

\_\_\_\_\_

STATE PROSECUTOR FOR SERIOUS ECONOMIC AND INTERNATIONAL CRIME

KAMPMANNSGADE 1 1604 COPENHAGEN V

TELEPHONE +45 72 68 90 00 FAX +45 45 15 00 16

E-mail: saoek@ankl.dk www.anklagemyndigheden.dk www.politi.dk

# **Money Laundering in Denmark National Risk Assessment 2018**

### Contents

| 1.  | Foreword  |
|-----|---|
| 2.  | Summary   |
| 3.  | Introduction7   |
| V   | Vhat is money laundering?   |
| 4.  | Consequences for society  |
| F   | redicate offences and derivative crime11                            |
| S   | tructural and economic consequences11                               |
| 5.  | Methods and data applied in the risk assessment                     |
| I   | dentifying threats and vulnerabilities14                            |
| A   | analysis of threats and vulnerabilities                             |
| 6.  | Conditions in society   |
| A   | ML legislation, the Money Laundering Directive and the AML strategy |
| I   | nternational cooperation17  |
| F   | inancial factors  |
| S   | ocial factors   |
| Т   | echnological factors  |
| 7.  | Trends in profit-driven crime                                       |
| A   | Actors in profit-driven crime                                       |
| C   | Current crime trends  |
| F   | uture crime trends  |
| 8.  | Convictions for handling stolen property                            |
| 9.  | Analysis and assessments (not publicly available)                   |
| 10. | Literature  |
| Ap  | pendix 1: Concepts and definitions                                  |

### 1. Foreword

Laundering the proceeds of crime is a serious societal problem that underpins criminal activity and undermines the integrity of the financial system, and thereby also the safety and security of our society. Money laundering is also a complex problem because it often involves methods from both the legal and the illegal economy to conceal criminal activity.

The key risk factors associated with the spread of laundering must be identified and analysed in order to effectively prevent and combat money laundering. National risk assessment is a core element of this risk-based approach to combating money laundering.

The first national risk assessment of money laundering was published in 2015. The authorities and private actors involved with preventing and combating money laundering face increasingly higher demands as criminals employ ever-more sophisticated methods, and the number of cases, particularly of economic IT crime, has risen sharply. Moreover, in recent years several major laundering cases have intensified the focus on fighting money laundering and illuminated the need for stronger collaboration between the authorities and private actors in this area.

Accordingly, the risk assessment for 2018 is based on a new, improved risk model intended to provide authorities and private actors with greater insight into the analytical basis and enable them to better and more swiftly identify new money laundering trends. The model has been used to analyse and assess the laundering risk in a number of specifically identified risk areas.

In the process of preparing the risk assessment, emphasis has been laid on involving relevant authorities as well as public- and private-sector cooperative partners, including representatives of banks and other institutions subject to the duty of reporting. All these entities have helped raise the quality of the national risk assessment, making it more targeted for the work of preventing and combating money laundering.

In this connection the State Prosecutor's Office (SØIK) would like to thank all those who have helped prepare this risk assessment.

Morten Niels Jakobsen

State Prosecutor for Serious Economic and International Crime

### 2. Summary

The purpose of the national risk assessment of money laundering is to determine the risk of money laundering and to identify the risk areas of preference that are particularly vulnerable to exploitation for money laundering purposes in Denmark.

The analysis of the identified risk areas assesses whether some areas are more attractive for laundering purposes than others. The areas generally assessed to have the highest money laundering risk are:

- Money remittance providers and alternative money remitters are often used by organised criminals to launder funds originating from criminal activities. Money remittance providers, including alternative remitters like *hawala*, can be used to transfer illegitimate funds to countries without a modern, formal banking sector and where anti-money laundering control is weak. Small money remittance providers and alternative remitters find compliance with antimoney laundering obligations particularly challenging. They are also harder to control and oversee than larger chain operators and their agents. The area is categorised as high-risk because many money remitters fail to register as required with the authorities, making crime detection difficult, and because the likelihood of prosecution and conviction is low, particularly in cases with an international dimension.
- > Currency exchange providers are used for money laundering in many criminal environments. One method is to exchange small-denomination banknotes acquired through unlawful activities into high-denomination banknotes. The 500 euro note has been particularly popular, but the EU decided to phase it out at the end of 2018. Exchanging funds into higher-denomination banknotes makes it easier for criminals to store or transport money out of the country, because the notes take up less physical space. The risk area is assessed as being easy to use and highly attractive because it offers the possibility of maintaining anonymity, and because using a currency exchange provider requires neither special knowledge nor planning. Criminals in this area have also been known to establish their own currency exchange offices, which makes it an attractive and easy method to use. 'Unofficial' currency exchange providers that have not applied for a licence to offer currency exchange services do thus exist and usually operate via smaller businesses. All else being equal, these constitute a higher money laundering risk. The area is assessed to be a high-risk area, in line with the findings of the last risk assessment. However, it should be noted that the focus on currency exchange providers has intensified since the last risk assessment. Monitoring of the area has also been transferred from the Business Authority to the Danish FSA, which, among other things, has led to the issue of fewer licences to operate a currency exchange business.

- Legal business structures are used in many criminal circles and at all stages of the laundering process. The method is especially used in subcontractor fraud and VAT carousels, where fictitious invoices are issued for work never carried out. Examples have been seen of criminals who either set up their own active companies or take over existing companies used for money laundering. Frontmen have also been known to be appointed as owners or directors in order to conceal the identity of the beneficial ownership and the real decision makers, enabling criminal actors to maintain their anonymity. Proceeds can also be laundered via smaller legal business structures through trade-based laundering. In this scenario, legitimate and illegitimate funds are combined, whereby all the funds ultimately appear legal. The area is categorised as a high-risk area, as it is assessed as being highly attractive for money laundering, and the risk of detection is low. As no supervisory authority proper exists for this money laundering area, the authorities often need to take thorough control measures to detect and identify this type of laundering.
- Physical cross-border transfer of currency is estimated to be used extensively to channel the proceeds of crime out of Denmark for potential placement in countries with weaker AML control. Banks continuously upgrade their procedures for monitoring suspicious transactions, making it more complicated for criminals to transfer funds via the financial system, for which reason they turn to alternative methods. Physical transport is relatively easy and requires little planning. This is assessed to be a high-risk area, partly because of the low risk of detection, particularly when currency is physically carried across border crossing points on land or at sea. It is also difficult to deduce the predicate offence of money laundering and thus determine the origin of the funds, because cash funds are non-traceable. European-level efforts are underway to amend the legislation regarding the control of cash leaving or entering the Community. Greater collaboration between authorities will be among the changes introduced.

Land-based betting, which refers to betting in which gambling provider and gambler meet physically, includes the buying and selling of receipts of winnings from land-based betting. This laundering method is popular in many criminal environments where receipts of winnings are traded to give the proceeds of crime the appearance of legitimate gambling winnings. This method was previously used primarily to launder cash originating from drug crime, but other criminal environments have also started taking advantage of the method. There are also instances of retailers and providers of land-based betting that facilitate laundering either by assisting criminals to bypass know-your-customer (KYC) procedures or by buying up receipts of winnings for resale. Money laundering via land-based betting is assessed as being easy to use because it requires neither special planning nor knowledge. It is furthermore attractive because it is fairly inexpensive and makes maintaining anonymity relatively easy. The risk of detection is low, partly because it is the gambling provider, rather than the retailer of land-based betting, that is subject to the obligations imposed by the Anti-Money Laundering Act.

### 3. Introduction

Money laundering activities play an important role in facilitating organised crime, both nationally and internationally, but it is extremely difficult to quantify the extent of these activities<sup>1</sup>. According to the Basel Institute on Governance (2016), no national or international data exist for adequately calculating the extent of money laundering.

According to a Europol report (2017) the primary criminal areas that use laundering to disguise the origin of funds are drug smuggling, migrant smuggling, human trafficking, cyber-crime, various forms of fraud (CEO fraud, document forgery, etc.) and trading in legal and illegal goods. The process used to launder the proceeds of serious and organised crime involves a variety of methods, which are often quite complex and combine elements from both the legal and the illegal economy. The commingling of illegal and legal transactions takes place inter alia through banks, currency exchange offices, gambling providers, payment institutions, money remittance providers and a range of business structures.

According to the Financial Action Task Force (FATF)<sup>2</sup>, a national risk assessment constitutes the foundation of a risk-based approach to preventing and fighting money laundering. The ongoing identification, assessment and, not least, understanding of laundering risks are thus key to implementing efficient measures in the area.

The first national risk assessment was published in 2015 (State Prosecutor's Office 2015), and the new edition is a development that builds on methodological improvements, particularly at the identification stage, and greater transparency underlying the risk assessments. Again, the purpose of the national risk assessment is to determine the risk of money laundering and to identify the risk areas – sectors, systems, products and services – preferred for and particularly vulnerable to exploitation for money laundering in Denmark.

