegian Environment Agency, «Kunnskap om marin forsøpling i Norge», Rapport M-265/2014.

47 The Norwegian Environment Agency, «Overordnet vurdering av kilder og tiltak mot marin forsøpling».

48 The Norwegian Environment Agency, «Kunnskap om marin forsøpling i Norge», Rapport M-265/2014.

49 Despande, Paritosh; Philis, Gaspard; Brattebø, Helge & Fet, Annik M., «Using Material Flow Analysis (MFA) to generate the evidence on plastic waste management from commercial fishing gears in Norway», Resources, Conservation and recycling: X, Vol. 5, 2020.

50 The Norwegian Environment Agency, «Overordnet vurdering av kilder og tiltak mot marin forsøpling».

51 UNEP, «Marine plastic debris and microplastics sources of macro and microplastics», 2016.

52 According to the MARPOL Convention and Marine Resource Act § 28.

53 The Norwegian Environment Agency, «Kunnskap om marin forsøpling i Norge», Rapport M-265/2014.

Welfare crime

The Norwegian welfare state guarantees equal access to benefits. Most public services are either affordable or free, and people are entitled to various financial benefits as needed.[54] The welfare state is to a large extent financed by tax on income, wealth and consumption.

Crimes such as tax evasion, work-related crime and abuse of public funding schemes threaten the financing of the Norwegian welfare state. The scope is unknown, but tax evasion and abuse of public funding schemes cause major losses annually to the Norwegian state. Tax evasion is committed by various actors, ranging from private individuals and small enterprises working off the books to those who make deliberate use of complex business structure and tax havens. Large sums are also handed out under the public trust-based funding schemes, and these schemes can be taken advantage of.

It is also a problem that the legislation and social rules are sometimes out of date, giving actors intent on taking advantage of the system more opportunities.

Welfare crime does not just rob society of income, it also puts pressure on negotiated laws and entitlements in working life when foreign employees are exploited in work-related crime to maximise profits.

In Sweden there has been a shift from using undeclared labour to using labour leased from foreign staffing agencies. Criminals control the foreign staffing agency in parallel with a Swedish enterprise. The staffing agency invoices the Swedish enterprise for use of labour and the payment is made to a foreign account. It is difficult to check whether the staffing agency complies with wage and working hour's provisions and pays the right taxes. It is likely that the same methods are used in Norway. Foreign employers and employees working in Norway do not necessarily know how the welfare system works or their rights.

[54] Store norske leksikon, «Velferdsstat», 4. september 2019.

Abuse of public funding schemes

Public funding is disbursed to a number of different enterprises and purposes, including support for enterprises in their set-up phase, agricultural subsidies to farmers and funding for climate adaptation measures to enterprises. The funding can also take the form of tax deduction schemes. Primarily, it is the state which loses if someone receives public funding based on incorrect information, but this also indirectly impacts those enterprises and organisations that did not receive funding.

There is little available information about the scope and abuse of public funding schemes, but Swedish authorities have uncovered how criminals establish organisations in order to receive public funding and that methods for committing welfare fraud can be bought as crime-as-a-service.[55]

In 2018, almost NOK 90 billion in public funding was disbursed to research and development projects. ØKOKRIM know of cases where incorrect information was provided to receive such support.

The SkatteFUNN tax refund scheme was introduced to motivate Norwegian businesses to invest more in R&D.[56] The results have been positive, but the scheme has also been abused by companies claiming tax deductions for ineligible expenses.[57] In one sector, more than half of companies audited that year had reported too high SkatteFUNN costs.

In 2015, the Government created a scheme to support measures against marine waste, and the Norwegian Environment Agency has since then awarded more than NOK 225 million under this scheme.[58] Abuse has been uncovered, and it is likely that increased possibilities to secure funding from the state to climate measures will result in more abuse.

The individual funding schemes are often modest and mostly trust-based. The detection risk is considered to be small. This makes it likely that fraud involving public funding takes place more often than media coverage and the number of criminal cases indicate.

55 Swedish Prosecution Authority, «Myndighetsgemensam Lägesbild om organiserad brottslighet», 2019.
56 The Research Council of Norway, «Vedlegg til årsrapport 2018. Del II Departementsvis rapportering», 2019.
57 The Norwegian Institute of Public Accountants, «SkatteFUNN – Fortsatt en gunstig ordning», 2019.
58 The Norwegian Environment Agency, «Disse får ryddestøtte», 2016, 2017, 2018 & 2019.

