

---

# National risk assessment of terrorist financing

January 2024





# Content

---

Preface	4
List of words and definitions	5
<b>01</b> Introduction	7
<b>02</b> Terrorist financing	11
<b>03</b> Criminalization of terrorist financing	16
<b>04</b> Threats relating to terrorist financing	19
<b>05</b> Vulnerabilities relating to terrorist financing	22
<b>06</b> Greenland and the Faroe Islands	25
<b>07</b> Cryptoassets	26
<b>08</b> The nonprofit sector	30
<b>09</b> Cash and high value goods	34
<b>10</b> Illegal value transfer systems	36
<b>11</b> Authorized money service businesses	38
<b>12</b> The banking sector	40
<b>13</b> Terrorist financing based on organized economic crime	44
<b>14</b> Identity misuse and derived crime	47
<b>15</b> Benefit fraud	48
<b>16</b> Other risk areas	50
<b>17</b> Empirical data and literature	52
<b>Appendix 1</b> Model for assessment of special risk areas	54

# Preface

---

This is the third time that the Danish Security and Intelligence Service (PET) publishes the National Risk Assessment of Terrorist Financing. The risk assessment has been prepared in cooperation with stakeholders from the entire Danish Realm, and PET would like to thank everyone for their interest and contributions as well as our dialogue. The cooperation has been constructive, reflecting the close relations across Danish authorities, trade organizations and obliged entities.

The risk assessment has been prepared on the basis of international recommendations as regards methodology and stakeholder involvement. We have also been inspired by foreign risk assessments of terrorist financing and money laundering, and we have drawn upon current research and risk assessments in other areas as well. This means that the methodology and format of risk assessments of terrorist financing in Denmark will change over time, and this new national risk assessment is no exception. Compared with the most recent risk assessment from January 2020, the most important changes are that the new risk assessment makes a clearer distinction between threats, vulnerabilities and risks in connection with terrorist financing and explains how these concepts affect each other. Further, we have focused more on the description of various risk areas as requested by many obliged entities.

PET and the Danish Financial Intelligence Unit (FIU) are benefiting from close and strong cooperation, which was further emphasized when we prepared the new national risk assessments of money laundering and terrorist financing, respectively. It has proved highly profitable to coordinate and share knowledge of vulnerabilities and thematic overlap.

During the preparation, both risk assessments formed the basis of the national strategy for prevention and countering of money laundering and terrorist financing 2022-2025 (National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025), which was published by the Danish government in July 2022. The new national strategy emphasizes that the crime picture as well as social developments are dynamic, which requires focused and coherent efforts to counter money laundering and terrorist financing.

PET looks forward to continuing these joint efforts, and PET's national risk assessments of terrorist financing together with the national risk assessments of money laundering published by the Danish FIU and the supra-national risk assessments of the European Commission will form a key basis for these efforts.

Enjoy the read!  
PET



## List of words and definitions



**Authorized money service businesses:** Authorized money service businesses may be businesses which have money transfers as their core service, or businesses which serve as the agents for major foreign money service businesses in connection with trade related to convenience or grocery stores. Authorized money service businesses are subject to supervision by the Danish Financial Supervisory Authority and the obligations stipulated by the Danish Anti-Money Laundering Act.

**FATF:** The Financial Action Task Force is an intergovernmental body, which is responsible for developing policies for combatting money laundering and terrorist financing.

**Hawala:** A money transfer service where the ingoing and outgoing money transfer locations differ, and where the outstanding balance between the two parties is settled separately, and therefore the transaction does not appear as an electronic transfer.

**Identity misuse:** The general term for the misuse of a (digital) identity involving property crime.

**Cryptoassets:** A digital representation of values or contractual rights which may be transferred or stored electronically via a distributed ledger technology (DLT) or a similar technology.

**The nonprofit sector:** Associations, nonprofit foundations and fundraising etc.

**Illegal value transfer systems:** Unregistered and thus illegal commercial transfers of funds via financial services or hawala.

**Obligated entities:** Pursuant to Section 26 of the Danish Anti-Money Laundering Act, companies and individuals covered by Section 1 of the Anti-Money Laundering Act must notify the Danish FIU if they know, suspect or reasonably assume that transactions, funds or activities are or have been related to money laundering or terrorist financing.



# Introduction

## Objective

The objective of this risk assessment is to prevent terrorist financing in Denmark and abroad. Thus, the risk assessment contributes to increasing the knowledge of terrorist financing among the obliged entities. Therefore, these companies and individuals should take the risk assessment into account when they assess the risk of being misused for money laundering or terrorist financing, and when they establish internal controls. Further, the authorities can apply the risk assessment in their risk-based approach to preparing guidelines and controls.