The national risk assessment is intended for the use of the supervisory authorities as well as the reporting undertakings and individuals (see section 1 of the Anti-Money Laundering Act). Both supervisory authorities and reporting entities are expected to use the risk assessment to take a risk-based approach to their work and to develop their own risk assessments within their respective sectors (see the legislative material for 2016/1 LSF41, paragraph 3.4, the Anti-Money Laundering Act). The risk assessment is additionally intended for use by the Danish police and the prosecution service, as it

<sup>&</sup>lt;sup>1</sup> Calculations from an international research project show that the money laundering potential in Denmark is approx. EUR 2.7 bn (Utrecht University 2013). A later report shows that illegal markets in Denmark generate approx. EUR 1.6 bn (Savona, Ernesto U. & Riccardi, Michele 2015). The calculations in both reports are based on information now almost 10 years old, for which reason the big difference in estimated money laundering potential must be ascribed to the choice of method.

<sup>&</sup>lt;sup>2</sup> The FATF is an inter-governmental collaboration forum under the auspices of the OECD that deals with developing recommendations on how to combat money laundering and terrorist financing.

may help clarify which methods can currently be used to launder the proceeds of crime. At the same time, the report will promote greater public insight into money laundering, thus providing policy makers, authorities and the private sector with a better basis for planning anti-money laundering work and developing preventive strategies that can curb and reduce the extent of money laundering in Denmark.

#### What is money laundering?

The Anti-Money Laundering Act defines money laundering as:

- 1. unlawfully accepting or acquiring for oneself or others a share in profits or funds obtained by a punishable violation of the law,
- 2. unlawfully concealing, keeping, transporting, helping with the disposal of or in a similar manner subsequently assisting in securing the profits or funds of a punishable violation of the law, or
- 3. attempting to commit or contribute to such actions.

The Anti-Money Laundering Act moreover comprises acts committed by the perpetrator of the criminal offence from which the proceeds or funds originate.

Under the Anti-Money Laundering Act, certain types of business undertakings (such as financial institutions) and professionals (such as accountants, lawyers and real estate agents) are subject to a number of investigative and reporting duties that constitute part of the private sector's measures to prevent laundering. Non-compliance with these duties may be punished by a fine or a prison sentence.

In criminal law, money laundering is covered by the two following provisions of the Criminal Code: Section 290 of the Criminal Code, which is worded as follows: *Any person who unlawfully accepts or acquires for himself or others a share in profits, which are obtained by a punishable violation of the law, and any person who unlawfully by concealing, keeping, transporting, assisting in disposal or in a similar manner subsequently serves to ensure, for the benefit of another person, the profits of a punishable violation of the law, shall be guilty of receiving of stolen goods and liable to a fine or imprisonment for any term not exceeding one year and six months, unless the offence is covered by section 290a.* 

(2) When the receiving of stolen goods is of a particularly aggravated nature, especially because of the commercial character of the offence, or in consequence of the amount of the gain obtained or intended to be obtained, or where a large number of offences have been committed, the penalty may be increased to imprisonment for any term not exceeding six years.

(3) Punishment pursuant to this provision cannot be imposed on a person who accepts profits as an ordinary subsistence from family members or a cohabiter, or any person who accepts profits as a normal payment for ordinary consumer goods, articles for everyday use, or services.

Section 290, the receiving of stolen goods, concerns all forms of proceeds from punishable offences (e.g., theft, people smuggling, drug crime and fraud). Both natural and legal persons (companies, associations, etc.) may be convicted for receiving stolen property/money laundering under the provisions of the Criminal Code.

Section 290a of the Criminal Code is worded as follows: Any person who converts or transfers funds directly or indirectly obtained by a punishable violation of the law, for the purpose of concealing or disguising the illegal origin of such funds, shall be guilty of money laundering and liable to a fine or imprisonment for any term not exceeding one year and six months.

(2) When the money laundering is of a particularly aggravated nature, especially because of the commercial or professional character of the offence, or in consequence of the amount of the gain obtained or intended to be obtained, or where a large number of offences have been committed, the penalty may be increased to imprisonment for any term not exceeding eight years.

Section 290a is directed at money laundering, both when money constitutes the direct proceeds of the predicate offence and when proceeds in any form other than money have been converted into money that is then laundered. The provision criminalises some of the acts concerning the handling of the proceeds of crime formerly comprised by section 290 of the Criminal Code on the receiving of stolen goods. Unlike section 290, the provision of section 290a also concerns acts that the perpetrator of the predicate offence carries out him- or herself. The provision thus expresses a certain new form of criminalisation regarding the perpetrator of the predicate offence. In practice, the perpetrator of the money laundering transactions he or she has carried out significantly exceed the customary handling of the proceeds of crime.

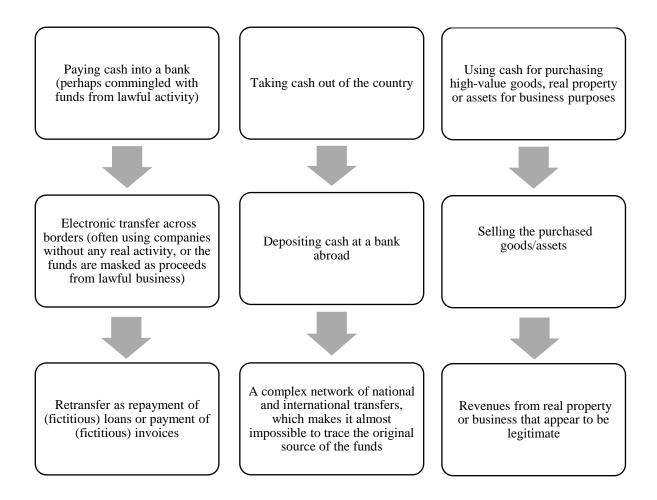
Money laundering transactions, which may take various guises, are intended to alter the identity of criminal proceeds or funds with the aim of making them appear to be legitimate funds or assets at some point.

Laundering may take place in several stages:

- 1. Placement: The physical placement of the proceeds in the financial system
- 2. Disguising: Separation of the proceeds from their source through (financial) transactions in order to hide the audit trail and achieve anonymity
- 3. Integration: Retransfer of funds to a person's property domain in a form in which the proceeds have been converted into funds that appear to be legitimate.

In practice these stages may, for instance, be carried out as follows:

#### Figure 1. Examples of money laundering



### 4. Consequences for society

The laundering of criminal proceeds has serious consequences for society regardless of the laundering method used.

It is assessed that when laundering criminal proceeds, criminal actors essentially do not take into account the consequences for society nor do they allow these consequences to affect them. For this reason, in the risk areas identified, the consequences for society are not assessed as affecting the risk of money laundering in different ways. For this reason, in the analysis, the consequences for society are assessed as a whole rather than under the individual risk areas.

#### Predicate offences and derivative crime

Money laundering is linked to virtually all criminal activities generating criminal proceeds (Europol 2017). The police experience that money laundering cases are often linked to organised crime such as drug crime or tax and VAT fraud. Money launderers often depend on the use or exploitation of people as frontmen or mules. This means that people not necessarily already criminal may be lured into committing crime for payment. Similarly, cases involving frontmen and mules may be associated with human trafficking, where foreigners are forced into committing crime. There has also been a rising trend in the organisation of money laundering networks as such, which offer laundering to third parties without the provider of the money laundering process necessarily having been involved in the predicate offence.

Money laundering sustains and contributes to the growth of criminal markets across the EU (Europol 2017). Measures to prevent, combat and curb money laundering may make it difficult for criminal actors to commit the predicate offences leading to proceeds that can be laundered. Such measures may also reduce the profit that crime can generate.

#### Structural and economic consequences

The efforts of criminal actors to disguise the proceeds of crime may weaken confidence in the financial system. The use of financial institutions for money laundering may undermine the financial sector's integrity, stability and reputation as well as threaten the single market and international developments (Official Journal of the European Union 2015).

Money laundering may also be detrimental to other associated financial institutions, legislative authorities and ordinary customers of the institution. (FATF n.d.)

Moreover, any perception that money laundering is going undetected or unpunished may subvert the public sense of justice. The laundering of criminal proceeds by criminal actors is also damaging to

the economy. Money laundering has both direct and indirect consequences, the direct consequences being loss of taxes and excise duties. Examples of the indirect consequences can be seen when large criminal proceeds are placed in specific types of goods or services. This may have negative consequences for the market, distorting competition for the people and businesses that carry on legal trade in these goods and services. The same is true for sectors known for their reliance on a good portion of underground economy, for example, certain parts of the service sector.

Money laundering methods involving the transfer of criminal proceeds abroad mean that taxes and excise duties on the criminal funds are not paid, nor are the funds generally re-integrated into the Danish economy.

### 5. Methods and data applied in the risk assessment

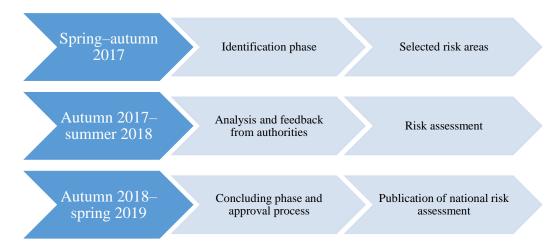
This national risk assessment of money laundering differs from the earlier risk assessment on several points. First and foremost, the State Prosecutor's Office has further developed the risk model used to analyse and assess the money laundering risk for each individual risk area. The risk model, shown on page 15, contains parameters related to both threats and vulnerability, and has been further developed to provide better insight into and more transparent assessments of the areas analysed. Additionally, the State Prosecutor's Office has involved many more cooperative partners from the private and public sectors than in the previous risk assessment, thus strengthening the basis and making the assessment as such more relevant and practicable for the reporting entities. Furthermore, the State Prosecutor's Office has drawn inspiration from other countries' risk assessments as well as the FATF Guidance (FATF 2013b) regarding the preparation of risk assessments for money laundering and terrorist financing.