Tax havens

Persons and companies domiciled in Norway are liable for tax on all income and wealth in Norway regardless of whether the assets are located or the income received abroad or in Norway (the global income principle). One of the methods for evading taxation in Norway is to hide assets in so-called tax havens. The term tax haven is commonly used about countries with a beneficial tax rate, few regulations and little transparency around ownership of bank accounts and/or companies.

Tax havens are used legally by Norwegian companies but are also used to conceal assets from taxation. Globally, it is estimated that assets worth USD 7.8 trillion were hidden in tax havens in 2016, corresponding to 10.4 per cent of global GNP.[59] It is estimated that hidden Norwegian assets in tax havens amount to USD 16.7 billion.[60] The ineffective handling of tax evasion may weaken trust in the Tax Administration and make people more willing to evade taxation.

In recent years, Norway has entered into several agreements with various countries about exchange of information that can be linked to Norwegian nationals, in order to make it harder to hide incomes and assets from Norwegian authorities. More international transparency is, seen in isolation, expected to reduce the threat of tax evasion via tax havens.

The real tax losses are probably significantly larger than the hidden assets indicate. Use of corporate structures to conceal off-the-books sales or profits from sale of assets, claiming tax deductions for fictitious costs from foreign companies and corporate structures which conceal that the tax subject is domiciled in Norway, result in further tax shortfalls.[61] It is likely to remain a problem that incomes generated abroad are not reported for taxation purposes in Norway and that complex structures are used to conceal who the real owners of assets are. This also raises the risk of money being laundered abroad.

The digitalisation of the economy, in particular new payment solutions and means of payments, will make it harder for tax authorities to trace money and easier for tax payers to conceal cross-border transactions and assets and incomes abroad.

59 European Commission, «Estimating International Tax Evasion by Individuals», 2019.

60 Alstadsæter Annette, Johannesen, Niels & Zucman, Gabriel, «Tax Evasion and Inequality», 2018.

61 The Norwegian Tax Authorities, «Hva vet vi om skjulte verdier i utlandet?», Analysenytt 02/2018.

Public sector corruption

From 2018 to 2019, Norway dropped from third to seventh in the Transparency International corruption index. This may be interpreted to mean that Norwegians consider corruption in the public sector to have become more common than was previously the case.[62] Popular perception of what can be termed corruption is probably broader than the definition in the Penal Code. There is generally little tolerance for persons who exploit their position to grant or receive unjustified advantages in Norway.

In recent years, several serious corruption cases have been uncovered within local planning authorities, in addition to cases involving public purchases. Corruption in the public sector can weaken confidence in local authorities and provide criminals with access to contracts awarded by local authorities.

There are large variations between local authorities in how they enforce integrity systems,63 and some work remains until the entire sector work systematically against corruption.64 Norwegian local authorities are therefore vulnerable to corruption and the risk of corruption is particularly high where the public sector interacts with the private sector.

We assess that the threat of corruption in local authorities will remain high in Norway, in particular regarding construction projects. The risk of corruption depends on the local authorities' own efforts to combat corruption, the availability of well-functioning whistle-blower channels, audit committees and proper protection of whistle-blowers.

The OECD considers procurement one of the most important corruption risk areas internationally. The regulations for public procurement are characterized by many concrete assessments, but also extensive use of procurement discretion. This discretion raises the risk of abuse.65 In Sweden, three out of ten tenderers in public tenders believe they have lost contracts due to corruption. There is a threat of criminals gaining access to tender processes in Norway as well.

In the current pandemic situation, many have been given new roles without possessing in-depth expertise about anti-corruption work. That may increase the risk of corruption.

62 According to Transparency International's corruption index of 2019 Denmark and New Zealand was ranked as number 1 followed by Finland and Singapore, Sweden and Switzerland on a shared 3 place. The index is based on peoples perception of corruption in the public sector.

