

Translated from Norwegian

**THE POLICE**

**PUBLIC VERSION**

# **Financially motivated sexual extortion**

**Intelligence report**



## **1. Key findings**

- Financially motivated sexual extortion, aka financial sextortion, is a global phenomenon, and several countries have recorded an increase. So has Norway. Between 01.01.23 and 31.10.24, at least 1891 Norwegians were victims of sexual extortion; 98% of them male. The number of unreported cases is very high. The victims have nothing in common, other than being male and using social media.
- Sexual extortion causes victims severe distress. The extent and severity of its impact varies from victim to victim, and may range from broken relationships, loss of employment, social isolation and anxiety to more serious reactions such as self-harm, attempted suicide and suicide.
- The criminals mainly operate from Nigeria, the Ivory Coast and the Philippines. They use slightly different methods. Those from Nigeria and the Ivory Coast tend to be lone criminals engaging in sexual extortion to supplement their income, whereas offenders from the Philippines tend to be members of an organised group, more cynical and have sexual extortion as their main source of income.
- The phenomenon will grow with the development of new technology if the authorities' response and countermeasures are inadequate. In particular, offenders may use AI to create more believable fake profiles and automate processes for wider reach and more accuracy in targeting high-status or wealthy victims.

## 2. Contents

<b>1. Key findings.....</b>	<b>2</b>
<b>2. Contents .....</b>	<b>3</b>
<b>3. Background and purpose .....</b>	<b>4</b>
3.1. Structure and scope of the report.....	4
<b>4. Information .....</b>	<b>4</b>
4.1. Method .....	4
4.2. Digital platforms .....	5
4.2.1. Image sharing.....	6
4.2.2. Payment.....	7
4.3. Methods used in specific countries.....	8
4.3.1. Nigeria .....	8
4.3.2. The Ivory Coast.....	9
4.3.3. The Philippines .....	9
4.4. Parties involved .....	10
4.4.1. Offenders .....	10
4.4.2. Victims.....	11
4.5. Impacts on victims .....	11
4.6. Prevalence .....	12
4.6.1. Unreported cases.....	12
4.7. International situation.....	13
<b>5. Drivers impacting development and prevalence .....</b>	<b>13</b>
5.1. Taking advantage of people in wealthy countries believed to be able and willing to pay .....	13
5.2. Emergence of new offenders.....	14
5.3. Artificial intelligence: a more efficient extortion process, but higher chances of detection. ....	15
5.4. High digital presence creates ample opportunities .....	15
5.5. Low detection risk and lack of countermeasures .....	16
<b>6. Assessment .....</b>	<b>17</b>
6.1. Introduction to assessments and scenarios .....	17
6.2. Scenarios .....	17
6.2.1. The most likely scenario .....	17
6.2.2. Worst-case scenario.....	17
6.3. Assessments.....	18
<b>7. Appendices .....</b>	<b>18</b>
7.1. Probability terms.....	18

### **3. Background and purpose**

Financially motivated sexual extortion is an international phenomenon reported by several countries to be a huge challenge. Both in Norway and internationally, there are examples of suicides directly due to sexual extortion. The FBI called it *the hidden pandemic*.

The spring of 2024 saw a broader analysis of the phenomenon than before based on information reported and gathered from 01.01.23 to 31.10.24. The sources are the police criminal intelligence and criminal case databases and various payment services. The external sources have been selected based on availability and relevance. We have for instance gathered information from four different payment services, but no information regarding gift cards, as this form of payment leaves few traces. The landscape may look somewhat different using other sources.

This report will describe, summarise and assess the findings relating to financially motivated sexual extortion of Norwegian victims.

#### **3.1. Structure and scope of the report**

The report has three parts. Firstly, the method used for financially motivated sexual extortion is described. Next, we will present various drivers which will, each in its own way, impact the future development and prevalence of the phenomenon. Lastly, we describe two scenarios, the most likely scenario and the worst-case scenario, followed by general assessments. The assessments have a three-year horizon.

Sexual extortion can be sexually or financially motivated. This report will only deal with financially motivated sexual extortion. Financially motivated sexual extortion is extortion where the offender threatens to share or publish sexual content unless the victim pays money.

The report will focus on financially motivated sexual extortion by offenders based abroad, but Norwegians are known to be behind some incidents.

Both adults and children fall prey to such criminals. The method described is generally applied to both groups. Where clearly different methods are used, this will be explained.

### **4. Information**

#### **4.1. Method**

Financially motivated sexual extortion is characterised by the offender contacting the victim online through social media, messaging services or dating services. The offender uses a fictitious female profile. Her conversation soon turns sexual; she often sends nude pictures of herself, and then encourages or convinces the victim to return the favour. The nude pictures or videos sent by the victim are stored by the offender.

Once the offender has received sexually explicit material, the extortion starts. The offender threatens to share the pictures or videos with the victim's friends, family or employer or to publish them on various websites unless the victim yields to the demands. If the victim pays, the extortion often continues with further demands for money. The extortion may therefore go on for a long period of time.

The victim's sexually explicit material can be shared whether money is paid or not. It varies how many people receive the sexually explicit material; there are examples of it being shared with a few individuals, and dozens of people.