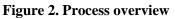
The preparation of the national risk assessment can be divided into two phases:

1) *identifying* threats and vulnerabilities relative to the money laundering risk and

2) *analysing* threats and vulnerabilities with a view to understanding the risks and assessing the likelihood that money laundering will occur.

Figure 2 below provides an overview of the process of compiling the risk assessment:





Compiling the national risk assessment has been a comprehensive process, with the identification phase running from the spring through to the autumn of 2017. Against the background of the risk areas identified, the analysis phase started and ran until the summer of 2018. The final phase, which included an approval process, was then initiated and ended in the autumn of 2018.

#### Identifying threats and vulnerabilities

A threat is defined as a person, group or activity that can potentially damage the state, society, economy, etc. A vulnerability is a weakness that can be exploited by a threat or facilitate the activities of the threat. Vulnerabilities can thus be weaknesses in the Danish anti-money laundering system, but may also be a product or service that renders a sector particularly vulnerable.

First, conditions in the external environment were examined with a view to identifying threats related to the laundering risk that may have significance for the extent of and methods used for money laundering (see page 18). Next, trends in profit-driven crime were considered (see page 20), as the money laundering potential depends on developments in specific forms of crime: embezzlement, tax and VAT fraud, drug crime, etc. It has not been possible to examine the breakdown of the offences preceding the laundering process (the predicate offences), because current legislation precludes the identification of all cases in Denmark involving money laundering.

The two respective sections about conditions in the external environment and trends in profit-driven crime are based on information from a wide range of sources, including Europol, the Crime Prevention Council, Statistics Denmark, the National Police Service and the Rockwool Foundation Research Unit. Information was also included from reports submitted to the FIU at the State Prosecutor's Office and records of reports of economic crime sent to the police.

Vulnerabilities were identified in collaboration with the following supervisory authorities: the Danish FSA, the Business Authority, the Gambling Authority and the Bar and Law Society. Finance Denmark, The Danish Association of Chartered Estate Agents (DE), Danish Auditors (FSR), Finance and Leasing (the Association of Danish Finance Houses) and Insurance & Pension Denmark (IPD) have also contributed information on behalf of their members. The Tax Agency's Anti-fraud Department has provided information from the unit that investigates cases where VAT carousel fraud and sub-contractor fraud specifically are suspected.

The process of identifying vulnerabilities ran from spring to autumn 2017, see Figure 2. Accordingly, additional vulnerable points not initially pinpointed in the identification phase itself may subsequently have proved to be relevant. For example, the State Prosecutor's Office has since become aware of several areas identified as possible risk areas, e.g, AIF/AIFM funds. However, this area has not been included in the current risk assessment, but will be incorporated and assessed in a future national risk assessment if relevant. Furthermore, it should be noted that the insurance and pension area was highlighted as an area vulnerable to misuse leading to money laundering. However, the subsequent risk assessment of the area showed that the current control measures and legislation regarding the payment of pension and insurance benefits make money laundering highly unlikely in this area, which was accordingly omitted from the analysis.

In addition, the organised crime departments of the police districts, including those of the Greenland Police and the Faroe Islands Police, submitted information about which threats and vulnerabilities can currently be related to the laundering risk in Denmark. The information was collected through interviews and derives primarily from investigations into the predicate offences of the laundering of criminal proceeds.

Against the background of the identification of threats and vulnerabilities carried out from spring to autumn 2017, the risk assessment deals with the following risk areas:

- ✓ Legal business structures
- ✓ Banks
- ✓ Payment institutions
- ✓ Money remittance providers
- ✓ Currency exchange providers
- ✓ Physical cross-border transfer of currency
- $\checkmark$  The gambling sector
- ✓ Real estate
- ✓ High-value goods
- ✓ Leasing
- ✓ Service providers
- ✓ Advisers
- ✓ Cryptocurrencies

### Analysis of threats and vulnerabilities

A five-parameter risk model has been developed for the analysis of threats and vulnerabilities: extent, accessibility, attractiveness, risk of detection and likelihood of prosecution and conviction. These parameters are weighted equally in the overall assessment of whether the laundering risk in each specific area is low, medium or high.

With the risk model as a starting point, each individually identified area was analysed and assessed meticulously in the light of previous experience and new information obtained from police districts, other authorities and interest organisations.

The results of the risk area analysis and assessment were all forwarded to the pertinent supervisory authorities and tax authorities, which thus had an opportunity to provide feedback and qualify the arguments in the relevant chapters for their area. As such, the analysis is based on valuable expertise and knowledge collected from these authorities, which has been combined with the knowledge and experience from criminal cases held by the police and the prosecution service.

|               | Parameter  | Risk<br>Low  | <b>Risk</b><br>Medium  | <b>Risk</b><br>High  |
|---------------|--|--|--|--|
| Threat        | Extent <sup>3</sup>                              | Limited<br>The money laundering<br>possibility is not used, as<br>far as it is known, or it is<br>used only by a small<br>group in criminal envi-<br>ronments  | Moderate<br>The money laundering<br>possibility is used by a<br>moderate number of in-<br>dividuals in criminal en-<br>vironments  | Large<br>The money laundering<br>possibility is used by<br>many individuals in<br>criminal environments  |
| Vulnerability | Accessibility                                    | <b>Difficult</b><br>Access is difficult and<br>requires extensive plan-<br>ning, knowledge and/or<br>technical expertise   | Moderate<br>Reasonably accessible<br>and requires moderate<br>planning, knowledge<br>and/or technical exper-<br>tise   | Easy<br>Easily accessible and re-<br>quires little or no plan-<br>ning, knowledge and/or<br>technical expertise  |
|               | Attractiveness                                   | Unattractive<br>Anonymity is hard to<br>maintain, and the<br>method is perceived as<br>unsafe and/or expensive<br>to use   | Moderately attractive<br>Anonymity is relatively<br>easy to maintain, and the<br>method is perceived as<br>reasonably safe and/or<br>less expensive to use   | Highly attractive<br>Anonymity is very easy<br>to maintain, and the<br>method is perceived as<br>safe and/or cheap to use  |
|               | Risk of detection                                | <b>High</b><br>Appropriate supervisory<br>authorities exist, and<br>laundering attempts are<br>likely to be detected   | Medium<br>Few supervisory author-<br>ities exist, and launder-<br>ing attempts are less<br>likely to be detected   | Low<br>Supervisory authorities<br>are weak or non-exist-<br>ent, and laundering at-<br>tempts are difficult to de-<br>tect   |
|               | Likelihood of<br>prosecution and convic-<br>tion | High<br>The legislation is fully<br>adequate for the pursuit<br>of potential money laun-<br>derers, and the police<br>and other authorities<br>have the resources and<br>competencies for the<br>purpose | Medium<br>The legislation is ade-<br>quate for the pursuit of<br>potential money launder-<br>ers, but the police and<br>other authorities have<br>limited resources and<br>competencies for the<br>purpose | Low<br>The legislation is inade-<br>quate for the pursuit of<br>potential money launder-<br>ers, and the police and<br>other authorities lack the<br>resources and competen-<br>cies for the purpose |

#### Table 1. Risk model for assessment of money laundering channels

<sup>&</sup>lt;sup>3</sup> It is noted that this parameter contains information about predicate offences of money laundering via the area in focus, and about other conditions in society of significance for the extent, e.g., developments in criminal environments and increased digitalisation.

### 6. Conditions in society

Several factors in societal development help determine the extent and type of crime and money laundering. Accordingly, the following sections review in more detail the legislative, international, economic, technological and social factors that may help promote the motivational factors and opportunities to commit money laundering crime.

#### AML legislation, the Money Laundering Directive and the AML strategy

The threat picture for money laundering and terrorist financing is constantly changing, a factor that has played a role in the creation of the EU's Fourth Money Laundering Directive, which is based on the FATF's (Financial Action Task Force) recommendations.

Rather than enabling Member States to relax their respective legislation systems, the directive focuses on introducing more stringent rules than previously required by the EU. The implementation of the Fourth EU Money Laundering Directive translated into tighter Danish regulations, and for this reason, a new, more rigorous amendment of the Anti-Money Laundering Act came into force in June 2017. Furthermore, in summer 2018 a new provision on money laundering was inserted into the Criminal Code; see the previous section 'What is money laundering?'

In June 2018 the EU adopted the Fifth Money Laundering Directive. Among other things, the directive focuses on criminals' use of electronic money and cryptocurrencies (Official Journal of the European Union 2018). The Danish government also entered into a new money laundering agreement on 19 September 2018, which contains the possibility of higher fines, a fast-track scheme, the expansion of the fit-and-proper requirement and a prohibition on the use of the 500-euro banknote in Denmark (Finance Denmark 2018 and the Ministry of Industry, Business and Financial Affairs 2018).