63 Kantar TNS, «Etikkarbeid i Kommunesektoren», 2017.

64 Transparency International Norway, «Korrupsjonskampen», 2019.

65 White Paper 22 (2018–2019) «Smartere innkjøp – effektive og profesjonelle offentlige anskaffelser», 2019.

3. Virtualisation

The virtualisation[66] of society takes many forms and has created new crime opportunities. Crime in the virtual space is increasingly committed without any physical contact, on new arenas and often using an identity that is separate from the physical person. The crime situation is currently characterised by crime relating to virtual currencies[67] and cryptocurrencies[68], mass fraud in the virtual space, abuse of personal information and data, online sexual abuse and online threats.

Virtualisation and digitalisation[69] are gathering speed both for consumers, critical infrastructure and private and public services. The internet of things (IoT), 5G, artificial intelligence (AI) and virtual and enhanced reality provide us with smart cities, houses, enterprises and services and will drive society onwards.[70] It is estimated that 60 per cent of the world's GNP will be related to the digital economy by 2022.[71] This can be abused by both state and non-state actors. The number of attacks on IoT devices rose by 300 per cent globally in the first half of 2019.[72] The percentage of Norwegians who use internet daily is now approximately 90,[73] and our most important functions and services are now online. The majority of Norwegian enterprises depend on IT support from foreign companies to operate their IT systems.[74]

The amount of information generated grows, as does the number of actors storing this

66 An increasing number of things in society, including the storage of data, shops and values are transformed from physical to virtual and are accessible in the virtual space.

67 A virtual currency is a digital expression of value, but it has been issued by a private actor, not a central bank or any other official authority.

68 A cryptocurrency is a virtual currency that uses cryptography to secure transactions.

69 Data are transformed from being analogue to digital.

70 The Norwegian National Security Authority (NSM), «Helhetlig digitalt risikobilde», 2019.

71 IDC, «FutureScape: Worldwide IT Industry Predictions 2019».

72 World Economic Forum, «The Global Risk Report», 2020.

73 Statistics Norway, «Dette er Norge», 2019.

74 NSM, «Helhetlig digitalt risikobilde», 2019.

information. Increased virtualisation increases the value of data. For instance, large data is now used to develop artificial intelligence. This may result in more computer break-ins and theft of information such as personal data and credit card numbers. During the cyber attack on Equifax in the US, hackers acquired the names and social security numbers of half of all US citizens.[75] The fact that increasingly large amounts of personal data are shared with companies abroad may also cause more vulnerabilities relating to ID theft. Criminals exploit available vulnerabilities. We see this during the ongoing coronavirus pandemic as well.

Criminals are increasingly using new technological solutions and will probably use both cryptocurrencies and digital payment platforms more often in the future. Virtual currencies and cryptocurrencies are well suited to financing crime and laundering money. We are also seeing how it can be used for extortion, as in the ransomware attack on Norsk Hydro in spring 2019.[76]

Cryptocurrency can also be used as a means of payment on the darknet, where illegal services and goods are sold.[77] Advanced tools and criminal services are on sale online and theft and fraud can be committed without the perpetrators ever setting foot on Norwegian soil.[78] Europol expects the darknet to fragment, with particularly small actors using encrypted communication applications such as Telegram and Discord.[79] New communication and trading platforms are also used to plan and commit crime.

---

75 New York Times, «U.S. Charges Chinese military officers in 2017 Equifax hacking», 2020.

76 NRK, «Skreddersydd dobbeltangrep mot Hydro», 2019.

77 National Crime Agency, UK, « National Strategic Assessment of Serious and Organised Crime », 2019.

78 NSM, «Helhetlig digitalt risikobilde», 2019.

79 EUROPOL, «Internet Organised Crime Threat Assessment (IOCTA) 2018», 2019.

Financial crime in the virtual age

Increased digitalisation and virtualisation make society more exposed to digital crime. Financial crime committed digitally has a global reach and criminal actors can easily target a large number of victims. In other cases, the perpetrators cooperate to target one carefully selected victim, who may suffer a major financial loss.

Robots and artificial intelligence (AI) can be used to manipulate markets and false websites can be used to collect payment card data and personal information. Online social manipulation is used by criminals to gain the victims' trust and then abuse this trust in various forms of fraud.

Romance scams are a frequently used method where victims are trapped in an emotional relationship they find it hard to break out of. In a case from 2017, the bank DNB was brought before the finance industry complaints board, Finansklagenemnda, when the bank refused to let a woman transfer money to her "fiancée".[80] Victims are often older adults with social media or dating site profiles. [81] As older people start using more social media, this group is likely to suffer more identity theft.