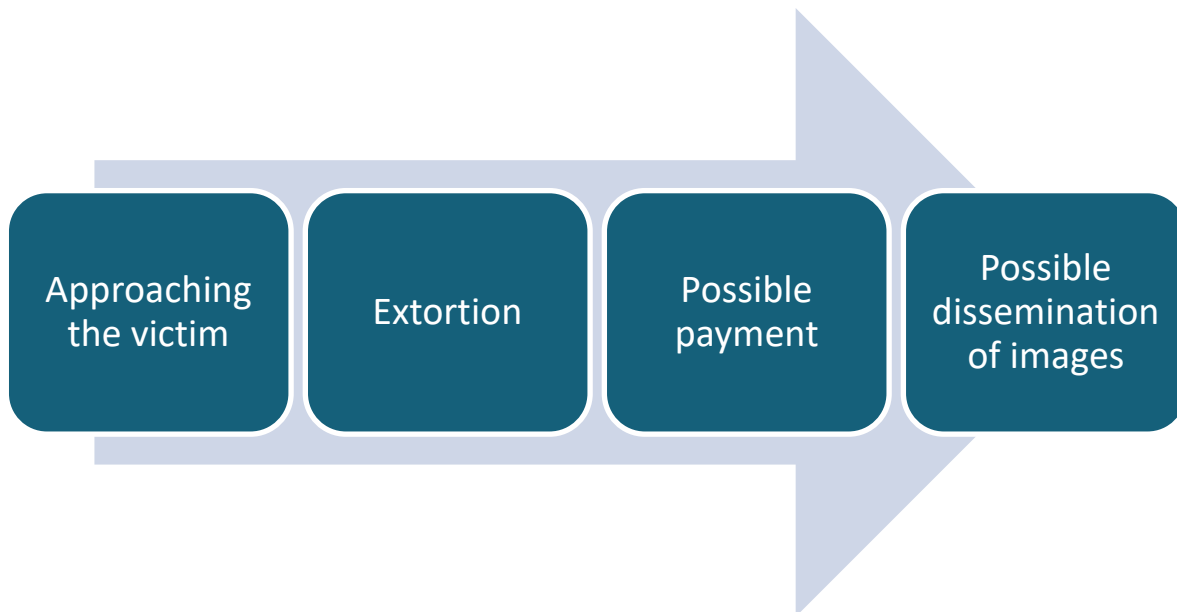


Figure 1: Illustration of the sexual extortion process.

#### 4.2. Digital platforms

Financially motivated sexual extortion consists of the stages approaching the victim, extortion, possible payment and possible dissemination of images. The different stages often take place on different platforms. This is done to maximise access to information about the victim for the purpose of extortion, but also to use the platform best suited for each stage.

For example, the approach may be made on a dating service which has limited image and video sharing features and provides limited information about the victim's social circle. For that reason, the victim often becomes friends or connects with the offender on other, more open platforms offering access to the victim's list of friends. The contact may then end up on a different platform, such as a messaging service more suited for video chatting or sharing of pictures and videos.

More than 70 different platforms used for sexual extortion have been identified. The platforms most favoured by offenders are Snapchat, Instagram, Facebook/Messenger, WhatsApp, Tinder, Happn and Telegram.

In general, children and adults are preyed upon on the same digital platforms, except for dating services, which are almost exclusively used by adults.

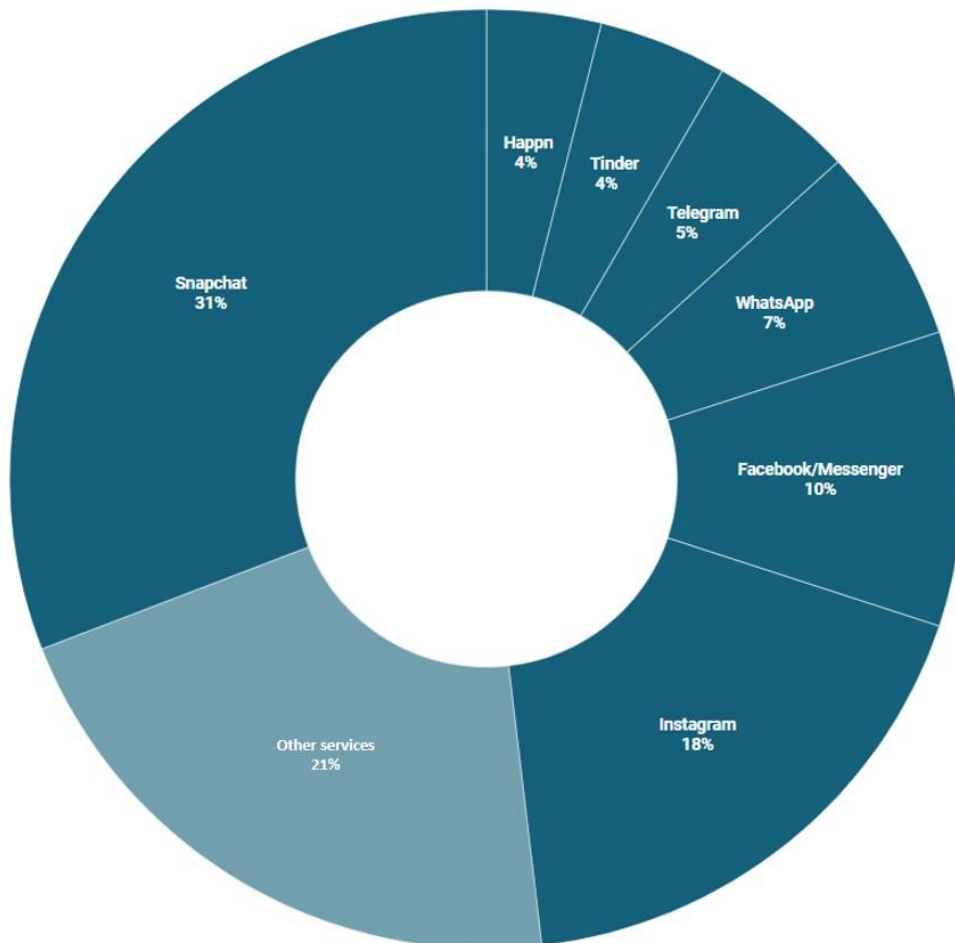


Figure 2: The shares of the most commonly used digital platforms.

#### 4.2.1. Image sharing

In more than 90% of cases, victims, both minors and adults, share genuine images of themselves, believing that they are communicating with a female. In other cases, victims report having sent nude images found online, which the offender then manipulates to look like a nude image of the victim. Some report that artificial intelligence (AI) has been used to generate synthetic nude images. There are also cases where victims report being hacked and having intimate pictures stolen by the offender.

In some cases, the offender creates an image collage of the victim by putting together several sexually explicit images of the victim with captions divulging the victim's name and phone number and alleging that he is wanted for child sexual abuse or similar, all false allegations.

No matter what method is used, it causes victims severe distress that the offender threatens to share the sexual material, in particular if the threat is carried out and the material is shared.

The sexual material is shared in at least 11% of cases, irrespective of payment status, whereas this is unknown in 85% of cases. In cases where images were shared, the victim had paid in about 30% and not paid in about 45% of cases, respectively. In many cases, it is not known if the sexual material was shared, as victims often contact the police during the extortion process and the police receive no further information from the victim

about the outcome.

#### 4.2.2. Payment

The offenders use more than 20 different payment services and methods of payment, e.g. bank transfer, digital payment services, gift cards and cryptocurrency to receive payment from victims. The most commonly used are PayPal, Remitly, cryptocurrency, gift cards, Western Union and bank transfers.

Children and adults largely use the same payment services. In several cases, minors have used digital methods of payment such as PayPal and cryptocurrency, although many of these services have a minimum age of 18.