#### **International cooperation**

Denmark's EU membership creates international mobility and the chance to seek jobs abroad, run business undertakings in several countries and transfer funds across national borders. However, at the same time the freedom of movement within the EU imposes the need for stronger cooperation between national authorities on the investigation and prosecution of citizens committing cross-border crime. Denmark's position in the EU's judicial cooperation has changed in recent years. In consequence, after voting against the opt-in regime for judicial cooperation in 2015, Denmark was forced to leave Europol on 1 May 2017. However, via liaison officers, the Danish police still have access to information held by Europol, and Denmark's status in the Eurojust<sup>4</sup> cooperation remains unchanged. As amendments are made in future to several legislative acts in judicial and national affairs, Denmark will no longer be able to participate in the cooperation on the same terms owing to its opt-out on

<sup>&</sup>lt;sup>4</sup> Eurojust is an EU cooperation initiative between the national prosecution services of the Member States in cases involving crossborder crime.

justice and home affairs. This may hamper Denmark's practical collaboration with other EU countries on cases concerning such matters as the tracing, seizure and confiscation of criminal proceeds (Sørensen 2018). Meanwhile, Denmark continues to be part of the Financial Action Task Force (FATF) cooperation on combating economic crime under the auspices of the OECD and the Egmont Group.<sup>5</sup>

#### **Financial factors**

Denmark has an open economy that is highly dependent on trade with other countries and also easily affected by external factors and international economic trends.

The current employment rate is the highest in many years, and Danes have more money to spend than in the past (Ministry of Economic and Interior Affairs 2018). With the decline in unemployment, fewer people are receiving public income support, and the tax rate has also dropped. The incentive to commit certain types of economic crime (including social benefit fraud, tax evasion and undeclared work) is therefore assessed to be lower than during the financial crisis years<sup>6</sup>. It should also be noted that the value of undeclared work in 2016 was estimated at between DKK 34 and 59 bn, corresponding to between 1.7 and 2.9% of Danish GDP (Andersen, L. H. 2017).

The Ministry of Economic and Interior Affairs believes that the growth-driven shortage of labour has put pressure on the Danish job market. Although this pressure has lessened owing to the increase in foreign labour, it still plays a role and could curb economic growth in the long term. According to the Danish Economic Councils (2018), there are signs that job opportunities for unskilled workers, and to a lesser degree also for skilled workers, will weaken in line with the increasing presence of foreign workers, as a large percentage of this group work in low-paid jobs. This may affect the incentive of individuals in this group to commit economic crime, including taking undeclared work.

#### **Social factors**

The OECD expects that the number of people living in fragile contexts worldwide will continue to rise – from 1.6 billion to 3 billion, or 32% of the global population, by 2050 (OECD 2016). In all probability, the increase will impact the refugee and migrant flows to Europe in future.

It is difficult to assess the consequence of these refugee and migrant flows, as they depend on political developments in Denmark, Europe and globally. As a result of the massive refugee and migrant influx, Denmark together with a number of other European countries introduced temporary border controls on 4 January 2016 (Ministry of Immigration and Integration 2017). Coupled with the increase

<sup>&</sup>lt;sup>5</sup> The Egmont Group is a collaboration between 155 of the UN's 192 member countries working together to combat economic crime and terrorist financing.

<sup>&</sup>lt;sup>6</sup> However, findings from a new study published by the Rockwool Foundation Research Unit (2018) show that employment among

<sup>25-54-</sup>year-olds continues to be significantly lower than during the pre-crisis years.

in refugees and migrants, these border controls have created a more attractive market for smuggling people. Migrant smuggling has emerged as one of the most profitable and widespread criminal activities for organised crime in the EU (Europol 2017). As well as the transport of migrants, document forgery is another key criminal activity linked to the migration crisis. In 2015, the migrant smuggling network was estimated to have generated profits of between EUR 4.7 and 5.7 bn in the EU as a whole. This profit has declined since 2016 by at least EUR 2 bn, which is in line with the decrease in the number of irregular migrants (Europol 2017).

Social fraud and unemployment fund fraud have a serious impact on the Danish welfare structure, particularly organised or extensive fraud involving public benefits. Since 2015, social fraud – primarily involving unemployment funds – has been one of the types of crime reported less frequently to the police (Police 2017). The trend is probably associated with Denmark's current low unemployment rate (Statistics Denmark 2018), which may lessen the incentive to commit social fraud.

#### **Technological factors**

Advances and the use of technological resources help create a basis for new forms of economic crime and the further development of existing crime. Types of crime previously requiring personal contact between criminals and victims can now take place via the internet. Using the net, criminal actors can quickly build up contacts and networks, enabling them to exploit a variety of skills and possibilities. Technological developments have thus spawned opportunities for new forms of business and crime such as hacking and data theft, sale and exploitation. Personal information about users is more widely shared via the internet, including about their behaviour, movements and preferences (Pedersen, Rene 2017).

The potential for economic IT crime in particular (credit card fraud, etc.) is great, among other things, because 77% of Danes aged 16–89 use the internet to shop online for clothes, travel, experiences and commodities, and the trend is on the rise (Danish Defence Intelligence Service 2017). Another growing and popular form of crime is trading in illegal items such as drugs and weapons via social media or the dark web. An upward trend in transactions is being seen where goods are paid for in crypto-currencies, particularly in dark web trading.

The technological developments are not purely negative, however, as they also open up new possibilities for the police. For example, the police have had a new IT system developed, POL-INTEL, which correlates information from a wide range of records to which the police normally have access (DR 2018). Offering more sophisticated search options than earlier systems, POL-INTEL is a powerful reference tool that enables more efficient investigation.

### 7. Trends in profit-driven crime

As described in the section on conditions in society, several societal factors influence developments in crime in both Denmark and the rest of the world. The interfaces between money laundering, internet-related and profit-driven crime are becoming increasingly blurred, with a frequent overlap between the various types of crime preceding the laundering process.

The reports the FIU receives regarding potential money laundering may give an indication of which types of predicate offence are committed, as well as how the laundering process is subsequently carried out. However, it is also relevant to incorporate other types of report and crime forms in order to provide an adequate overview of the dominant trends in profit-driven crime and money laundering.

The FIU acts as Denmark's Financial Intelligence Unit and as such receives reports of potential money laundering or terrorist financing from the businesses or persons subject to a reporting duty under the provisions of the Anti-Money Laundering Act. The FIU may also receive reports from authorities, businesses and citizens who find a particular circumstance suspicious and send a report to the Secretariat without being obliged to do so. In 2017, the FIU received almost 25,000 reports, 33% more than the previous year (Table 2).

#### Table 2. Number of reports submitted to the FIU

| 2013  | 2014  | 2015   | 2016   | 2017   |
|-------|-------|--------|--------|--------|
| 5,166 | 7,255 | 15,619 | 18,669 | 24,911 |

The number of reports submitted to the FIU has probably risen because the authorities and reporting entities have increased their focus on money laundering and terrorist financing. In addition, in 2014 an electronic reporting format was made mandatory, which prompted banks and other institutions to introduce systems facilitating the submission of electronic reports to the FIU. It cannot be ruled out that the rise in number of reports may also be due to growth in profit-driven crime.

The majority of the reports received by the FIU come from banks. Most of the reports forwarded by the FIU are passed on to the tax authority, as they often concern suspected fraud involving public income support or welfare benefits.

In July 2013 the limit of the cash payment prohibition was reduced from DKK 100,000 to DKK 50,000 to lessen the risk of funds being laundered through cash transactions, which may also have caused reporting entities to intensify their focus. This means the reporting entities (business operators, accountants, lawyers and banks) must be alert to large cash amounts and suspicious deposits and report them to prevent this method of money laundering.

The reporting entities focus strongly on compliance, including detecting and passing on information about violations of the Anti-Money Laundering Act. For instance, the supervisory authorities have intensified their focus on detecting social fraud and tax and excise duty fraud. Among other things, the tax administration upgraded its monitoring efforts in 2018 by changing its structure and dividing the authority into seven new agencies (Tax Administration N.d.).

Suspected laundering via online gambling operators is among the crime forms often mentioned in the reports received by the FIU. The opportunities for money laundering by this means increase as more online gambling operators appear. In the past, trading in physical lotto and pools coupons was a particularly popular method of laundering funds generated by drug dealing, but this method is now being used for other types of predicate offences as well.

#### Actors in profit-driven crime

According to the Danish Crime Prevention Council, profit-driven crime has generally shifted from the street to cyberspace. The risk factors and incentives for committing crime are the same, however. The perpetrators of both internet-related and profit-driven crime therefore have largely the same profiles as the people who commit crimes in the physical world (Kruize, Peter 2018).

According to the FIU's data, the criminal actors operating in money laundering are often individuals already in the spotlight of the police and other supervisory authorities in connection with other case categories. However, individuals with ties to outlaw motorcycle gangs figure relatively seldom in the laundering reports, as do other organised crime groups. There is a tendency for persons from a foreign background who have stayed briefly in Denmark to be used as frontmen in complex company structures. Accordingly, they appear a good deal in the reporting statistics, thus camouflaging the identity of the true organisers of the crime concerned. The FIU publishes quarterly reports describing new money laundering trends and also shares knowledge with the police districts in the form of information about potential criminal actors singled out according to various criteria based on the reports it receives.

With almost global internet access and the digitalisation of many processes conducted by Danish authorities, criminals can often be found in other countries while committing crime. This makes it harder for the police to investigate the criminals and for the prosecution service to prosecute them. Establishing the identity of the true perpetrators may also be difficult, for which reason it is important for the reporting entities to shed light on the area by contributing their information.