Social manipulation is also effectively used in ID theft, and 2018 saw a considerable increase in SIM swapping. Attackers persuade telecom providers to transfer someone's telephone number to a SIM card they control.[82]

The relatively few cases of reported digital fraud can be linked to the police rarely prosecuting such cases. In most cases, the money quickly disappears out of Norway, and the chances of getting the money back are small. The fact that the police are not involved when businesses, public authorities, organisations and individuals become victims of digital crimes, challenges the rule of law. Only three out of ten Norwegians believe the police handle ID theft and fraud well.[83]

---

80 Dagens Næringsliv, «Overførte 745.000kr til kriminelle – klager på DNB fordi hun ikke får sende mer penger», 2018.

81 NorSIS, «Trusler og trender 2018 – 19», 2018.

82 Telenor, «Slik angriper de», 2019.

83 National Police Directorate, «Politiets innbyggerundersøkelse», 2019.

New payment service providers

Several new digital payment service providers have come on the market in recent years. These actors specialise in services outside the traditional banking system and offer card payments, currency exchange and money transfers nationally and internationally. They also offer more anonymity and quicker transfers at lower prices. Several providers[84] have already secured licences from the Financial Supervisory Authority to operate cross-border activities as e-money enterprises.[85] We believe that they will invest significantly more in banking services in coming years.[86]

Estimates indicate that around 39 million people use so-called neo-banking, i.e. banks that operate globally and only digitally outside of the traditional banking system. [87] In Denmark, the use of neo-banking increased markedly from 2018 to 2019.

New digital payment services pose several challenges: The real sender or recipient is often concealed, requiring use of several sources to gain a full overview of the chain of transactions. It is also uncertain whether the new payment services conduct sufficient customer checks to determine whether the customer is at risk of committing or being exploited for money laundering or terrorist financing. When transactions in addition can be performed in realtime across national borders and in bulk, the work to trace transactions to combat money laundering and terrorist financing becomes more complex. It will also be more difficult to distinguish between legitimate and suspicious transactions.

Foreign providers are required to report suspicious transactions relating to money laundering and terrorist financing to the authorities of the country where they are domiciled, even if the transaction takes place in or from Norway. Experience has shown that this results in fewer reports to Norwegian supervisory authorities. This in turn results in important information not reaching Norwegian police and supervisory authorities, and it becoming time-consuming to collect information when suspecting that crimes have taken place.

The anonymity and speed of international transfers make them likely to be used by criminals to launder proceeds or to transfer money to terrorist organisations.

84 As exampe Alipay, Amazon, Apple, Facebook, Google, Paysera, Revolut and Transferwise.

85 From FSAs register of businesses. As of March 3rd 2020 there are 169 foreign e-money companies with cross border activity with a licence from FSA.

86 Wired, «Every tech company wants to be a bank – Someday, at last», 2019.

87 Business insider, «The global neobanks report», 2019.

Digital payment platform is a term for applications and web-based software used to make money transactions, but which are not online banks.

Card fraud

Card fraud involves using someone else's payment card or card information to carry out purchases or cash withdrawals. The fraud either takes place by physical use of the card, or by using stolen or false card information (Card-not-present, CNP). Card information is stolen through skimming, social manipulation or breaking into the systems of suppliers which store customer information. Both card information and payment cards are traded on the darknet. In the first half of 2019, there was information from 23 million stolen credit cards for sale on the darknet.[88]

The financial loss from abuse of payment cards in Norway was NOK 149 million in 2018, with CNP making up NOK 115 million.[89] Card fraud primarily affects the card owner, but the loss is often covered by the card issuer or vendor.[90] There are also additional costs for the card issuer in connection with case processing.

Online shopping has risen sharply over recent years and is likely to grow significantly in the near future as a consequence of the coronavirus measures. This increase is expected to endure. Fraudsters also create false online stores and attract customers with very low prices to get hold of their card information.[91] When new people start shopping online, they are more vulnerable to false websites.

There is also great competition in making payments as seamless as possible and the wait until the goods arrive as short as possible. This helps fraudsters succeed more often, and the rapidity of the transactions also make them difficult to cancel or stop.[92] The rise in online shopping is therefore a driver in card fraud.