Offenders primarily choose methods of payment based on their availability in their home countries, but they will adapt to victims' preferences. They often instruct the victim during the payment process, telling them what information to state for the payment and often demand documentation from them in the process.

If the payment somehow fails on the chosen platform, other payment platforms are tried. This process continues until the payment is successful or the victim blocks the offender. In several cases, the victim tried, and actually completed, payments using three or more payment services.

Norwegian victims have been extorted for and paid about NOK 8 million in total. Adult victims pay in about 50% of cases. Those who do pay, pay an average of NOK 10,000. Minors pay in about 20% of cases. They pay an average of NOK 2800.

Norwegian victims have paid about NOK 1 million in total to offenders from Nigeria, more than NOK 1 million to offenders from the Ivory Coast, and nearly NOK 4 million to offenders from the Philippines.

Amounts paid by victims vary, ranging from a few NOK to hundreds of thousands. Average amounts paid increase slightly with the victim's age.

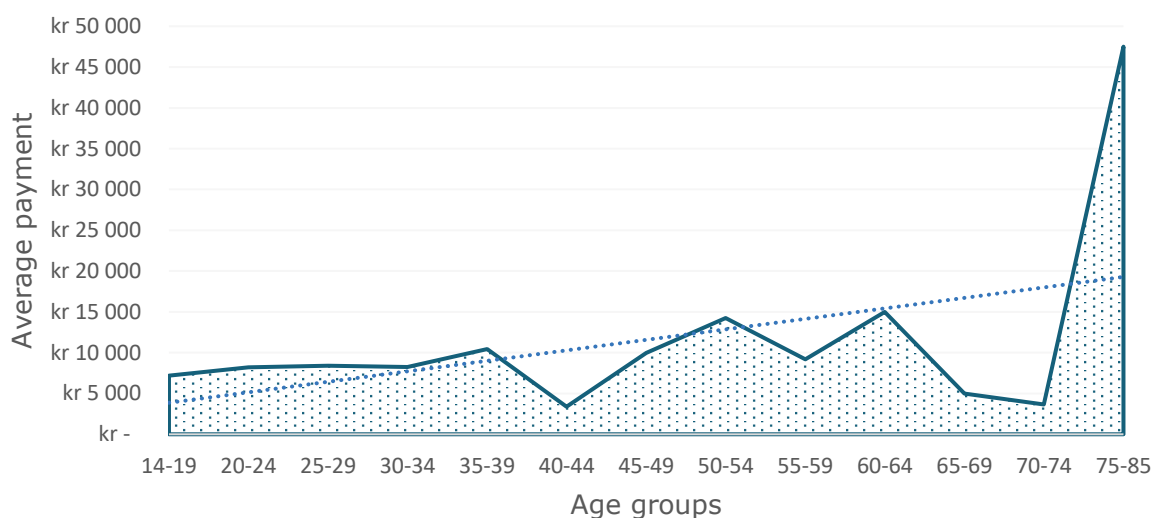


Figure 3: Average payment by victim age group.

### 4.3. Methods used in specific countries

Financially motivated sexual extortion mainly takes place from three countries. They are the Ivory Coast (8%), Nigeria (16%) and the Philippines (30%).<sup>1</sup> The FBI points to the same three countries as hotspots for financially motivated sexual extortion.<sup>2</sup> Offenders from these three countries use slightly different methods, which will be presented below.

#### 4.3.1. Nigeria

Offenders operating from Nigeria mainly use Snapchat and Instagram both to approach their victims and to extort money from them. Nigeria's official language being English, they communicate fairly well with victims in English.

Norwegian children experiencing sexual extortion are predominantly victims of Nigerian criminals, with children making up 30% of their victims. Many children use social media such as Snapchat and Instagram. They are platforms frequently used by Nigerian offenders.

In connection with the extortion, the offender sometimes alleges that the victim has sexually abused or exposed themselves to minors, and that they have the images to prove it, images which they will publish. There have also been cases where the offender offers to take over the victim's social media account instead of payment, so that the offender may use the account to extort money from more victims.

Payments to Nigeria mainly take place through PayPal, gift cards and cryptocurrency.

Due to a long history of frauds, several payment services have implemented preventive measures regarding transfers to and withdrawals of money in Nigeria. Offenders circumvent these measures by e.g. using accounts linked to other countries.

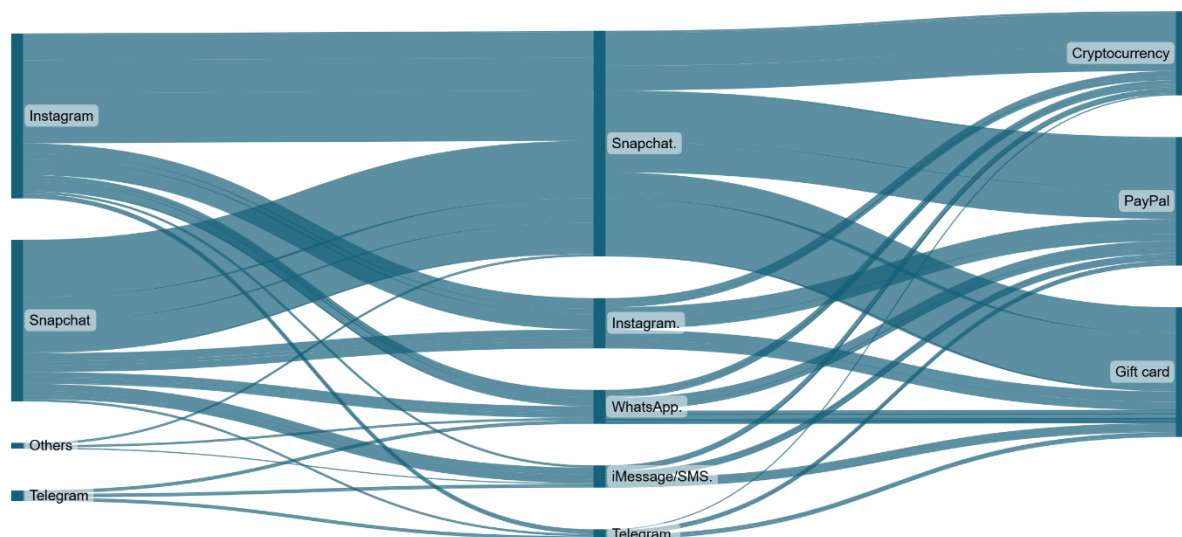


Figure 4: An outline of the extortion process of offenders from Nigeria. The diagram is read from left to right and shows the different stages from making contact to payment. The platforms used are shown in text boxes and the lines show how they are used in combination. The thickness of the lines indicates the frequency of each platform.