#### **Current crime trends**

Crime in Denmark has fallen generally in recent years, with youth crime in particular dropping steadily from 25,125 suspected offences/charges in 2006 to 11,487 suspected offences/charges in 2016 (Kyvsgaard 2017). Despite the general decline in crime, all types of internet-related and acquisitive crime have risen since 2016, primarily in the form of (identity) theft and credit card abuse. Only about 36% of all internet-related acquisitive crime is presumed to be reported to the police. Credit card abuse is the most commonly reported offence, but the invisible statistics for the area are probably high (Police 2017).

According to the national strategic analysis conducted by the police (2017), a significant rise in the number of reported fraud cases was seen from about 8,000 reports in 2009 to about 44,000 in 2016. One of the possible reasons is the sharp increase in e-commerce in the period, which naturally has an influence on the increase in the number of reports. During the first three quarters of 2016, Danish banks reported 970 cases to Finance Denmark in which cybercriminals had attempted to gain access to Danish online banks by enticing bank customers to provide information (Danish Defence Intelligence Service 2017).

Collaborating with the other Danish police districts, Copenhagen Police took the consequences of the rise in internet-related crime and opened a new centre in autumn 2018 – the National Centre for Economic Cybercrime (LCIK). Established in order to create a better overview of developments in the area, the centre will be the starting point for reporting and assessing all cases, regardless of the location of the crime scene in Denmark. Case processing needs to be better integrated and more uniform if the police are to handle the growing number of reports of credit card fraud, phishing, smishing, sextortion and BEC/CEO fraud on the net.

IPR crime concerns violations of the legislation within the areas covered by the Copyright Act, the Trademark Act, the Design Act and the Patent Act, as well as the distribution of products and services. The most common offences are the sale of fake brand goods on social media (Facebook) and unlawful streaming of TV channels, films and services. These are new forms of crime, and following a pilot period, a central department was established within the office of the State Prosecutor for Serious Economic and International Crime, where IPR cases are processed (Prosecution Service 2018). Dealing with the cases centrally will ensure better coordination and investigation and encourage the identification of any new tendencies and trends.

Tax and VAT fraud, illegal work, social fraud and money laundering are case categories often seen in the context of wider, more complex structures. Both the police and the tax authority are familiar with cases of money laundering via illegal work in particular, primarily within the service sector (cleaning, restaurants, etc.). This also includes the risk of human trafficking, also mentioned in the section on conditions in society. According to the national strategic analysis published by the police (2017), the number of reports of serious tax and VAT fraud more than doubled in the 2009-2016 period. Since the number of reports reflects the authorities' efforts in the area, it is difficult to say anything about the true development, because the number of reports is not necessarily an indication of the extent of crime.

As mentioned earlier, the use of frontmen who are migrants staying briefly in Denmark is a trend seen in relation to money laundering as well as to tax and VAT fraud. These frontmen, often from southern or eastern Europe, come to Denmark to set up a NemID login and bank account, after which they disappear without trace. They establish business undertakings that are often operated for a brief period, during which the undertakings are drained of financial assets and then declared bankrupt. The businesses often issue and receive fictitious invoices as part of the money laundering process.

Establishing and registering a business undertaking in Denmark is both easy and inexpensive. Between 1 January 2014 and 15 April 2019, it was possible to establish an entrepreneurial limited company (IVS company), a special type of private limited company subject to relatively lenient rules regarding start-up capital, liability, audit obligations and so on. The registration fee for establishing private limited company (ApS) and IVS company formats is DKK 670. A start-up capital of no less than DKK 50,000 is also required to establish an ApS company, but only DKK 1 for an IVS company<sup>7</sup>. Since the introduction of the IVS format, the number of new companies registered has risen steadily, with newly established IVS companies accounting for 39% of the total number of companies established in the first six months of 2017 (Danish Chamber of Commerce, Experian and Danish Auditors 2017). Approximately half of the newly established IVS companies are located in the capital area. Once an IVS company has been established, it can later be converted into an ApS company, provided certain conditions are met. However, this is neither a requirement nor an obligation, but simply an option for the owner of the IVS company. An analysis by the Danish Chamber of Commerce, Experian and Danish Auditors (2017) shows that few owners of IVS companies convert their undertaking into an ApS company. Owners of private limited companies, including IVS companies, are not personally liable, as liability is limited to the company's assets.

An audit may serve as a supervisory measure, as the company thereby has an (impartial) auditor to review the company's financial statements, finances, structure, etc. In principle, companies must have their financial statements audited. However, small companies may opt out of an audit if they meet special conditions concerning balance sheet total, revenue and number of employees. As regards published financial statements as of 30 June 2017, 3.9% of IVS companies and 28.2% of ApS companies had had their financial statements audited (Danish Chamber of Commerce, Experian and Danish Auditors 2017). The disadvantage of the simplicity and negligible cost of establishing an IVS

<sup>&</sup>lt;sup>7</sup> In this connection, business entities covers/refers to all types of businesses and companies, while companies covers company formats with no personal liability, such as IVS, ApS and A/S companies.

company may be that it is easier and more attractive for criminal actors to exploit this company structure for laundering purposes.

The findings of an analysis from the Business Authority (2018) show that in 2017, IVS companies accounted for around 12% of new companies registered for VAT, while at the same time constituting approx. 33% of potentially fraudulent business undertakings that the tax administration refused to register under the provisions of the tax and excise duty legislation. However, it should be noted that the authorities have tightened their scrutiny of newly established IVS companies, and this may encourage criminal actors to acquire and re-register already active companies instead. This activity gives authorities no immediate cause for concern, for which reason a company can potentially be exploited for a lengthy period without attracting the authorities' attention.

#### **Future crime trends**

The Centre for Cyber Security at the Danish Defence Intelligence Service describes the following four activities as the primary threats within cybercrime, all conducted via the internet: espionage, acquisitive crime, activist actions and terrorist operations (Danish Defence Intelligence Service 2017). Hacking, primarily in the form of cyber espionage, is another major threat to Denmark now and in the future.

Both state/public sector actors and private companies may be the target of espionage and hacking attacks. The threat is assessed as high, and ransomware and distributed-denial-of-service (DDoS) attacks are particularly popular methods. To date, such attacks have only involved information theft or blackmail, without endangering or putting human lives at risk. As technologies grow more sophisticated, the hacking of self-driving cars or other wifi- or bluetooth-operated equipment will put human lives and health in danger.

The above-mentioned trends such as IPR crime, hacking and fraud will probably emerge in both economic and internet-related crime. Although there is also a risk that the use of cryptocurrencies will become an attractive way to launder the proceeds of crime in future, this method has seldom been observed to date. Cryptocurrencies are still not recognised as valid currency by the Danish financial system, and their use is accordingly a relatively risky money laundering method.

The physical cross-border transfer of currency is another laundering trend expected to increase in future, because the financial sector and other reporting entities are getting better at complying with their obligations to register and report transactions, thus making it difficult for criminals to move illegitimate funds through the financial system.

Missing trader and CEO fraud are expected to become more prominent crime trends in future, as it is relatively easy to set up a NemID, companies and bank accounts with associated credit cards and online banking in Denmark. However, closer collaboration between authorities and intensified police efforts in the area will counter this trend.

### 8. Convictions for handling stolen property

As referred to in the section 'What is money laundering?' above, money laundering was not independently criminalised until 1 July 2018. Therefore, in principle, money laundering had to be punished either as part of the predicate offence or under the provision on handling stolen property of section 290 of the Criminal Code. An analysis of convictions for handling stolen property in 2016 has now been carried out to illustrate the extent of money laundering cases under section 290 of the Criminal Code. An additional purpose of the analysis has been to determine, to the extent possible, what predicate offences preceding money laundering the analysed cases had comprised.

#### **Methods applied**

The State Prosecutor has searched the police case management system (POLSAS) to retrieve all cases having 2016 as their date of conviction and having been adjudged with the following offence codes: 76601 (Handling stolen property), 76602 (Handling stolen property – aggravated/in a business context), 76611 (Handling stolen property regarding controlled drugs), 76612 (Handling stolen property regarding controlled drugs), 76612 (Handling stolen property regarding weapons/ammunition) and 76622 (Handling stolen property regarding weapons/ammunition). Next, with assistance from the Director of Public Prosecutions, the State Prosecutor obtained the relevant decisions from the police districts (judgments and fixed-penalty notices primarily). It should be noted that the method is associated with some uncertainty, because, other things being equal, the data is required to be of adequate quality and the POLSAS system must have been updated with correct offence codes. These must have been entered once judgment has been passed in both single-charge and multi-charge cases. In addition to the cases obtained from the POLSAS system, the State Prosecutor's office has contributed three cases involving five individuals and three companies.

Based on the case data obtained, the judgments have been reviewed, analysed and assessed by way of a range of objective criteria (such as the number of offences, type of decision, length of sentences, etc.), which has made it possible to draw up a descriptive analysis of convictions for handling stolen property in 2016. In addition, a subjective assessment has been made to check whether the cases contained elements of money laundering and, if so, the money laundering channel used. Against the background of the list of identified risk areas that emerged after the identification phase in 2017, it was assessed what money laundering channels had been used in the cases obtained.

#### Analysis

The State Prosecutor obtained information about 875 cases that resulted in at least one conviction for violation of section 290 on handling stolen property in 2016.