Most cases where card information is stolen begin with third-party data being compromised. The introduction of the Revised Payment Services Directive (PSD2)[93] in 2018 requires banks to give third-party actors access to their customer's wage accounts if the customer has consented. This makes banks vulnerable to third-party weaknesses.[94] More online shopping and associated use of card information, as well new payment solutions, the introduction of PSD2 and hidden online marketplaces are likely to raise the risk of card information being stolen in the coming years.

88 EUROPOL, «Internet organised crime threat assessment (IOCTA) 2018», 2019.
89 BITS, «Bits AS har dessverre oppdaget en feil i rapporterte tall for svindel for 2018», 2019.
90 NTAES, «Bedrageri mot næringslivet», 2019.
91 AT&T, «Protect yourself from phishing and false websites» og Telenor, «Unngå kortsvindel i vinterferien», 2020.
92 Cifas, «Fraudscape», 2019.
93 The Second Payment Services Directive (EP/Rdir. 2015/2366).
94 EUROPOL, «Internet organised crime threat assessment (IOCTA) 2018», 2019.

Investment fraud

Investment fraud entails private individuals or enterprises being deceived into investing in projects or products that are non-existent or without value. Social manipulation is a key part of the fraud process.

Many Norwegian banks work actively to prevent customers being defrauded. In 2019, 725 customers in the Norwegian bank DNB were subjected to investment fraud attempts, with potential losses totalling almost NOK 200 million. This is a marked increase from 469 victims in 2018.[95]

Investment fraud is linked to various assets. Recently, there has been an increase in investment fraud in connection with sale of cryptocurrency. In many cases, the fraud is linked to collection of capital to kickstart a new cryptocurrency which does not exist.[96] Several cryptocurrency frauds can be traced to Nigeria.

Pyramid schemes are a frequently used method to attract investors with promises of high returns. The increase in value promised to investors is just an illusion, and any disbursements to investors are merely funds transferred from investors further down the pyramid.

OneCoin appears to be a pyramid scheme linked to something presented as a cryptocurrency. The fraud is believed to have attracted almost EUR 4 billion between 2014 and 2018 and has been linked to organised criminals in the Balkans.[97]

Use of property to commit fraud has proven to be very lucrative in Norway. The Financial Supervisory Authority reported that investments in false companies amounted to NOK 92 millions in 2018.[98] The method generally involves buying a property, starting a limited company to "operate" the property, recruiting investors to the company and then selling the property to the limited company at an overprice. The fraudsters appear to be professional, both in appearance and behaviour. The fact that the companies are registered with the Financial Supervisory Authority also creates an impression of legitimacy. Operations in several major property fraud enterprises have now been stopped. There may therefore be fewer victims of such investment fraud going forward.

In connection with the coronavirus pandemic, fraudsters are convincing their victims that falling share prices make it a good opportunity to invest now in order to profit from the coming upturn. DNB reports that many of those who now sit alone at home, in particular older people, are vulnerable to being exploited by fraudsters.[99]

95 DNB, «Annual Fraud report 2019», 2020.
96 Dagens Næringsliv, «Fortviler over kryptosvindel – klager på henleggelse», 2019.
97 BBC, «Cryptoqueen: How this woman scammed the world, then vanished», 2019 and Financial Times, «Crypto scam offers modern twist on classic pyramid fraud», 2019.
98 The Norwegian Financial Supervisory Agency, «Risiko og sårbarhetsanalyse for 2018», 2019.
99 DNB, «Investeringssvindel har eksplodert», 2020.

CEO fraud

CEO fraud is perpetrated by criminals analysing an enterprise's internal organisation and manipulating employees to make transfers and/or approve payments. The perpetrators often pose as the head of the enterprise and communicate with the person in charge of the finances or the accountant. Criminal actors manipulate email accounts by forging the sender address of the email or hacking into the enterprise's computer system, so-called business email compromise (BEC). There have also been cases involving surveillance of an enterprise's email communication and manipulation over the telephone. CEO fraud has posed a major threat to Norwegian enterprises over several years.

In 2019, 13 per cent of Norwegian enterprises stated to have been subjected to CEO fraud over the last year. Large enterprises are particularly at risk, but NGOs are also targeted by such criminals. The fraud is perpetrated by organised criminal groups abroad, making investigation and tracking of transactions harder. The risk of detection and prosecution is low, weakening confidence in the police.