<sup>1</sup> In about 40% of cases, it is not known from which country the offender operates.

<sup>2</sup> <https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens>

### 4.3.2. The Ivory Coast

The great majority of offenders operating from the Ivory Coast use Facebook both to approach their victims and to extort money from them. In contrast to offenders from other countries, offenders from the Ivory Coast use fictitious profiles with traditional Norwegian names and profile pictures of apparently Norwegian women, claiming to have attended local schools and held jobs in Norway. Communication is normally in Norwegian, but at a level suggesting automated translation.

In connection with the extortion, they often threaten to publish sexual material of the victim on YouTube or in the media unless he pays up. Offenders also often appeal to their victims' conscience by claiming to have a seriously ill relative in need of money for hospital treatment.

Payment is mainly made using Remitly, PayPal and bank transfer. Offenders from the Ivory Coast sometimes use money mules. There are several examples of Norwegian victims being forced to receive payments from other Norwegian victims before the money is transferred out of Norway.

Children make up 15% of victims of offenders from the Ivory Coast.

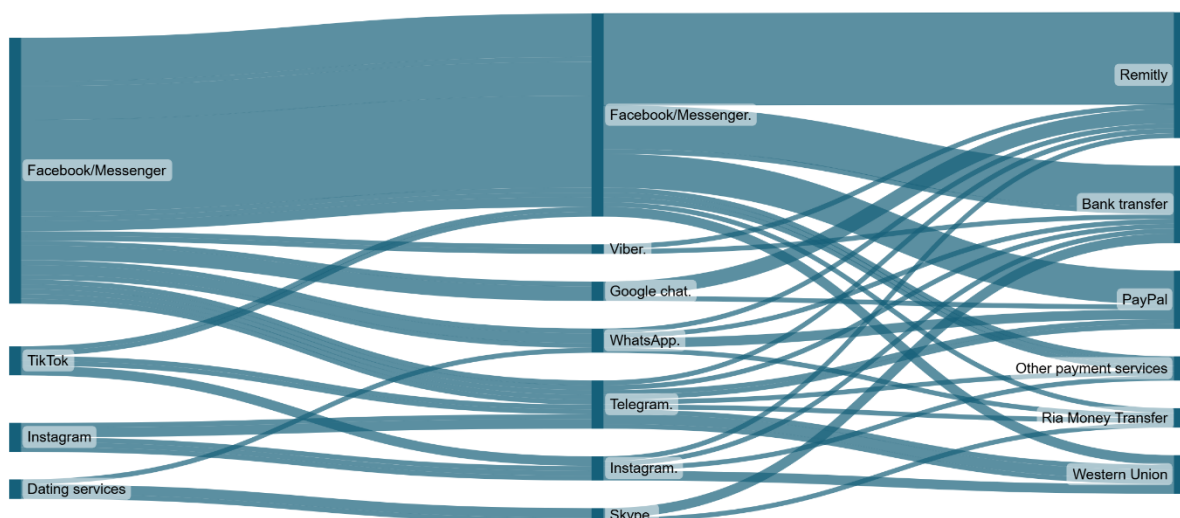


Figure 5: An outline of the extortion process of offenders from the Ivory Coast. The diagram is read from left to right and shows the different stages from making contact to payment. The platforms used are shown in text boxes and the lines show how they are used in combination. The thickness of the lines indicates the frequency of each platform.

### 4.3.3. The Philippines

Offenders operating from the Philippines predominantly use dating services for making contact, often chatting with their victims on Instagram before starting the extortion on services such as WhatsApp, Discord and Telegram.

Victims are initially blackmailed into paying to prevent distribution of the sexual material. Then, they are frequently blackmailed into paying for the material to be deleted from various folders and storage services. In some cases, the victim also paid to receive the password for storage services containing the images to be able to delete them themselves. Despite repeated payments, the password was never shared with the victim.

Payments from victims to the Philippines are mainly made through Remitly, PayPal and Western Union.

Filipino offenders top the list of offenders with Norwegian victims, but only 7% of their victims are children. The reason may be the offenders' preference for contacting victims on dating services, which are not used by children.

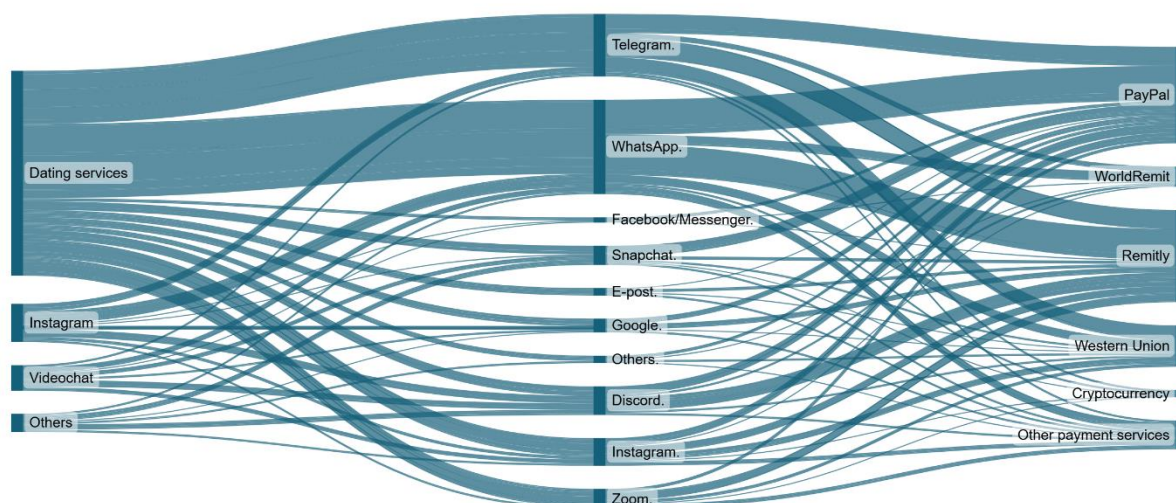


Figure 6: An outline of the extortion process for offenders from the Philippines. The diagram is read from left to right and shows the different stages from making contact to payment. The platforms used are shown in text boxes and the lines show how they are used in combination. The thickness of the lines indicates the frequency of each platform.