## Analysis design

The risk assessment consists of two parts: Part I is of a general nature, with Chapter 2 introducing the reader to terrorist financing and the risk concept, and with Chapter 3 giving an account of the current criminalization of terrorist financing in Denmark. Chapters 4 and 5 are about the threats and vulnerabilities relating to terrorist financing in Denmark. Chapter 6 concludes Part I by separately assessing threats and vulnerabilities relating to terrorist financing in Greenland and the Faroe Islands.

Part II of the risk assessment consists of chapters 7-16, with each chapter focusing on high-risk areas such as illegal value transfer systems and cryptoassets. The focus of each chapter is a separate assessment of the risk of terrorist financing within the area in question.

## Main findings

Chapters 4-15 start by summarizing the most important findings of each chapter. The main findings of the risk assessment are summarized below.

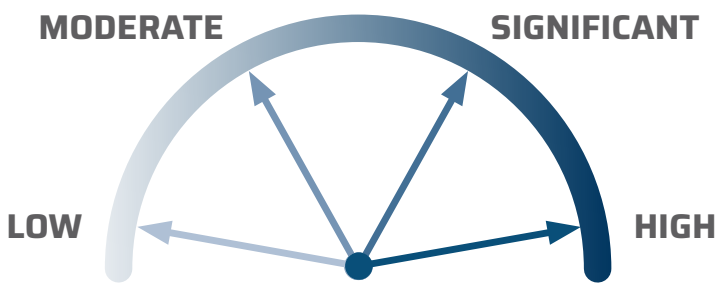
### The threat relating to terrorist financing

Based on the most recent Assessment of the Terrorist Threat to Denmark published by PET's Centre for Terror Analysis (CTA) in March 2023, PET assesses that terrorist financing by individuals in Denmark is mainly channelled to militant Islamist groups in Syria, Iraq, Somalia and Türkiye, and to a lesser extent Afghanistan, Lebanon and Palestine. The funds help sustain terrorist groups and promote their activities, and the inflow of financial resources improves their capacity to carry out operations and to recruit and retain members.

### Vulnerabilities relating to terrorist financing

In PET's assessment, there are a number of structural vulnerabilities underlying terrorist financing, such as inadequate knowledge and understanding among obliged entities, a need for further sharing of data and information between relevant actors and a need for further IT support of data sharing. In addition, more obliged entities should register in order to be able to notify relevant parties electronically of any suspicion of money laundering and terrorist financing.

## BAROMETER FOR ASSESSING THE TERRORIST FINANCING RISK



The terrorist financing risk is assessed on the basis of the above risk model, which reflects the threat of terrorist financing coupled with financial vulnerabilities and consequences. The threat is relatively homogeneous for all the risk areas, whereas the vulnerabilities within the individual risk areas differ more. This applies for instance to costs, anonymity and cross-border transactions.

The model has four levels: Low, moderate, significant and high. The same risk model is seen in the national risk assessment of money laundering 2022 (Den Nationale Risikovurdering af Hvidvask 2022) published by the Danish FIU.

### Greenland and the Faroe Islands

PET assesses that the risk of terrorist financing in Greenland and the Faroe Islands is **low** due to a minimal terrorist threat level.

### High risk of terrorist financing via cryptoassets

PET assesses that there is a **high** risk that cryptoassets are being used for terrorist financing. Cryptoassets are an attractive means of terrorist financing as there is a

demand for transactions that may be carried out swiftly and without any geographical limitations.

### High risk of terrorist financing via the nonprofit sector

PET assesses that the risk of terrorist financing via the nonprofit area is **high**. The reason is that in PET's assessment there is a network in Denmark with the capability and will to procure funds through, for instance, fundraising in support of terrorist organizations or terrorist-like activities.


### High risk of terrorist financing via cash and high value goods

PET assesses that the risk that cash and high value goods are being used for terrorist financing is **high**. Cash and high value goods are attractive in several stages of terrorist financing, and the means of payment are characterized by a low risk of detection and low costs.

### High risk of terrorist financing via illegal value transfer systems

PET assesses that the risk of terrorist financing via illegal value transfer systems is **high**. Illegal value transfer systems are one of the few ways of moving funds into con-





flict zones, and there are a number of important vulnerabilities within the area.

### **High risk of terrorist financing via authorized money service businesses**

PET assesses that there is a **high** risk that authorized money service businesses are being misused for terrorist financing. The risk of terrorist financing is high because money service businesses are typically able to transport funds closer to conflict zones and at a lower cost than banks.

### **Significant risk of terrorist financing via the banking sector**

PET assesses that there is a significant risk that the banking sector is being used for terrorist financing.

Banking services are easily accessible and can be used at all stages of terrorist financing. However, most banks have integrated a number of mitigating actions and invested in technical as well as human resources.

### **Significant risk of terrorist financing via organized economic crime**

PET assesses that the risk of terrorist financing based on the proceeds of organized economic crime is **significant**.