In 2018, losses from CEO fraud in Norway amounted to around NOK 34 million. In 2019, one single energy company was defrauded of 150 million.[100]

Reported fraud in Norway rose by 36 per cent from 2009 to 2018. As eight out of ten enterprises subjected to fraud do not report it to the police, [101] the volume of unreported crime must be great, both as regards scope and amounts lost.

Deepfake is a relatively new phenomenon where images, sound and videos are manipulated to make a face, voice or movements appear to be another person. This technique can be used in telephone conversations and on Skype, and can very easily be used for extortion, bank transfers or fake news. The required technology is available online, and the software to implement it is becoming increasingly easy to use.

It is likely that deepfake will be used against Norwegian enterprises. This will highly likely make it harder to expose CEO fraud, and the number of fraud attempts resulting in financial loss is likely to increase.

The fact that an increased number of employees work from home during the coronavirus pandemic may also make enterprises more vulnerable and raise the risk of enterprises being manipulated in this type of fraud.

100 The Norwegian Business and Industry Security Council (NSR), «Kriminalitets- og sikkerhetsundersøkelsen (KRISINO) 2019», 2019.

101 NSR, «Kriminalitets- og sikkerhetsundersøkelsen (KRISINO) 2019», 2019.

4. Pandemic and economic uncertainty

The coronavirus, first discovered in China in late 2019, has developed into a world-wide pandemic with thousands dead. Norwegian and international authorities have implemented strict measures and efforts to prevent infection that impact both business and industry and people's freedom of movement.

The measures to prevent infection have already caused share markets to fall and created economic problems worldwide. The coronavirus pandemic has also laid bare vulnerabilities in the global trade and supply chains. Interrupted deliveries from one part of the world impact production, health services and human behaviour in other parts of the world.

The IMF is expecting the greatest economic recession since the Great Depression in the 1930s. Growth is expected to pick up again once the lockdown is over. A steep decline in production is expected for Norway as well in 2020.[102] Lower house prices and many, both enterprises and employees, struggling to pay high debts are considered likely. Long-term negative effects on employment rates and production levels are also expected, and may make themselves felt for years after the coronavirus measures have been lifted.[103]

Business and industry will be severely affected. Many Norwegian enterprises are now experiencing lost incomes and strained liquidity. In the short term, the measures will be particularly serious to service industries and tourism, and for enterprises that were already struggling before the pandemic. When the restrictions are gradually lifted, businesses and industry are highly likely to see growth and employment make a comeback.[104] However, a large downturn in sales can result in many bankruptcies and a significantly reduced number of enterprises once the situation becomes more normal. However, parts of the business and industry sectors show great willingness to adjust.

Norway is one of the countries in the world best equipped to compensate enterprises for loss of income. The Government Pension Fund Global can and will be used to save many enter-

[102] IMF, «World Economic Outlook April 2020 », 2020.

[103] Dagens Næringsliv, «Regjeringens ekspertgruppe: Dette vil ulike koronascenarioer ha å si for norsk økonomi de neste ti årene», 2020.

[104] Menon Economics, «Effekt av Korona på norsk eksportrettet næringsliv», Menon-publikasjon #33/2020.

prises from bankruptcy. Many other countries are less well equipped to support its businesses and industries, and many of our trading partners will probably be worse hit by the crisis than Norway. Lower demand in other countries will impact Norwegian export industries.

As the pandemic struck the world, the price of Norway's number one export commodity, oil and gas, fell markedly due to a price war. This has resulted in price fluctuations in the securities market, falling share prices and a lower exchange rate for the Norwegian currency. The lower exchange rate is, seen in isolation, positive for the export sector, but prices on imported consumer goods rise and the buying power of Norwegians are reduced, which in turn have a negative impact on stores and jobs.

The pandemic comes on top of the world economy entering a so-called synchronised slowdown in the preceding decade.[105] The large and expansive stimulus packages are now causing state debt to grow all over the world. To finance this debt, central banks are printing money and lowering their rates. This may cause increased inflation and extend the crisis, which in turn will increase the chance of a collapse in the high-yield bond market. Should this happen, we will see the same consequences for investors in high-risk investment products that we saw during the financial crisis in 2008.[106]

Unemployment rates in Norway are already at over 10 per cent, [107] and many more are expected to lose their jobs.[108] It is particularly serious that many young people in professions characterised by workers having little education lose their jobs. These are persons at a higher risk of becoming long-term unemployed.