## 4.4. Parties involved

### 4.4.1. Offenders

The blackmailers are criminals who, through varying levels of professionalism and organisation, work for profit. The sharing of sexual material is not their goal; it is merely an effective means of making money. The offenders are cynical in their approach, playing on their victim's emotions and conscience. Many of them tell victims they are not scared of being reported to the police, being professionals who have been extorting money from victims for many years. The report *Trends in financially motivated sexual extortion* from Thorn confirms their cynicism<sup>3</sup>:

*"... the pressure [the victim] was under was unbearable to the point that during this exchange" the victim "... finally tells [the perpetrator], 'hey, I'm going to commit suicide, I'm going to kill myself,' and they respond with, 'go ahead, because you're already dead.'"*

Norway's National Criminal Investigation Service (NCIS) has carried out an analysis of offenders from the Ivory Coast, the Philippines and Nigeria. Some appear to be lone actors, while others appear more organised. The analysis shows that 139 Norwegians were victims of extortion by the same offender(s) in the Philippines.

The report *Trends in Financial Sextortion* also points out that such extortion often appears to be an organised activity where many cases use almost identical language, the same profile pictures and can very often be linked to a few international locations. The two countries most frequently linked to extortion in the report are Nigeria and the Ivory

<sup>3</sup> [https://info.thorn.org/hubfs/Research/Thorn\\_TrendsInFinancialSextortion\\_June2024.pdf](https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf)

Coast.<sup>4</sup>

#### 4.4.2. Victims

The NCIS has identified 1891 Norwegian victims during the period from 01.01.23 to 31.10.24, i.e. about 86 victims per month. Children make up 18% of victims.<sup>5</sup>

Victims are predominantly males aged 10–85, the majority 14–30. They share no obvious characteristics other than being male. They come from all walks of life, all professions and every part of Norway.

There is also a small percentage of female victims of financially motivated sexual extortion. The method used against women differs from that used for men, by offenders generally telling them they have been hacked and had sexually explicit images stolen. They are then pressured into paying to prevent the distribution of this material.

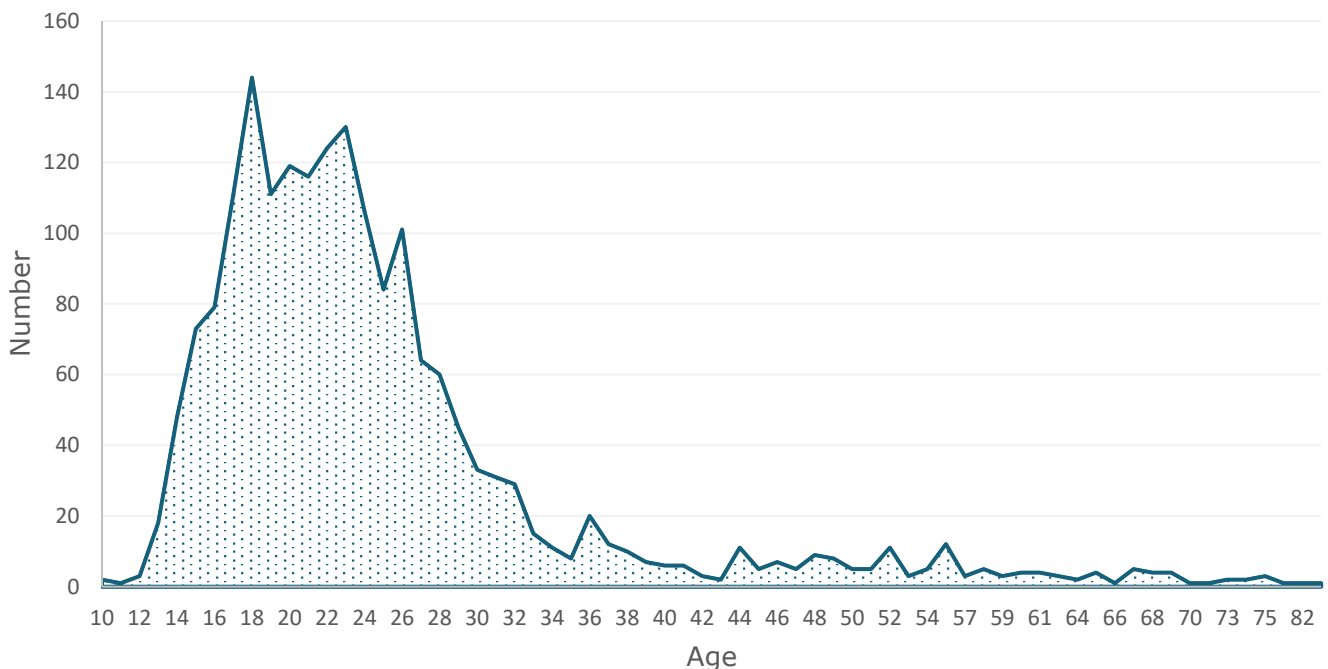


Figure 7: Age distribution of victims

#### 4.5. Impacts on victims

Financially motivated sexual extortion can cause victims severe distress. On average, it takes 45 minutes from approach to extortion, but there are several examples of victims living under the offender's control for weeks, months and even more than one year.

In 2017, a Norwegian boy killed himself shortly after becoming a victim of sexual extortion. No further suicides caused by sexual extortion have been recorded in Norway since then. Still, financially motivated sexual extortion severely impacts most victims, be they children or adults. Examples of common reactions are shame, social isolation, problems concentrating, problems sleeping, physical reactions such as vomiting due to stress, broken relationships, loss of employment and gambling addiction, but some have

<sup>4</sup> [https://info.thorn.org/hubfs/Research/Thorn\\_TrendsInFinancialSextortion\\_June2024.pdf](https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf)

<sup>5</sup> 18% represents 335 children.

even more serious reactions such as self-harm, suicidal thoughts and attempted suicide. Sometimes these reactions lead to emergency hospitalisation. Thorn reports that about one sixth (17.5%) of financially motivated sexual extortion victims experience thoughts of self-harm or suicide.<sup>6</sup>

The Norwegian Centre for Violence and Traumatic Stress Studies reports that image-based sexual abuse (IBSA)<sup>7</sup> may impact victims in numerous ways, both psychologically, socially and physiologically. Potential psychological reactions may range from feeling strange and uncomfortable, shame, stress, anger, humiliation, guilt, loss of control and shock, to mental ill-health such as anxiety and depression, including suicidal thoughts and self-harm. Social consequences may be isolation, harassment, bullying, spreading of rumours and lack of trust, while physiological reactions may be weariness, weight change, poor concentration and poor performance at e.g. school.<sup>8</sup>

In March of 2022, the FBI observed a sharp increase in the prevalence of financially motivated sexual extortion. Reviewing 13,000 reports of extortion during the period from October 2021 to March 2023, the FBI and Homeland Security Investigations (HSI) found over 20 cases of suicide among victims, i.e. in 0.15% of cases.<sup>9</sup>

#### **4.6. Prevalence**

It is hard to estimate the true prevalence of financially motivated sexual extortion. In many cases, incidents go unreported; in other cases, they are reported to friends or other confidants, various support services or the police.