The reason is that there may be extremist sympathies in criminal networks and that economic crime by professionals contains elements of anonymity, cross-border transactions, large amounts and the acceptance of financial costs.

### **Significant risk of terrorist financing via identity misuse and derived crime**

PET assesses that identity misuse and derived crime represent a **significant** risk of terrorist financing. This area is attractive for procurement of illegal funds, and the risk of detection may be reduced, because this type of crime may appear legal as true digital identities are used.

### **Moderate risk of terrorist financing via benefit fraud**

PET assesses that there is a **moderate** risk that benefit fraud may be used for terrorist financing. Benefit fraud is assessed to be attractive among individuals in extremist communities, but the considerable focus on the threat by the authorities as well as by obliged entities is assessed to mitigate the risk. ■



MasterCard

4375

4375

3388

# 02

## Terrorist financing

Terrorist financing is defined as activities aimed at providing financial support to an individual, a group or an association that intends to commit acts of terrorism. Activities related to terrorist financing may be divided into four stages<sup>1)</sup>:

- Procurement of funds, for example through legitimate income, fundraising or criminal activities
- Storage of funds
- Transfer of funds, for example to recipients abroad
- Actual use of funds for terror-related activities.

Assessing terrorist financing in Denmark has always been, and still is, difficult. PET assesses that terrorist financing in Denmark cannot be compared with money laundering in economic terms as the economic value of terrorist financing is less important.

Relatively few sentences for terrorist financing have been issued in the Nordic countries. In Denmark, 13 individuals were charged with violation of Section 114 b of the Danish Criminal Code in five cases from 1 January 2019 to 1 October 2022.

It may be difficult to establish, and thus provide evidence of, the financial trail through or to jurisdictions far away from Denmark, and it may also be difficult to prove direct intent to finance terrorism.

PET benefits significantly from notifications with suspicion of terrorist financing as they contribute to the general intelligence picture and to PET's actual knowledge of known actors as well as individuals and communities previously unknown to PET.

There is no minimum threshold for notifying on suspected terrorist financing. The amounts involved in terrorist financing are often smaller than those involved in money laundering, and therefore terrorist financing often appears in less complex constructions than for example invoice fraud and trade-based money laundering. PET assesses that the two-digit million amounts involved in a case from 2016 concerning PKK and a case from 2022 concerning Arab Struggle Movement for the Liberation of Ahwaz (ASMLA) are higher than what is usually seen in terrorist financing. The ASMLA case is described further below.

Funds for terrorist financing may have been obtained legally or illegally. Further, funds may appear legal at some stages and illegal at other stages on their way to the final destination. Thus, terrorist financing may involve "blackwashing", which means that legally acquired funds are being used to finance illegal activities or are otherwise being transferred from a legal to an illegal context, or it may involve funds obtained from one or more criminal acts and used for financing terrorism.

The specific use of the funds may be attack and/or organizational financing. In general, attack financing will usually concern one or a few individuals preparing an attack, and their costs will equal the ongoing operational task. By contrast, organizational financing generally relates to a more long-term organizational build-up with established income and cost structures. Such organizational structures may resemble those of a company or an association.

---

1) For ease of communication, PET applies a four-stage model. For more information on the stages of terrorist financing, see Davis (2021): *Illicit Money: Financing Terrorism in the 21st Century*, page 5.

ATTACK FINANCING	ORGANIZATIONAL FINANCING
Rent and accommodation expenses	Propaganda and recruitment
Communication expenses for telephones, pay-as-you-go cards, internet	Intelligence activities and operational security
Purchases of weapons, explosives and components	Social benefits, wages and salaries, unemployment and other benefits
Purchases of operational equipment	Corruption and political lobbying
Car rental and other transport expenses	Financing of attacks and cells
Other living expenses	Support to other terrorist organizations

Another characteristic of terrorist financing is that it generally follows a linear path in which funds are procured and transported in a chain, from procurement to the end user. By contrast, money laundering is generally a circular process in which the illegally obtained funds are repositioned, laundered and returned to the same criminal person.

It is being debated whether new technologies will change terrorist financing substantially and give rise to much concern, or whether the new technologies do not represent a higher risk<sup>2</sup>. PET assesses that terrorist financing is characterized by traditional methods and behaviour, but simultaneously it is supplemented by new technological opportunities for procurement, storage and transfer of funds. This assessment is shared by researchers from the EU-supported Project CRAFT<sup>3</sup>, who write the following about organizational financing: *"...there are few indications that new technologies have displaced older techniques, such as MSB's, hawala and cash couriating, which continue to dominate the scene. What appears to be the case is the use of old and new methods together, in pragmatic combinations that suit the terrorist financiers."*<sup>4</sup>

### Method for assessment of terrorist financing risk

The Financial Action Task Force (FATF) defines terrorist financing risk as a function of threats, vulnerabilities and consequences relating to terrorist financing.