Even with an expected decline in financial growth going forward, the Norwegian economy will do relatively well compared with many other countries. As a country with a high degree of financial and political stability, Norway will become even more attractive for foreign investment. We can also expect that proceeds of crime will be channelled to Norway.

---

105 World Economic forum, «The Global Risks Report 2020», 2020.

106 Aftenposten, «Slik har et tiår med lave renter skapt et gjeldsberg I risikable selskaper», 2020.

107 Gross unemployment in April 2020.

108 Menon Economics, «Effekt av Korona på norsk eksportrettet næringsliv», Menon-publikasjon #33/2020.

Crisis-related crime

The coronavirus pandemic has created opportunities for criminals seeking to exploit the vulnerable situation we are in. Companies in Norway are receiving false invoices for hand disinfectant and other contagion protection equipment and abroad, fake websites and ads seemingly related to the coronavirus pandemic have been used to steal personal information.

Sale of fake health and sanitary products has risen internationally since the coronavirus outbreak.[109] In Norway, one hospital received and used pirated 3M masks, and the Customs Service has stopped the import of around 58,000 masks.[110] Several hospitals and health institutions have had health and sanitary products stolen. We also expect that medicines that may have an effect on the virus will become attractive to steal from pharmacies and that they will be traded on the black market. The struggle to get hold of health and safety products can also become a driver for crime, for instance for corruption.

The pandemic has also resulted in falling and violently fluctuating prices in the securities market. To maintain the integrity of the securities markets and the confidence of the investors, it is important that securities issuers uphold their duty to provide continuous information and handle information relating to effects, risks and measures that the outbreak imposes on enterprises. The coronavirus pandemic has raised fears for own investments, and rapid changes in information can result in more insider trading and market manipulation.

At the same time, various types of fraud are on the increase. Fraudsters exploit the reduction of stock markets arguing this is a good time to invest. DNB reports that in particular elderly are vulnerable to fraud.[111]

Crises put trust and financial sustainability to the test. We have information which indicates that employers are laying off employees, who then receive unemployment benefits, while the employees continue to work off-record, saving wages for the employer. There is also a risk that the urgent measures implemented by the Government will be abused. Abuse of unemployment benefits and stimulus packages is committed by both criminal opportunists and ordinarily law-abiding people who exploit any opportunities they see to keep their own finances or that of their enterprise afloat. We are also likely to see an increase in bankruptcy crime.

---

109 Europol, « An assessment of the impact of the COVID-19 pandemic on serious and organised crime and terrorism in the EU», 2019.

110 Dagbladet, «Stoppet 58 000 munnbind på grensa», 2020 og Aftenposten, «Sykehusansatt smittet etter bruk av falsk vernemaske: – Skyldes menneskelig svikt», 2020.

111 DNB, «Investeringssvindel har eksplodert», 2020.

Unemployment benefit fraud

Shut-down enterprises and large-scale sales and production declines in other enterprises resulting from the coronavirus pandemic have resulted in many employees being temporarily laid off. One of the urgent measures implemented by the Government was to reduce the period employers have to pay full wages to laid-off workers from 15 to two days, upon which the state starts disbursing unemployment benefits fully compensating wages up to NOK 599,148 from day 3 to day 20.[112]

ØKOKRIM has received information that some enterprises in Norway are committing benefit fraud by laying off employees who continue to work for the enterprise. It is being suspected that laid-off employees continue to work while receiving unemployment benefits and receiving wages under the table from the employer. There are also examples of employers helping foreign employees file unemployment benefit applications in return for employees working some of their hours for free. In this manner, the employer does not have to pay full wages, can offer cheaper goods and services and ensure that the enterprise can remain in operation in economically uncertain times. This method is well-known in work-related crime and can result in law-abiding enterprises being outcompeted.

In the beginning of April, the Norwegian Labour and Welfare Administration (NAV) had received 405.600 unemployment benefit applications, against 160,500 in 2019 and 166,600 in 2018 overall. [113] Extended case processing times resulted in the Government allowing NAV to disburse unemployment benefit before applications had been processed. [114] This will increase the rate at which disbursements are made and may mean that there is less control over whether unemployment benefits are merited.