##### **4.6.1. Unreported cases**

The number of unreported cases of financially motivated sexual extortion is very high. Research shows that men often find it extremely difficult to open up about sexual abuse for reasons such as cultural and social expectations of masculinity, feeling ashamed and fear of stigma. That may lead to men tending to undercommunicate or not report such experiences until many years later. Figures from Norway and international studies show that men also report sexual abuse to a lesser extent, a tendency reflecting their fear of not being believed or the incident becoming public knowledge.<sup>10</sup> Many victims therefore keep the abuse they have suffered to themselves, while some confide in close family or friends and others contact support services or the police.

Of several hundred Norwegian victims identified by the NCIS through sources other than police systems, only about 5% had reported the incident.

In 2023, the US National Center for Missing and Exploited Children (NCMEC) received 26,600 reports of financially motivated sexual extortion of children. Children make up 18% of Norwegian victims, about one fifth. Based on these figures, the estimated total number of reported incidents worldwide, including adult victims, is 133,000 annually. In

---

<sup>6</sup> [https://info.thorn.org/hubfs/Research/Thorn\\_TrendsInFinancialSextortion\\_June2024.pdf](https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf)

<sup>7</sup> IBSA: Sharing, or threatening to share, nude or other sexual images without consent.

<sup>8</sup> <https://www.nkvts.no/content/uploads/2024/01/NKVTS-Rapport-3-2023-Digitale-seksuelle-overgrep-mot-barn-og-unge.pdf>

<sup>9</sup> <https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens>

<sup>10</sup> <https://www.fhi.no/he/folkehelse/rapporten/skader/vold/?term=https://uni.oslomet.no/voldsprogrammet/2021/11/01/ny-studie-digitale-overgrep-er-na-er-nesten-like-vanlige-som-fysiske/>

addition, there are the unreported cases.

#### 4.7. International situation

Financially motivated sexual extortion is a global challenge and several countries are recording an increase in reported cases.<sup>11</sup>

Between 2021 and 2022, NCMEC reports regarding such extortion rose by 7200%. They more than doubled from 2022 to 2023, from about 10,700 to 26,718.<sup>12</sup> Between August 2022 and August 2023, NCMEC received an average of 812 reports of sexual extortion per week, more than two thirds of which were financially motivated cases. Instagram and Snapchat were the most commonly used platforms. In addition, NCMEC has recorded an increase in the use of end-to-end encrypted platforms.<sup>13</sup>

Thorn's key findings in the report *Trends in Financial Sextortion* show that financially motivated sexual extortion continues to be a major and ongoing threat. Perpetrators leverage tactics to intentionally fan a victim's worry about the life-changing impacts of their nudes being shared – often repeating claims that it will "ruin their lives". The report further points out that there are reasons to worry about whether digital platforms are underreporting.<sup>14</sup>

From August 2022 to March 2023, the FBI saw a 20% increase in reported cases of financially motivated sexual extortion of minors, compared to previous years.<sup>15</sup>

Europol also reports that financially motivated sexual extortion is a persistent problem, and that the extortion process may go on for an extended period of time. They point out that cybercriminals involved in child sexual exploitation and online fraud will continue to take advantage of deepfake technology as its quality improves and it becomes more accessible and user-friendly.<sup>16</sup>

## 5. Drivers impacting development and prevalence

This section will discuss a number of drivers that may impact the development of financially motivated sexual extortion. These drivers will be taken into account in the scenarios described in the next chapter. Each driver is assessed separately.

### 5.1. Taking advantage of people in wealthy countries believed to be able and willing to pay

The Philippines, Nigeria and the Ivory Coast have relatively low gross national incomes (GNI) per capita compared to Asia and Africa in general. They are far behind Europe in GNI per capita. Europe is far higher on the list due to industrialisation, technology and a

---

<sup>11</sup> <https://www.weprotect.org/thematic/sextortion/>

<sup>12</sup> <https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf>

<sup>13</sup> <https://www.missingkids.org/blog/2024/where-is-sextortion-happening-new-trends-growing-crisis>

<sup>14</sup> [https://info.thorn.org/hubfs/Research/Thorn\\_TrendsInFinancialSextortion\\_June2024.pdf](https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf)

<sup>15</sup> <https://www.nprillinois.org/equity-justice/2024-01-25/fbi-warns-about-growing-threat-of-sextortion>

<sup>16</sup>

<https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf>

mature economic development.<sup>17</sup> Countries such as the Philippines, Nigeria and the Ivory Coast also score high on Unesco's Corruption Perceptions Index.<sup>18</sup> Coupled with weak legal systems, this lowers the risk of arrest and prosecution for financial crimes.<sup>19</sup>

Norway has a solid, independent economy and a GNI per capita which is among the highest in Europe, 112% above the EU average.<sup>20</sup> Norwegians also have easy access to various payment services, and it is easy both for children and adults to send money out of the country. This may reflect high solvency. Offenders appear to have insight into the economy in Europe and deliberately target Norway in many cases. Several offenders use social media accounts and dating platforms with manipulated location data showing a location in Norway, and claim to live in Norway. In several cases, they also get many local friends on social media, making the profile appear integrated in the local community and raising its credibility.

Norwegians can also be assumed to be willing to pay, as sexual extortion is a social taboo and victims feel very ashamed. Having their nude images shared may greatly impact victims, socially as well as career-wise, and may make boys and men easy to take advantage of.

**Point assessment:** It is *likely* that offenders have knowledge of the economy in Europe in general and Norway in particular and hence often deliberately target Norwegians. The global economic gap will *highly likely* continue to be a driver going forward. Many countries have GNIs as low as Nigeria, the Ivory Coast and the Philippines. As long as profits remain high, it is *likely* that actors from other countries may use the method. Our assessment is that Norwegians are *likely* ready to pay to avoid or lessen the consequences. **End of point assessment.**

## 5.2. Emergence of new offenders

Guides describing how to commit financially motivated sexual extortion with ease are sold and shared online. Knowledge of the method is also shared between friends and members of communities. The phenomenon has received considerable media attention too, potentially making more people aware of this opportunity to make easy money.