The cases involved 1,032 individuals and three companies.<sup>8</sup> The breakdown of the actors involved is shown by Table 3.

| Gender/company | Number |
|----------------|--------|
| Male           | 955    |
| Female         | 77     |
| Company        | 3      |
| Total          | 1,035  |

#### Decisions in cases involving handling stolen property

The vast majority (90%) of the individuals were convicted of handling stolen property contrary to section 290(1), whereas the remaining 10% and the three companies were convicted of aggravated handling stolen property contrary to section 290(2). Furthermore, in 19 cases an individual was convicted of contravention of section 290(1) on at least one count and aggravated handling stolen property contrary to section 290(2) on at least one count. This is illustrated by Table 4.

Table 4. Individuals and companies shown by the handling stolen property category of their conviction

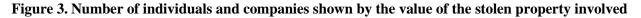
| Conviction             | Number |
|------------------------|--------|
| Section 290(1)         | 919    |
| Section 290(2)         | 97     |
| Section 290(1) and (2) | 19     |
| Total                  | 1,035  |

#### Value of stolen property handled

In many of the cases, the value of the stolen property handled was calculated fully or partly. The values calculated vary widely, ranging from a few hundred kroner to many million kroner, reflecting substantial differences in the extent and character of the cases involved. Several of the cases with a high calculated value of the stolen property handled were associated with currency exchange offices, involving specific laundering of proceeds from crime. The same pattern was also reflected by the amounts of the fines imposed as shown by Table 7. The value of the property handled is illustrated by Figure 3.

<sup>&</sup>lt;sup>8</sup> A total of 20 individuals were convicted of handling stolen property twice in 2016. Thus, the number of unique persons was 1,013.





It was indicated in 31 cases that the crime was of a business-related or professional character, which was stated specifically as an aggravating circumstance under section 290(2) of the Criminal Code. In 14 cases it was stated that the handling involved carriage of funds to and from other countries.

#### Offences involved in the cases

In addition, it appears from the cases analysed that 165 individuals were convicted on the Prosecution's alternative charges concerned with handling stolen property, which means that the court had not found it proved sufficiently that the defendants were guilty of the primary charges for an offence. Alternative charges were involved in slightly fewer than two of three cases in decisions convicting defendants on at least one count of theft under section 276 of the Criminal Code. It appeared moreover that 130 individuals had previously been convicted of handling stolen property, which is of relevance particularly for the sentencing.

It should be noted that most frequently individuals and companies were convicted of more than one criminal offence in the same case. The other offences were typically related to other contraventions of the law than handling stolen goods, i.e., theft or other property crime primarily. See this breakdown in Table 5.

| Table 5. Individuals and companies broken down by number of offences <sup>9</sup> |
|---|
|---|

| Number of offences included in the conviction | All offences | Handling stolen property |
|---|--------------|--------------------------|
| 1   | 282          | 708                      |
| 2-5   | 341          | 244                      |
| 6-20  | 313          | 74                       |

<sup>9</sup> In two cases charges were dropped, for which reason no offences were registered (0 offences). These have been left out of the table.

*<sup>1-10,000 10,001-100,000 100,001-500,000 500,001-1,000,000</sup>* 

| 21-50  | 87    | 5     |
|--------|-------|-------|
| 51-100 | 8     | 0     |
| +100   | 2     | 2     |
| Total  | 1,033 | 1,033 |

#### **Types of decision**

The numbers referred to above naturally affected the types of decision, which were therefore rarely a reflection of only the sentence for the handling of stolen property in the cases, and the same applies to the duration of sentences and/or amounts of fines. On average, the handling stolen property of-fences accounted for only approx. 1/3 of the total number of offences comprised by the judgments analysed. See the breakdown by type of decision in Table 6.

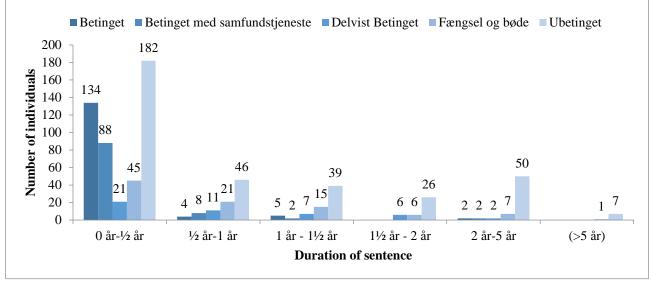
Table 6. Individuals and companies broken down by type of decision<sup>10</sup>

| Types of decision                | Number |
|----------------------------------|--------|
| Unsuspended                      | 350    |
| Unsuspended and a fine           | 95     |
| Partly suspended                 | 47     |
| Suspended                        | 147    |
| Suspended with community service | 101    |
| Fine                             | 267    |
| Dropped charges                  | 3      |
| Total                            | 1,010  |

The duration of the sentences was indicated in the judgments in days, months and years depending on the duration and character of sentences. To achieve comparable sentence durations across the judgments, the judgments were converted into days, with one month being equal to 30 days and a year equal to 12 months (360 days).<sup>11</sup> For partly suspended sentences, the total sentence duration is indicated, not the suspended part. Figure 4 shows the breakdown by sentence duration and type of decision.

<sup>&</sup>lt;sup>10</sup> The remaining 25 comprise cases in which sentences were passed but the defendants unfit for punishment (hospital orders) as well as cases in which a caution was issued or in which no supplementary penalty was ordered relative to previous judgments in the same multi-charge case.

<sup>&</sup>lt;sup>11</sup> The method is consistent with the method used by Statistics Denmark when measuring sentence duration in their statistics concerning judgments.



#### Figure 4. Individuals broken down by type of decision and sentence duration

Suspended - Suspended with community service - Partly suspended - Imprisonment and fine – Unsuspended (år = year)

The far greater part of the prison sentences imposed in cases involving at least one offence of handling stolen property were of less than 180 days of imprisonment (equal to ½ year). In the cases in which the full sentence was unsuspended, slightly more than half of those convicted received a prison sentence of less than 180 days. Among the eight persons sentenced to imprisonment for more than five years was a director of a currency exchange office and a person sentenced for extensive transfers to a money remittance provider.

#### Value of fines

Table 7 shows a breakdown of fines by value. The table naturally includes only the individuals and companies who received penalties by way of fines, possibly in combination with a prison sentence. The total number of individuals and companies fined is 419. The amount of the fines imposed most frequently was DKK 1,501 - 5,000, while only few individuals and companies received fines exceeding DKK 100,000.

Table 7. Individuals and companies broken down by the value of fines

| Value of fines    | Number |
|-------------------|--------|
| 500-1,500         | 52     |
| 1,501-5,000       | 191    |
| 5,001-10,000      | 85     |
| 10,001-25,000     | 56     |
| 25,001-100,000    | 27     |
| 100,001-1,000,000 | 2      |
| Over 1 million    | 6      |
| Total             | 419    |

#### Money laundering channels

As described in connection with methods, an assessment was made of whether the cases comprised an element of money laundering and which laundering channels had been used. Table 8 below shows an overview of the number of cases broken down by money laundering channel.

| Money laundering channel     | Number |
|------------------------------|--------|
| High-value goods             | 92     |
| Banks                        | 24     |
| Money remittance providers   | 13     |
| Trade-based money laundering | 3      |
| Currency exchange provider   | 2      |
| Total                        | 134    |

Table 8. Cases broken down by money laundering channel used

#### Summary of judgments for handling stolen property

Based on the 875 cases analysed, it has been assessed that a total of 134 cases included an element of money laundering, the vast majority of them involving high-value goods. Many convictions were for possession of stolen goods, even when an assessment indicated that an element of money laundering was involved. Thus, in most cases, high-value goods had not been used as a method of specifically laundering funds originating from a criminal offence. Most of the cases involved possession of stolen high-value goods that might have been acquired from criminal funds. Against that background, very few of the total number of cases had a specific element of money laundering. The cases involving an element of money laundering have been included in the risk assessment where relevant.

In an attempt to quantify which predicate offences had resulted in conviction for money laundering, information was obtained concerning the nature of the other offences comprised by the judgments. However, in practice there was no link in many cases between the other offences charged and the handling stolen property offence. This is because companies or individuals convicted of handling stolen property will frequently also have been convicted of other, not necessarily related, offences such as drug crime under section 191 of the Criminal Code, as was also indicated under the analysis of the type of decision. Overall, based on the judgments, it is therefore not possible to draw conclusions on the predicate offences that precede a possible charge for money laundering.

In a few cases, money laundering was punished under section 290, i.e., the handling stolen property provision of the Criminal Code. In addition, the analysis of risk areas showed that in cases involving an element of money laundering, the crime for which perpetrators were convicted was often the predicate offence such as computer fraud or drug crime. It is not possible at this time to separate these cases in the police systems, one reason being the registration practice that only allows searching by offence codes (frequently only one per case or multi-charge case) or by the summary (the subject of the case), which is drawn up by the police officers themselves. In addition, search keys may be attached to cases. However, to date few of these have been relevant in relation to money laundering.