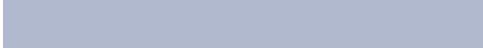

The FATF is an international organization which aims to combat money laundering, terrorist financing and proliferation financing (the financing of proliferation of weapons of mass destruction). The FATF has adopted 40 specific recommendations for technical measures to be implemented by the member countries, and in addition the organization has adopted 11 different efficiency criteria that focus on the extent to which the member countries are able to reduce risk and threats in relation to money laundering, terrorist financing and proliferation financing. More than 200 jurisdictions worldwide have joined the FATF.

The threat relating to terrorist financing shall be taken to mean individuals or organizations wanting to finance terrorist attacks or terrorist organizations. In a criminal law context, the threat related to terrorist financing means the threat that individuals or organizations will finance terrorism, cf. Section 114 b of the Danish Criminal Code.

2) See for instance Reimer & Redhead (2022): *Bit by Bit - Impacts of New Technologies on Terrorism Financing Risks*, page 11

3) Project CRAFT is an academic research and community-building initiative designed to build stronger, more coordinated counter terrorist financing (CTF) capacity across the EU and in its neighbourhood. The project engages with authorities and private entities in order to promote cross-border connectivity and targeted research. Project CRAFT.

4) Reimer & Redhead (2022): *Bit by Bit - Impacts of New Technologies on Terrorism Financing Risks*, page 37. See also Davis, Jessica (2022): *New Technologies but Old Methods in Terrorism Financing*, page 5.



The FATF defines vulnerabilities as follows: *“The concept of TF vulnerability comprises of those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type of service that makes them attractive for TF”*.<sup>5</sup> Thus, a vulnerability or weakness is something that a potential threat may exploit, or that may facilitate or support activities relating to the threat. The vulnerabilities may be structural, deriving from weaknesses in the regulation or legislation in an area (which makes it attractive to finance activities from or through the country in question). Vulnerabilities may also relate to risk areas associated with specific industries or special financial products or services.

An example of the interrelation between threats and vulnerabilities relating to terrorist financing is the increasing importance of terrorist financing vulnerabilities specifically relating to foreign transfers triggered by the growing terrorist financing threat caused by the conflict in Syria and Iraq as these vulnerabilities could enable transfers to the conflict zones or neighbouring countries such as Türkiye, Iraq and Lebanon.

Theoretically, there is often overlap between vulnerabilities relating to money laundering and terrorist financing, and this also applies to Denmark. Readers of this risk assessment are recommended to read the chapter on vulnerabilities in Danish money laundering efforts in the national risk assessment of money laundering 2022 published in January 2023 by the Danish FIU.

Consequences refer to situations in which terrorist financing actually takes place and thereby enables acts of terrorism. Compared with money laundering, the consequences of terrorist financing are often more severe, and they may cause deaths, injuries or damage to critical infrastructure, but there are also more structural consequences for society and democracy.

The complexity of the assessment of the terrorist financing risk is high, as the terrorist threat may come from Denmark and/or abroad. This was illustrated by a city court decision concerning ASMLA in March 2022. Three individuals were convicted of financing, and attempting to finance, terrorism as they had procured DKK 15m and had attempted to procure at least DKK 15m from a Saudi intelligence service to ASMLA and its armed subgroup Martyr Muhyiddin Al-Nasser Brigade in Iran<sup>6</sup>.

---

5) FATF (2019): *Terrorist Financing Risk Assessment Guidance 2019*, page 8.

6) *The court of Roskilde (2022): Decision in the criminal case against three members of ASMLA. Domstol.dk*



The terrorist threat in the ASMLA case was directed at Iran, but parts of the network engaged in the financing were located in Denmark. The funds that they attempted to procure came from the Saudi intelligence service.

When PET assesses that a risk area has a certain risk level, cf. chapters 7-16, it does not mean, for instance, that the same risk level applies to all obliged entities within this risk area. Risks may often differ significantly depending on the products, customers and geographical area of the companies. The obliged entities must, in their own risk assessments, evaluate their business models, products, customer segments etc. and thus their own specific risk.

Obliged entities are very much encouraged to base their work on hypotheses when they examine the risk of money laundering and terrorist financing in specific cases. Thus, if an obliged entity observes a suspicious incident, for instance in connection with a customer request or in their transaction monitoring, the suspicion is dealt with on the basis of relevant hypotheses. It is assessed whether the incident may involve trade-based money

laundering, terrorist financing, legal matters, fraud, trade in drugs or something else entirely. The different hypotheses are strengthened or weakened by the data available and any new information obtained. In this connection, the methodology of the risk assessment may be used as a basis for hypotheses about the specific suspicion.