New actors emerge, offering the development of new technologies to be applied for more efficient commission of financially motivated sexual extortion. This includes the development of AI agents<sup>21</sup> for use in automated processes. The threshold for committing cybercrime lowers as the technology becomes more accessible and user-friendly. It is relatively easy to take advantage of various AI services to achieve the desired results, despite several providers setting restrictions for their services.

**Point assessment:** There is an *even chance* that financially motivated sexual extortion will spread to new actors, including organised crime groups in Europe. The reason is that potential profits are high, the required technology easily available and the set-up costs for the enterprise low. Descriptions of the method are also readily available. **End of**

---

<sup>17</sup> [www.statista.com](https://www.statista.com)

<sup>18</sup> <https://www.unesco.org/en/world-media-trends/corruption-perceptions-index>

<sup>19</sup> <https://worldjusticeproject.org/rule-of-law-index/global>

<sup>20</sup> <https://www.ssb.no/priser-og-prisindekser/konsumpriser/statistikk/sammenlikning-av-prisniva-i-europa/artikler/norges-bnp-mer-enn-det-doble-av-eu-snittet>

<sup>21</sup> NCIS: Cybercrime 2024 Source: <https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf>

**point assessment.****5.3. Artificial intelligence: a more efficient extortion process, but higher chances of detection.**

The generation of synthetic sexual material<sup>22</sup> showing victims can make extortion more efficient, as offenders no longer need actual intimate images shared by victims.<sup>23</sup> On the other hand, it may lead to immunity where victims feel less pressured into paying, as the general volumes of synthetic material will be high and there is greater public awareness of and openness about this common threat.

AI helps fake offender profiles appear more genuine using a larger image gallery of the 'girl' they pose as, better and more varied language in chats, and language adapted to the age of each individual victim. Offenders will instantly appear more trustworthy when they contact new victims and may gain their trust more quickly.

AI may also be used to more accurately and efficiently detect financially motivated sexual extortion and help prevent and uncover it at an earlier stage, and to a higher degree. As a result, the phenomenon may seem to be on the increase, while in reality, unreported cases are being detected.

**Point assessment:** AI will continue to evolve and provide more opportunities. It is *likely* that AI will increase the actual and reported prevalence of sexual extortion. It is *likely* that individuals will find it harder to recognise fake profiles due to the higher quality of the approach, and thus, more people will fall victim. **End of point assessment.**

**5.4. High digital presence creates ample opportunities**

Statistics from 2023 show that 88% of Norwegians aged 16–79 use social media, an 8% increase over the past five years.<sup>24</sup> So Norwegians, including children, have easy access to technology and social media. According to the 2024 Children and Media Survey, almost all 9-year-olds in Norway have access to a mobile phone, and more than 90% to a computer, either a school or a home computer.<sup>25</sup>

In recent years, an increasing number of children have shared sexually explicit material, of themselves and others, with other individuals and groups on social media. This phenomenon has been termed a culture of sharing.<sup>26</sup> Nevertheless, the 2024 Children and Media Survey showed that the percentage of children who report having shared nude images of themselves over the past year has dropped to 9%, from 15% in the 2022 survey.<sup>27</sup>

---

<sup>22</sup> Fake nude images or similar

<sup>23</sup> <https://arxiv.org/pdf/2406.13843#page=11.35>

<sup>24</sup> <https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene/artikler/ni-av-ti-nordmenn-bruker-sosiale-medier>

<sup>25</sup> The Norwegian Media Authority. Children and Media 2024. Topic report: Children and young people's media habits and access to technology. Source: <https://www.medietilsynet.no/fakta/rapporter/barn-og-medier/barn-medievaner-2024/>

<sup>26</sup> Police Threat Assessment 2024. Source: <https://www.politiet.no/globalassets/tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2024.pdf>

<sup>27</sup> The Norwegian Media Authority. Children and media 2024 – a survey of the media habits of 9–18-year-olds. Source: [https://www.medietilsynet.no/globalassets/publikasjoner/publikasjoner/barn-og-medier-undersokelser/2024/241128\\_barn\\_og\\_medier\\_2024.pdf](https://www.medietilsynet.no/globalassets/publikasjoner/publikasjoner/barn-og-medier-undersokelser/2024/241128_barn_og_medier_2024.pdf)

Studies show a clear increase in children's and young people's sexual exploration and development on digital platforms, and social media play a large part in their exposure to sexual content, unsolicited approaches and sexual abuse.<sup>28</sup> The fact that many young people have already shared intimate images of themselves online makes them vulnerable to distribution of the images and extortion, now or in future.

The high digital presence of Norwegians is also reflected in the dating market, which has become digitalized to a large extent. 70% of young Norwegian use, or have used, dating apps, and only 7% of young adults find partners on the town. Meeting potential new partners behind a screen may feel safer, but studies show that on dating apps, users experience a higher level of rejections, which may take its toll on the self-confidence needed to meet new partners in real life.<sup>29</sup>

The digital shift in the dating market may hence involve a number of challenges. Research e.g. shows that a large group of boys and men in Norway live in involuntary celibacy, so-called incels. They struggle with their body image, self-confidence, anger issues and loneliness, and connect with like-minded people online.<sup>30</sup> The past year has seen a lively media debate on the dysfunctional dating market which leaves many men without their desired access to women.<sup>31</sup> Such lack of access to women may be a factor making these men and boys extra vulnerable and easy targets for extortion.

**Point assessment:** A very high digital presence means ample opportunities for sexual extortion. It is *likely* that Norwegian children are victims of financially motivated sexual extortion due to their high digital presence, not because they are deliberately targeted. The fact that many boys and men are already in a vulnerable position and/or feeling lonely, coupled with the fact that sexual exploration and dating have largely moved online, makes it *likely* that potential victims will be easier to lure into an extortion situation, as offenders play on exactly these vulnerability factors. **End of point assessment.**

## 5.5. Low detection risk and lack of countermeasures

Both the actual and perceived detection risk for perpetrators of financially motivated sexual extortion are low. The identification of offenders is difficult for various reasons, including limited chances of identification of telephone and IP subscriptions, low priority by the police in the offender's home country, and barriers in international cooperation such as differences in legislation, working methods and language.