In 2019, 881 persons were reported to the police for having received a total of NOK 139 million in benefits they were not entitled to. Most of the cases involved unemployment benefit fraud, with recipients not informing NAV that they had received an income.

Higher numbers of temporary lay-offs, the state fully compensating loss of income for those laid off and the decision to disburse benefits before applications have been processed are likely to cause more unemployment benefit fraud. This will cause a major loss to the welfare state and it is likely that foreign employees unaware of their rights will be exploited so that employers can profit from unemployment benefit disbursements.

112 The Norwegian Government, «Slik blir endringene i permitterings- og dagpengeregelverket», 2020.
113 The Norwegian Labour and Welfare Administration, «Statistikk - Søknader om dagpenger», 2020.
114 The Norwegian Government, «Regjeringen åpner for forskuttering av dagpenger», 2020.

Exploitation of national urgent measures

Norway is well equipped to handle an economic crisis resulting from the pandemic. With a large oil-revenue fund and a well-functioning welfare state, we can mitigate negative financial effects. On this background, the Government has created various stimulus packages for business and industry.

One of them is a compensation scheme which will entail the state covering a percentage of fixed costs, such as rent and insurance premiums, for enterprises who suffer minimum a 30 per cent drop in sales as a result of the pandemic. The scheme involves cash handouts and will disburse NOK 10–20 million per month. The scheme is initially intended to apply to March, April and May 2020, but may be extended as needed.[115]

The virus outbreak and the contagion protection measures have put enterprises in acute financial trouble. They depend on receiving money to keep renting their premises and pay insurance premiums while trying to avoid bankruptcy or letting people go. The support is based on seven principles and is intended to be quick, efficient and easy to use. A digital platform with an automated process will ensure that this is the case from receipt of the application until the money has been deposited in the enterprise's account. The scheme is subject to compliance and audits, but is to a large extent based on trusting that enterprises provide correct and exhaustive information.

The quick disbursement, the lack of bureaucracy and the trust-based approach will probably make it vulnerable to exploitation.

Compensation schemes can be abused by e.g. presenting the financial situation as more strained than is the case or by using the received funds for other purposes. Considering the amount made available, the scheme is likely to attract criminals looking to make a profit.

[115] Regjeringen, «Finansministerens innledning på pressekonferanse om kompensasjonsordning til bedrifter», 2020.

Bankruptcy crime

As a result of the coronavirus contagion protection measures, several business sectors have been ordered to shut down, and other enterprises are seeing demand drop, resulting in many now experiencing cash flow problems.

Liquidity shortages are often a driver in bankruptcy crime. Historically, financial crises have been followed by major bankruptcy crime cases. Enron in the US, Finance Credit in Norway and the bank crash in Iceland provide examples of what lies in wait. It is likely that bankruptcy crime in Norway will increase going forward as a result of the economic difficulties caused by the coronavirus pandemic.

Bankruptcy crime can be described as multi-crime linked to financial difficulties in enterprises. Large enterprises are often unlawfully bled of assets while still operating, by e.g. selling assets at lower-than-normal prices. Prior to bankruptcy being declared, credit institutions and investors are often defrauded to unlawfully inject operating capital into an enterprise which is no longer viable. Bankruptcy is also used as a tool to commit or conceal other crimes. A noted method in work-related crime is changing the registered address of an enterprise just before being declared bankrupt to exploit some police districts having less investigating capacity.

Recurring bankruptcy actors who repeatedly exploit companies and declare them bankrupt constitute a major threat to society.

Providing credit to businesses is a cornerstone of our financial system, but it entails a risk to those who lend money to and invest in enterprises. If credit providers cannot trust the information provided about an enterprise's real financial situation, this may lead to less willingness to inject capital or provide services against later payment. This may weaken the mechanisms of the market economy.

Most bankruptcies have nothing criminal about them. Going bankrupt is not a crime. The expected increase in bankruptcies will, however, make it harder to detect bankruptcy crime.

ØKOKRIM

Mailing address: Postbox 2096 Vika, NO-0125 OSLO
Visiting address: C.J. Hambros plass 2 C, NO-0164 OSLO

Contract: +47 23 29 10 00 / post.okokrim@politiet.no
Tips: +47 23 29 11 00 / desken@okokrim.no

www.okokrim.no