PET has initiated a number of ongoing preventive efforts, including PET training sessions, presentations, awareness and training activities, and the risk assessment will be a key component of the continued efforts to minimize risk relating to terrorist financing. The assessment of the terrorist financing risk may serve as the basis for such activities and for a continuous dialogue with the authorities, obliged entities as well as academia. ■



# 03

## Criminalization of terrorist financing

In Denmark, terrorist financing is a criminal offence under Section 114 b of the Danish Criminal Code, which reads as follows:

“Imprisonment for a term not exceeding 12 years is imposed on any person who –

- (i) grants financial support, whether directly or indirectly, to;
- (ii) organizes or raises funds, whether directly or indirectly, for; or
- (iii) makes funding, other property, or financial or other similar services available, whether directly or indirectly, to: a person, a group or an association committing or intending to commit any terrorist act falling within Sections 114 or 114a.”

The aim of this provision is to counter any financing of terrorist activities by way of financial support or dissemination etc. to individuals or groups who commit or intend to commit acts of terrorism or terror-like activities.

- **Section 114 b (i)** concerns individuals who donate their own funds to a person, a group or an association committing or intending to commit terrorism or terror-like activities covered by Sections 114 or 114 a of the Danish Criminal Code.
- **Section 114 b (ii)** concerns the intermediary or go-between organization which raises or otherwise procures funds, for example by procuring loans to such person, group or association committing or intending to commit activities covered by Sections 114 or 114 a of the Danish Criminal Code.
- **Section 114 b (iii)** concerns banks and other organizations which, in a business context or otherwise and

with the purpose of financial gain extend loans, provide other financial services or facilitate such services to terrorist groups.

Section 114 b of the Danish Criminal Code is an alternative stipulation relative to accessory liability pursuant to Sections 114 or 114 a, cf. Section 23.

The preparatory work for this provision presupposes that it is punishable by law to provide funds or financial services not only for the illegal activities of a terrorist group, but also for the legal activities of such a group. However, this presupposes intent with regard to the terrorist activities or objectives of the group. It is not a prerequisite that the money or financial services are directly transferred or made available to the group, as the only requirement is that the group is the final beneficiary.


### From intelligence to a criminal case

A terrorist financing case may be initiated in a number of ways. For instance, it may be initiated by suspicion of terrorist financing which PET has screened and found relevant. When PET has investigated the case, charges may be brought and the matter referred for criminal prosecution.

### PET's screening and preliminary investigation

Pursuant to Section 1(1)(i) of the Danish PET Act, the objective of PET is to prevent, investigate and counter crimes against the independence and security of the state and crimes against the constitution and supreme authorities of the state, cf. Chapters 12 and 13 of the Danish Criminal Code. Further, pursuant to Section 6 of the PET Act, investigation and the use of coercive measures (such as telephone interceptions, searches and seizures)





by PET are governed by the general provisions of the Danish Administration of Justice Act, which also apply to the rest of the Danish police.

In certain areas, however, the Danish Administration of Justice Act contains special rules governing the investigation of offences covered by Chapters 12 and 13 of the Danish Criminal Code.

As a general rule, any investigation of potential offences covered by Chapters 12 and 13 (including Section 114 b concerning terrorist financing) of the Danish Criminal Code is conducted by PET. If PET decides that an investigation should be launched, it is possible for PET, in special cases and following submission to the public prosecutor, to agree with the relevant police district that it investigates the case in cooperation with PET.

### **Charges**

PET is the primary authority for assessing whether there are any grounds for pressing charges under the provisions of Chapters 12 and 13 of the Danish Criminal Code. If so, PET brings the case before the public prosecutor. If the public prosecutor agrees that charges should be brought in the case, the public prosecutor will brief the Director of Public Prosecutions on the matter.

When charges have been brought, the continued investigation is carried out by the relevant police district in cooperation with PET.

Furthermore, PET must always be informed if a police district considers initiating an investigation against any person suspected of violating Section 136 of the Danish Criminal Code in relation to crimes covered by Chapters 12 and 13 of the Danish Criminal Code.

Additionally, the Special Crime Unit (NSK) provides PET with any information it may have on possible violations of Chapters 12 or 13 of the Danish Criminal Code. This may include reporting pertaining to the Danish Anti-Money Laundering Act and other types of information. Any investigations launched on the basis of such information must be handled in the same way as other investigations of potential offences covered by Chapters 12 and 13 of the Danish Criminal Code.

### **Decisions on charges**

If the public prosecutor assesses that charges should be brought for violations of the provisions of Chapters 12 and 13 of the Danish Criminal Code, the public prosecutor will bring the case before the Director of Public Prosecutions, who may bring the case before the Minister of Justice, recommending that charges should be brought. If the Minister of Justice endorses the recommendation, charges may be brought.