<sup>28</sup> <https://oda.oslomet.no/oda-xmlui/bitstream/handle/11250/2755418/NOVA-Rapport-3-2021.pdf?sequence=1&isAllowed=y>  
<https://www.nkvt.no/>

<sup>29</sup> [https://www.nrk.no/trondelag/sjekke-opp-noen\\_-mange-jenter-blir-overrasket-nar-kim-hamre-sjekker-dem-opp-pa-byen-1.16721827](https://www.nrk.no/trondelag/sjekke-opp-noen_-mange-jenter-blir-overrasket-nar-kim-hamre-sjekker-dem-opp-pa-byen-1.16721827)

<sup>30</sup> <https://psykologisk.no/2022/02/for-forste-gang-har-incels-i-norge-blitt-kartlagt-av-og-til-ma-man-forske-pa-menn/> // <https://www.forskning.no/kjonn-og-samfunn-om-forskning-psykologi/incels-i-norge-vi-vet-for-lite-og-gjor-ikke-nok/1899491#:~:text=Incel%20st%C3%A5r%20for%20%C2%ABinvoluntary%20celibate%C2%BB%2C%20eller%20ufrivillig%20s%C3%B8libat%2C,qjerne%20beskrevet%20som%20ekstrem%20og%20hatefull%20overfor%20kvinner>

<sup>31</sup> [https://www.aftenposten.no/meninger/kronikk/i/dRLdeB/mads-larsen-singel-dating-barnloeshet?utm\\_source=iosapp&utm\\_medium=share](https://www.aftenposten.no/meninger/kronikk/i/dRLdeB/mads-larsen-singel-dating-barnloeshet?utm_source=iosapp&utm_medium=share)  
<https://psycnet.apa.org/fulltext/2024-78558-001.pdf>  
<https://www.nrk.no/livsstil/slik-kartla-vi-det-nye-singel-norge-1.15714921>  
<https://www.vg.no/helse/i/76o59K/faar-ikke-sex-slik-unngaar-du-ufrivillig-soelibat>

Some established service providers have over the past year updated their services to enhance users' privacy and security. But this makes the detection of sexual extortion more difficult, because communication between users is encrypted. When the content of chats is encrypted, it cannot be scanned for sexual language or child sexual abuse material. For example, Meta has implemented end-to-end encryption for Messenger, making a vast amount of communication and file exchange invisible for detection.<sup>32</sup> Meta argues that end-to-end encryption gives users an extra layer of security and improved privacy.<sup>33</sup>

**Point assessment:** It is *likely* that more and more platforms will implement encryption technologies, which will hamper detection and prosecution. **End of point assessment.**

## 6. Assessment

### 6.1. Introduction to assessments and scenarios

This chapter describes two scenarios and provides overall, general assessments that apply to the whole report.

The scenarios and assessments have a three-year horizon.

### 6.2. Scenarios

Four different scenarios have been painted, the most likely of which is presented below.

#### 6.2.1. The most likely scenario

Cases of financially motivated sexual extortion are on the rise in Norway, of children and adults alike. Blackmailers use AI to generate believable profiles with tailored language and home locations. While AI boosts detection rates, the encryption of many platforms weakens this effect. The perpetrators of sexual extortion come from several new countries and continents and adapt to countermeasures by improving their operational security. The ubiquity of sexual extortion has made some victims less willing to pay because threats to publish nude images no longer scare victims as much. Also, the quality of synthetic nude images is so good that some victims who have their images published claim they are fake.

#### 6.2.2. Worst-case scenario

There is a sharp increase in the prevalence of financially motivated sexual extortion in Norway, of children and adults alike. Automated processes can be used for contacting victims with tailored communication. Offenders systematically scan potential victims to target their attacks. Having your nude images shared is still associated with shame. Overall, the development has resulted in high profits and high pressure on victims. Moreover, offenders use more cynical and lengthy methods, which has led to higher victim suicide rates.

---

<sup>32</sup> <https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/amp/>

<sup>33</sup> <https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/amp/>

Perpetrators of financially motivated sexual extortion are hard to identify and few are prosecuted. They are based across the globe, both lone actors and organised criminal networks. Their diverse locations make it difficult to target measures.

### 6.3. Assessments

It is *likely* that the prevalence of financially motivated sexual extortion will continue to rise due to a low detection risk and high profits.

It is *highly likely* that the number of unreported cases is very high, as it is a taboo subject and difficult to talk about among boys and men. Few victims report the matter to the police.

Offenders operate on various digital platforms. It is *likely* that minors are random victims because they use a service frequented by offenders. It is *likely* that Nigerian offenders have more child victims because they prey on users of Snapchat and Instagram etc., whereas Filipino offenders *likely* have the fewest child victims because they chiefly approach victims on dating services.

There is an *even chance* that victims continue to feel intimidated by the threat of having their nude images shared and remain willing to pay. But there is also an *even chance* that due to increased public awareness of extortion and the rising volumes of synthetic nude images, victims will perceive it as normal and be less ready to pay. It is *likely* that both reactions will occur among different victims.

It is *likely* that financially motivated sexual extortion will continue to have a severe impact on victims. It is *likely* that several Norwegian victims have been or will be driven to suicide by extortion, without the cause being identified.

The phenomenon will grow with the development of new technology if the authorities' response and countermeasures are inadequate. It is *likely* that offenders may use AI to generate more believable fake profiles, to automate processes for wider reach and more accurately target high-status or wealthy victims.

Despite the majority of offenders operating from Nigeria, the Ivory Coast and the Philippines, some perpetrators from other countries have been identified, including Norway. Financially motivated sexual extortion receives regular media attention, requires no particular preparations and carries low risk. It is *likely* that lone actors and organised crime groups in Europe will engage more in financially motivated sexual extortion to make money. There is an *even chance* that they will be more successful due to their knowledge of European systems and culture and better technological know-how. But there is also an *even chance* that several European organised actors are already engaging in such extortion, unbeknownst to us.

## 7. Appendices

### 7.1. Probability terms

Assessments are invariably associated with some degree of uncertainty. To handle this uncertainty in a standardised and coherent manner, we have used probability levels (see table).

<b>National standard</b>	<b>Description</b>	<b>NATO standard</b>
<i>Highly likely</i>	There is very good reason to expect ...	Highly likely (>90%)
<i>Likely</i>	There is reason to expect ...	Likely (60–90%)
<i>Even chance</i>	There is an even chance ...	Even chance (40–60%)
<i>Unlikely</i>	There is little reason to expect ...	Unlikely (10–40%)
<i>Highly unlikely</i>	There is very little reason to expect ...	Highly unlikely <10%