## 9. Analysis and assessments (not publicly available)

### 10. Literature

**The Danish Bar and Law Society. 2017.** "Advokatrådets vejledning om hvidvaskloven" (The Danish Bar and Law Society's guide to the Anti-Money Laundering Act). The Danish Bar and Law Society, accessed on 18 October 2018,

https://www.advokatsamfundet.dk/Advokatregulering/Hvidvask /~/media/Hvidvask/VEJLEDNING%20TIL%20HVIDVASKLOVEN%202017.ashx

Andersen, L. H., et al. 2017. *Danskernes liv med skatter, sort arbejde og gør det selv-arbejde.* (*Life of the Danes with taxes, moonlighting and DIY*). Odense: Syddansk Universitetsforlag – with support from the Rockwool Foundation.

**The Prosecution Service. 2018.** "Styrket indsats over for rettighedskriminalitet bliver samlet hos SØIK". (Strengthened action against IPR crime to be gathered at SØIK). Prosecution Service, accessed on 18 October 2018, https://www.anklagemyndigheden.dk/da/styrket-indsats-over-rettighedskriminalitet-bliver-samlet-hos-soik

**Basel Institute of Governance. 2016.** "Basel AML Index 2016". International Centre for Asset Recovery, accessed on 18 October 2018, https://index.baselgovernance.org/sites/index/documents/Basel\_AML\_Index\_Report\_2016.pdf

**Payments Council. 2016.** "Rapport om nye aktører på betalingsområdet" (Report on new actors in the payments area". Central Bank, accessed on 18 October 2018, https://www.national-banken.dk/da/publikationer/Documents/2016/08/Report%20om%20nye%20akt%C3%B8rer%20be-talingsmarkedet.pdf

**CoinMarketCap. 2018.** "Top 100 Cryptocurrencies by Market Capitalization". CoinMarketCap, accessed on 13 September 2018, www.coinmarketcap.com

**Statistics Denmark. 2017.** "Mobilen er den foretrukne enhed til internetadgang" (The mobile is the preferred device for internet access). Statistics Denmark, accessed on 18 October 2018, https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=24235#

Statistics Denmark. 2018. "Fortsat stigning i beskæftigelsen" (Continued increase in employment). Statistics Denmark, accessed on 18 October 2018, https://www.dst.dk/da/Statistik/nyt/Ny-tHtml?cid=26718

**Danish Chamber of Commerce, Experian and Danish Auditors. 2017.** "Analyse af Iværksætterselskaber" (Analysis of entrepreneurial companies). Danish Chamber of Commerce, accessed on 18 October 2018, https://www.danskerhverv.dk/siteassets/mediafolder/downloads/fakta/analyse-af-ivarksatterselska-ber-juli-2017

**The Danish Economic Councils. 2017**. "Dansk økonomi, forår 2017" (The Danish economy, spring 2017). The Economic Councils, accessed on 18 October 2018, https://dors.dk/vismandsrap-porter/dansk-oekonomi-foraar-2017

**The Danish Economic Councils. 2018.** "Udenlandsk arbejdskraft bidrager til vores økonomiske velstand" (Foreign labour contributes to our economic wealth). Altinget, accessed on 18 October 2018, https://www.altinget.dk/arbejdsmarked/artikel/de-oekonomiske-raad-udenlandsk-arbejdskraft-bidrager-til-vores-oekonomiske-velstand

**Official Journal of the European Union. 2015.** "REGULATIONS: REGULATION OF THE EU-ROPEAN PARLIAMENT AND OF THE COUNCIL (EU) 2015/847". EUR-Lex, accessed on 18 October 2018, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32015R0847&from=PT

**Official Journal of the European Union. 2018**. "DIRECTIVES: DIRECTIVE OF THE EURO-PEAN PARLIAMENT AND OF THE COUNCIL (EU) 2018/843". EUR-Lex, accessed on 18 October 2018, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32018L0843&from=EN%20

**The European Council. 2018.** "Kontrol med likvide midler, der føres ind i eller ud af EU: Rådet godkender aftale" (Control of liquid funds carried into or out of the EU: The Council approves agreement). The European Council, accessed on 18 October 2018, http://www.consilium.eu-ropa.eu/da/press/press-releases/2018/06/27/controls-on-cash-entering-and-leaving-the-eu-council-endorses-agreement/

**DR. 2018.** "Nyt supervåben i politiet: Mand pågrebet for to voldtægter" (New super weapons in the police: Man arrested for two cases of rape). DR, accessed on 18 October 2018, https://www.dr.dk/nyheder/indland/nyt-supervaaben-i-politiet-mand-paagrebet-voldtaegter

**Elmark, Nils. 2017.** "Kun en tåbe frygter ikke neobankerne" (Only a fool does not fear the neobanks). The Financial Services Union, accessed on 18 October 2018, https://www.finansforbundet.dk/da/nyheder-aktuelt/Sider/Kunentaabefrygterikkeneobankerne.aspx

**The Ministry of Industry, Business and Financial Affairs. 2016.** "Troels Lund Poulsen tightens the grip on exchange offices". The Ministry of Industry, Business and Financial Affairs, accessed

on 18 October 2018, https://em.dk/nyheder/2016/16-09-14-troels-lund-poulsen-strammer-grebet-om -vekselkontorer

**The Ministry of Industry, Business and Financial Affairs. 2018.** "Ny hvidvaskaftale bringer bødeniveauet i Danmark i den absolute top i Europa og effektiviserer tilsynet med bankerne" (New anti-money laundering agreement brings the penalty level in Denmark into the absolute top in Europe and introduces more efficient supervision of banks). The Ministry of Industry, Business and Financial Affairs, accessed on 18 October 2018, https://em.dk/nyheder/2018/09-19-hvidvaskstrategi

**Danish Business Authority. 2017.** "Reelle ejere" (Beneficial owners). Danish Business Authority, accessed on 18 October 2018, https://erhvervsstyrelsen.dk/reelle-ejere

**Danish Business Authority. 2018.** "Analyse af iværksætterselskaber 2018" (Analysis of entrepreneurial companies 2018". Danish Business Authority, accessed on 18 October 2018, https://erhvervsstyrelsen.dk/sites/default/files/media/analyse\_af\_ivaerksaetterselskaber.pdf

**European Commission. 2017.** "Report from the Commission to the European Parliament and the Council – on the assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities – Annex SNRA Part 2". European Commission, accessed on 18 October 2018, http://ec.europa.eu/newsroom/document.cfm?doc\_id=45653

**European Commission. 2018.** "Strengthened EU rules to prevent money laundering and terrorism financing". European Commission, accessed on 18 October 2018, http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc\_id=48935

**European Banking Authority. 2014.** "EBA Consumer Trends Report 2014". EBA, accessed on 18 October 2018, http://www.eba.europa.eu/documents/10180/534414/EBA+Consumer+Trends+Report+2014.pdf

**Europol. 2015.** "Why cash is still king". Europol – Financial Intelligence Group, accessed on 18 October 2018,

https://www.europol.europa.eu/sites/default/files/documents/europolcik%20%281%29.pdf

**Europol. 2017.** "SOCTA – European Union, Serious and Organised Crime Threat Assessment, Crime in the age of technology". Europol - The European Union, accessed on 18 October 2018, https://www.europol.europa.eu/sites/default/files/documents/socta2017\_0.pdf

**FATF. 2010.** "Money Laundering through Money Remittance and Currency Exchange Providers". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/ML%20through%20Re-mittance%20and%20Currency%20Exchange%20Providers.pdf

**FATF. 2013a.** "The role of Hawala and other similar service providers in money laundering and terrorist financing". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf

**FATF. 2013b.** "National Money Laundering and Terrorist Financing Risk Assessment". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/content/images/National\_ML\_TF\_Risk\_Assessment.pdf

**FATF. 2013c.** "Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf

**FATF. 2015a.** "Money Laundering Through the Physical Transportation of Cash". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf

**FATF. 2015b.** "Guidance for a risk-based approach to virtual currencies". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

**FATF. 2017.** "Anti-money laundering and counter-terrorist financing measures – Denmark – "Mutual Evaluation Report". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Denmark-2017.pdf

**FATF. N.d.** "Money Laundering". FATF, accessed on 18 October 2018, http://www.fatf-gafi.org/faq/moneylaundering/

**Danish Bankers Association. 2017**. "Transaktioner – Se statistik på straksbetalinger og intradagstraktioner herunder" (Transactions - See statistics of instant payment and intraday transactions). Danish Bankers Association, accessed on 18 October 2018, https://finansdanmark.dk/toerre-tal/institutter-filialer-ansatte/betalinger/transaktioner/

**Danish Bankers Association. 2018.** "Ny hvidvaskstrategi og task force vil opruste indsatsen" (New anti-money laundering strategy and task force will boost action). Danish Bankers Association,

accessed on 18 October 2018, https://www.finansdanmark.dk/nyheder/2018/ny-hvidvaskstrategi-og -task-force-vil-opruste-indsatsen/

**Financial Sector Training Centre. 2014.** "Digitale tendenser i finanssektoren – Neobanker" (Digital trends in the financial sector – Neobanks). Financial Sector Training Centre, accessed on 18 October 2018,

http://ipaper.ipapercms.dk/FinansUdd/FUbrochurer/Digitaletendenser2014/Neobanker/?page=1

**Danish FSA. 2018.** "Pengeinstitutternes størrelsesgruppering - Pengeinstitutterne fordelt efter størrelse 2018" (Grouping of banks by size – banks distributed according to size 2018). Danish FSA, accessed on 18 October 2018,