Reference is made to a letter dated 27 March 2015, in which the Director of Public Prosecutions thoroughly describes the guidelines governing the cooperation between the police districts, PET and the public prosecutor<sup>7</sup>. ■

---

**7)** Chapter 3 is based on the statement of the Director of Public Prosecutions (2022): *Submission and notification etc.* (Forelæggelse og indberetning mv.).



# 04

## Threats relating to terrorist financing

### Summary

Based on the most recent Assessment of the Terrorist Threat to Denmark published by PET's Centre for Terror Analysis (CTA) in March 2023, PET assesses that terrorist financing from individuals in Denmark is mainly aimed at militant Islamist groups in Syria, Iraq, Somalia and Türkiye, and to a lesser extent Afghanistan, Lebanon and Palestine. The funds help sustain terrorist groups and promote their activities, and the inflow of financial resources improves their capacity to carry out operations and to recruit and retain members.

Based on the many notifications concerning terrorist financing, the amounts involved are generally in the range of DKK 0-5,000. Further, most of the notifications concern transactions related to Denmark only.

### Militant Islamism and terrorist financing

PET defines militant Islamism as an interpretation of Islamist ideology that legitimizes the use of violence to achieve political, religious or ideological ends.

In its Assessment of the Terrorist Threat to Denmark from March 2023, CTA assesses that the terrorist threat to Denmark from militant Islamists is significant. The threat picture remains affected by the presence of militant Islamist sympathizers in Denmark who may have

the intent to commit acts of terrorism in Denmark and who take inspiration from transnational militant Islamist groups such as Islamic State and al-Qaeda.

The most likely militant Islamist terrorist attack in Denmark is an attack carried out by a lone actor or a small group using easily accessible means, firearms or improvised explosive devices<sup>8</sup>.

In its Assessment of the Terrorist Threat to Denmark from March 2023, CTA furthermore assesses that terrorist financing from individuals in Denmark is mainly aimed at militant Islamist groups in Syria, Iraq, Somalia and Türkiye and, to a lesser extent, Afghanistan, Lebanon and Palestine. The funds help sustain terrorist groups and promote their activities, and the inflow of financial resources improves their capacity to carry out operations and to recruit and retain members<sup>9</sup>.

In recent years, there have been a number of convictions for violation of the terrorist financing legislation in Denmark. All the cases involved the transfer of money in support of specific individuals or small networks of individuals. In November 2022, four individuals were convicted of terrorist financing as they had made multiple money transfers to two Danish travellers who had joined Islamic State in Syria/Iraq in the period 2013-2017<sup>10</sup>.

---

<sup>8</sup>) CTA (2023): *Assessment of the Terrorist Threat to Denmark*, page 8.

<sup>9</sup>) CTA (2023): *Assessment of the Terrorist Threat to Denmark*, page 15.

<sup>10</sup>) CTA (2023): *Assessment of the Terrorist Threat to Denmark*, pages 15-16.

In connection with suspicion of terrorist financing, the Danish authorities previously focused on the financial behaviour and financial trails of travellers before going to a conflict zone. For instance, situations where one or more individuals procured as much cash as possible, took out a number of several on-line consumer loans, or transferred their identity papers.

The attention of the authorities was due to at least 161 adults travelling to the conflict zones in Syria and Iraq in the period 2012-2016 in order to join militant Islamist groups<sup>11</sup>.

However, according to CTA's Assessment of the Terrorist Threat to Denmark from March 2023, no one has travelled from Denmark to the conflict zone in Syria/Iraq since 2016<sup>12</sup>. PET assesses that the current threat of terrorist financing in connection with future travels to a conflict zone has been significantly reduced.

### **Right-wing extremism and terrorist financing**

PET defines right-wing extremism as a generic term that covers various political views on the extreme right of the political spectrum characterized by combinations of nationalist, authoritarian, anarchist, anti-parliamentary, racist, xenophobic and anti-Semitic viewpoints. The ideological foundation of right-wing extremism may derive

from Nazism, fascism or national conservatism. Right-wing extremists question or reject democracy and consider the use of violence a legitimate means to achieve political ends.

In March 2021, CTA upgraded the threat level to Denmark from right-wing extremism from "limited" to "general", and this threat level was maintained in the most recent Assessment of the Terrorist Threat to Denmark from March 2023.

### **Notifications of terrorist financing**


The Danish FIU informs PET, as the competent authority within terrorist financing, of all suspicions of terrorist financing notified by obliged entities pursuant to Section 26 of the Danish Anti-Money Laundering Act. These notifications form a part of the overall threat and risk picture for terrorist financing, but they are characterized by the heterogenous understanding of the terrorist financing risk picture of the obliged entities, and therefore the notifications differ widely as regards the grounds for suspicion and other aspects. PET screens and assesses all notifications received by the Danish FIU from the obliged entities.

PET's assessments are not only based on the notifications of suspected terrorist financing, but also on PET's

---

**11)** See also *Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism)*, page 73.

**12)** CTA (2023): *Assessment of the Terrorist Threat to Denmark*, page 13.



other sources, including national and international intelligence, investigations of terrorist financing as well as qualitative and quantitative enquiries etc.

In PET's assessment, there should be no lower threshold for amounts giving rise to a notification of suspected terrorist financing, as even small amounts may be of importance to terrorist attacks.

This assessment is supported by PET's most recent data analysis of notifications from the Danish FIU. It clearly appears from the notifications received from the summer of 2020<sup>13</sup> to the end of 2021 that the amounts involved in terrorist financing generally range from DKK 0 to DKK 5,000. PET has experienced that notifications involving small amounts may have a significant intelligence and investigative value, thus contributing to both analyses, intelligence products and actual criminal investigations.

The same data also shows that most notifications concern transactions related to Denmark only. PET assesses that this is due to the fact that banks represent by far the largest source of notifications, and that this proportion would change if for instance money service businesses increased their number of notifications given that banks are far less involved in transfers to high-risk areas.

A review of the notifications of transfers to foreign countries has shown that the quality of the notifications is high: They are relevant and contain a well described and well documented reason for the suspicion. As expected, numerous transactions are made to destinations such as Türkiye and Djibouti, which serve as transit countries to for instance Syria and Somalia. The geographical distribution underpins the threat assessment of terrorist financing of militant Islamism. ■

---

**13)** *In the summer of 2020, PET and the Danish FIU entered into a new agreement on reporting criteria for which reason this time delimitation has been made.*

# Vulnerabilities relating to terrorist financing

## Summary

In PET's assessment, there are a number of structural vulnerabilities that are relevant to both money laundering and terrorist financing such as: Inadequate knowledge and understanding among obliged entities as well as a need for further sharing of data and information between relevant actors and for further IT support of data sharing. In addition, more obliged entities should register in order to be able to notify relevant parties electronically of any suspicion of terrorist financing and money laundering. PET assesses that it is a vulnerability that the phase where funds are transferred for terrorist financing is underrepresented in the notifications because the amount of notifications from money service businesses is insufficient.

## Structural vulnerabilities

Terrorist financing and money laundering share a number of key structural vulnerabilities, which are addressed in the Danish government's most recent national strategy within the area<sup>14</sup>:

Inadequate knowledge and understanding about terrorist financing are vulnerabilities as regards the authorities, trade organizations and obliged entities. In order to counter the threat from terrorist financing, it is crucial

that everyone has a risk-based approach and has a correct view of the threats and risks. Not least among the obliged entities, which are often the first bulwark against terrorist financing. PET assesses that, in recent years, financial institutions have gained a better understanding of risk than non-financial sectors, and that this is due to their understanding of criminal actors and risks. This view is shared by the Danish FIU<sup>15</sup>.

It remains a vulnerability that the sharing of data and information is affected by the differing rules of the authorities. The consequence is that law enforcement, administrative and supervisory authorities cannot freely share information that serves to counter money laundering and terrorist financing. In addition, obliged entities are not able to share information on specific actors. For instance, a bank cannot currently share its suspicion of terrorist financing with another bank in connection with a potential new customer.

This vulnerability also relates to the IT support of the authorities' efforts within anti-money laundering and counterterrorism financing, where the need for automated data sharing and searches in joint systems is growing. The terrorist financing and money laundering field is characterized by large quantities of data and cases. For

<sup>14</sup> The Danish Government (2022): *National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025 (Denmark's 2022-2025 national strategy for combatting money laundering and terrorist financing)*.

<sup>15</sup> The Danish Financial Intelligence Unit (2022): *Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering)*, section 04.4.

instance, the Danish FIU received about 90,000 notifications of suspected money laundering in 2022, and therefore appropriate case handling requires that data and information can be collected automatically.

As identified in the national risk assessment of money laundering published by the Danish FIU (*National Risikovurdering af Hvidvask*), only about 10% of the obliged entities have registered with goAML (IT platform used by the Danish FIU for notifications), which allows them to notify the authority about money laundering and terrorist financing<sup>16</sup>. Obligated entities are not required to register with goAML, but notifications depend on this communication channel, as it is generally not possible to use other channels. It is obviously a vulnerability within terrorist financing that so many obliged entities are unable to do so. This situation is particularly acute for obliged entities that are not part of the financial sector.

As appears from the chapter “Threats relating to terrorist financing”, these companies and individuals will often have ties to geographical areas that have weak mechanisms for combatting terrorist financing and money laundering, and where banks and sometimes also money service businesses find it difficult to have a presence. This reduces the possibility of identifying and document-

ing the money trail and limits the legal tools of the Danish authorities for collecting information.