 $https://www.finanstilsynet.dk/ \sim /media/Tal-og-fakta/2017/Gruppeopdeling2018-xlsx.xlsx?la=da/Salaa-balaa-balaa/Salaa-balaa-balaa/Salaa-b$ 

**Danish Defence Intelligence Service. 2017.** "Trusselsvurdering – Cybertruslen mod Danmark" (Threat evaluation – The cyber threat against Denmark). Danish Defence Intelligence Service, Threat Evaluation Unit at the Centre for Cyber Security, accessed on 18 October 2018, https://fe-ddis.dk/cfcs/cfcsdocuments/cybertruslen%20mod%20danmark.pdf

**Kruize, Peter. 2018.** "Internetkriminalitet 2017 – Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cyberspace" (Cybercrime 2017 – Victim study in identity theft, fraud, extortion and harassment in cyberspace". Faculty of Law, Copenhagen University and the Crime Prevention Council, accessed on 18 October 2018, https://dkr.dk/media/13026/internetkriminalitet-2017-final.pdf

**Kyvsgaard, Britta. 2017.** "Udviklingen i børne- og ungdomskriminalitet 2006-2016" (Developments in child and juvenile crime 2006-2016). Research Office of the Ministry of Justice, accessed on 18 October 2018,

http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningsrapporter/2017/rapport\_udviklingen\_i\_boerne\_og\_ungdomskriminalitet\_2006-2016.pdf

Laursen, Anders & Kyed, Jon Hasling. 2014. Virtuelle valutaer (Virtual currencies). Denmark's Central Bank, accessed on 18 October 2018, http://www.nationalbanken.dk/da/publikationer/Documents/2014/03/Virtuelle\_KVO1\_2014.pdf

**OECD. 2016.** "States of Fragility 2016: Understanding Violence". OECD, accessed on 18 October 2018, http://www.keepeek.com/Digital-Asset-Management/oecd/development/states-of-fragility-2016\_9789264267213-a#.WRnEfLtdC70#page8

**Pedersen, Rene. 2017.** "IOT-producenterne er fuldstændig ligeglade med sikkerhed" (IOT producers could not care less about security). IDA Universe, accessed on 18 October 2018, https://universe.ida.dk/artikel/iot-producenterne-er-fuldstaendig-ligeglade-med-sikkerhed-35415/

**Police. 2017.** "National strategisk analyse" (National strategic analysis 2017). Danish Police, accessed on 18 October 2018, https://www.politi.dk/NR/rdonlyres/60D84675-DFA7-46FE-BDEC-6FE6545FC8AF/0/Rapport\_NSA17\_enkeltsider.pdf

**The Government. 2016.** "Aftale om Danmarks tilknytning til Europol efter 1. maj 2017" (Agreement on Denmark's association with Europol after 1 May 2017). The Government, accessed on 18 October 2018, https://www.regeringen.dk/media/2740/aftale-om -europol-pdf.pdf

**Rockwool Foundation Research. 2018.** "Bag beskæftigelsesrekorden: Arbejdsmarkedets kernetropper fortsat langt under 2008-niveau" (Behind the employment record: The labour market's core troops still far below 2008 level). Research of the Rockwool Foundation, accessed on 18 October 2018, https://www.rockwoolfonden.dk/app/uploads/2018/03/Kort-Nyt-Marts-2018-Bagbeskæftigelsesrekorden.pdf

Savona Ernesto U. & Riccardi Michele. 2015. "From illegal markets to legitimate businesses: The Portfolio of Organised Crime in Europe". Final Report of Project OCP – Organised Crime Portfolio, accessed on 18 October 2018, http://www.transcrime.it/wp-content/uploads/2015/12/ocp.pdf

**Tax Authority. 2017.** "Kontrolaktiviteter i 2017 - Styrket regelefterlevelse på skatteområdet" (Control activities in 2017 – Strengthened compliance in the tax area). Tax Authority, accessed on 18 October 2018, <u>www.skat.dk/getFile.aspx?id=133852</u>

**Tax Administration. N.d.** "Om skatteforvaltningen" (About the Tax Administration). The Tax Administration, accessed on 18 October 2018, <u>https://www.skatteforvaltningen.dk/om-skatteforvalt-ningen/</u>

**Ministry of Taxation. 2017.** "Forslag til en stærkere myndighedsindsats mod organiseret svindel" (Proposals for reinforced measures from the authorities against organised fraud). Ministry of Taxation, accessed on 18 October 2018, <u>https://www.skm.dk/media/1554416/rapport-tvaerministeriel-arbejdsgruppe-moms-og -skattesvig.pdf</u>

**Gambling Authority. 2018a.** "Årsberetning 2017" (Annual Report 2017). Gambling Authority, accessed on 18 October 2018, https://spillemyndigheden.dk/sites/default/files/filer-til-down-load/spillemyndigheden \_-\_aarsberetning\_2017.pdf

**Gambling Authority. 2018b.** "Vejledning om væddemål og onlinekasino – Beskrivelse af krav til ansøgere til tilladelse om udbud af væddemål og onlinekasino" (Guidelines on betting and online casino – Description of requirements for applicants for permission to provide betting and online casino). Gambling Authority, accessed on 18 October 2018, https://spillemyndigheden.dk/sites/de-fault/files/filer-til-download/vejledning\_om\_vaeddemaal\_og\_onlinecasino\_-juli\_2018\_.pdf

**SØIK. 2015.** "Hvidvask i Danmark – Den nationale risikovurdering 2015" (Money laundering in Denmark – National Risk Assessment 2015). Prosecution Service, accessed on 18 October 2018, https://www.anklagemyndigheden.dk/sites/default/files/Documents/hvidvask-i-danmark-den-natio-nale-risikovurdering-%202015.pdf

**Sørensen, Catharina. 2018.** "Retsforbehold kan blokere konfiskation af milliarder" (The judicial opt-out may block confiscation of billions". Think Tank Europa, accessed on 18 October 2018, http://thinkeuropa.dk/sites/default/files/notat\_retsforbehold\_kan\_blokere\_konfiskation\_af\_milliarder.pdf

**UBS. 2017.** "Cryptocurrencies". UBS, Chief Investment Office Americas, Wealth Management, accessed on 18 October 2018, https://www.ubs.com/content/dam/WealthManagementAmericas/cioimpact/cryptocurrencies.pdf

**Ministry of Immigration and Integration. 2017.** "Regeringen opretholder grænsekontrollen" (The Government maintains border control). Ministry of Immigration and Integration, accessed on 18 October 2018, http://uim.dk/nyheder/2017/2017-10/regeringen -opretholder-graensekontrollen

Utrecht University. 2013. "The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy". Universiteit Utrecht, accessed on 18 October 2018, http://www2.econ.uu.nl/users/unger/ecolef\_files/Final%20ECOLEF%20report%20(digital%20version).pdf

**Ministry of Economic and Interior Affairs. 2018**. "Økonomisk Redegørelse - August 2018" (Economic Statement - August 2018). Ministry for Economic and Interior Affairs, accessed on 18 October 2018, https://oim.dk/media/20423/oekonomisk-redegoerelse-2-270818\_web.pdf

### **Appendix 1: Concepts and definitions**

AIF/FAIF funds: (Administrators of) alternative investment funds.

**BEC/CEO fraud:** (Business e-mail compromise) False invoices or false e-mails that seem to be genuine are sent to the person responsible for financial affairs or the bookkeeper in a company. The sender pretends to be an executive or a colleague who asks the employee to pay the invoice or transfer a specific amount to a particular named account held by the criminal.

**Chip dumping:** One or several poker players in a tournament dump(s) their chips with a particular player (according to agreement), whereby that player in the tournament has a very low risk and big winnings. It is categorised as game fixing, but can be difficult to detect.

**DDos attack:** (Distributed denial of service) A website is flooded by an individual who controls several computers at the same time, making them send enquiries automatically to the same internet address endlessly, causing the website to be inaccessible.

E-wallet: an electronic wallet which makes it possible to carry out instant payments.

**IPR:** (Intellectual Property Rights) Crime which infringes rights in branded goods (sale of counterfeit branded goods) or illegal streaming of television signals or films.

**Leasing (financial):** In financial leasing, the lessee is responsible for negotiating with the supplier and, provided the leasing agreement contains residual value, will be obliged on demand from the lessor to present a buyer for the leased object at the end of the leasing period. In financial leasing, the leasing payments cover repayment of the whole of or material parts of the purchase price.

**Leasing: (operational):** In operational leasing, the lessor is responsible for negotiating with the supplier and bears the risk of the residual value of the object on expiry of the leasing period. The leasing payments do not cover repayment in full of the entire purchase price.

**Phishing:** A fraudster tries to trick a person's user name, password, credit card or bank details out of the person. The most frequent MO is to make the user receive a false e-mail, which appears to come from a company in which the individual has confidence. The individual passes on the information voluntarily, not knowing that the e-mail is false and that the information is being passed on to criminals who misuse it subsequently.

**Ransomware:** A website or an IT system is infiltrated by a virus that freezes or encrypts all data. Next, the owner is required to pay a ransom by way of cash or knowledge to have the data released again.

**Smishing:** Phishing via SMS, where persons are tricked out of their codes, card information or similar.

**Sextortion:** Extortion where a perpetrator has acquired access to sexual photos of a person or pretends to have such access, whereupon the perpetrator extorts the person by threatening to publish the photos if the person does not pay money or send further photos to the perpetrator.