### **Over- and underrepresentation of notifications of terrorist financing**

In 2021, Danish banks accounted for a very significant amount of notifications of terrorist financing, whereas PET received relatively few notifications from money service businesses.

PET assesses that it is a vulnerability that transfers to foreign countries are underrepresented in the notifications, because the number of notifications from for instance money service businesses is insufficient. The fact that most of the money laundering notifications concern transfers within Denmark contrasts with PET’s assessment that terrorist financing from individuals in Denmark is chiefly aimed at militant Islamist groups in Syria, Iraq, Somalia, Lebanon, Afghanistan and Palestine. PET assesses that this is probably due to a number of factors, such as the fact that banks only to a very limited extent carry out transactions to high-risk countries, but also that a number of other obliged entities do not notify as much as warranted by their risk profile. ■

---

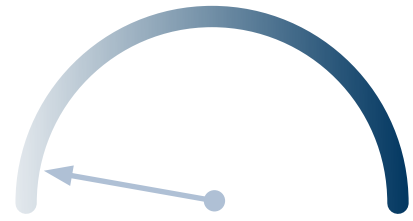
**16)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 04.3.*





# 06

## Greenland and the Faroe Islands



### Summary

PET assesses that the risk of terrorist financing in Greenland and the Faroe Islands is low due to a minimal terrorist threat level. There are vulnerabilities both in Greenland and the Faroe Islands as regards terrorist financing, but as the threat is minimal, their impact on the risk remains limited.

According to the Assessment of the Terrorist Threat to Denmark published in March 2023, the level of the terrorist threat to Greenland is minimal. In terms of PET's definitions, this means that there are no indications of any threat: There is absence of intent, capability or both. CTA assesses that violent extremism is less widespread in Greenland. However, extremist propaganda may still influence individuals in Greenland to commit acts of violence. Socially marginalized or vulnerable young people may be particularly susceptible to radicalization.

PET assesses that the risk of terrorist financing is highly affected by the minimal terrorist threat to Greenland, and therefore the threat level reduces the risk implication of the vulnerabilities. PET has thoroughly mapped out the vulnerabilities of the financial infrastructure in Greenland together with the Danish FIU. In this connection, reference is made to the FIU's national risk assessment of money laundering, which contains a comprehensive chapter on Greenland that may also form part of the efforts aimed at countering the terrorist financing risk.

The small size of the population of Greenland represents a vulnerability as there is a risk of conflicting interests or of shared interests between closely related individuals. For instance, there is a risk when an employee is to carry out customer due diligence procedures or examine sus-

picious circumstances regarding a customer whom the employee knows from another context. Further, it is a relevant vulnerability that Greenland is a more cash-intensive society, which offers better opportunities for collecting and transferring funds for terrorist purposes without being detected. The handling of foreign corporate structures is assessed to represent a vulnerability with regard to the possibility of identifying beneficial owners.

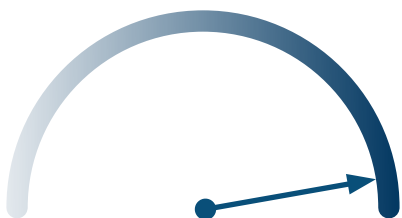
CTA also assesses that the level of the terrorist threat to the Faroe Islands is minimal. CTA assesses that violent extremism is less widespread in the Faroe Islands. Extremist propaganda may influence individuals in the Faroe Islands, or individuals travelling there, to commit acts of violence. This may be triggered by specific political issues such as animal welfare. Socially marginalized or vulnerable young people may be particularly susceptible to radicalization.

As was the case with Greenland, PET has mapped out the vulnerabilities of the Faroe Islands in cooperation with the Danish FIU. Reference is made to the national risk assessment of the Danish FIU, which thoroughly describes the Faroe Islands. As regards terrorist financing, the vulnerabilities relating to correspondent banks, the control level of Skráseting Føroya (which is in charge of the Faroese companies register etc.), beneficial owners and the delayed implementation of the Danish Anti-Money Laundering Act are particularly relevant and should be taken into consideration by both the authorities and the obliged entities. These vulnerabilities contribute to rendering terrorist financing possible, but because the threat level is minimal, the overall terrorist financing risk is **low**. ■

# Cryptoassets

## Summary

PET assesses that there is a **high** risk that cryptoassets are used for terrorist financing. Cryptoassets are an attractive means of terrorist financing as there is a demand for transactions that may be carried out swiftly without any geographical limitations. Further, privacy enhancing mechanisms and differing global regulation and control are significant terrorist financing vulnerabilities<sup>17</sup>.



PET assesses that Danish networks wanting to finance terrorism are interested in cryptoassets. The risk that cryptoassets will be used for terrorist financing has picked up since the most recent national risk assessment of terrorist financing in Denmark, and the threat has manifested itself in the form of specific interest and use. CTA assesses that Islamic State will increasingly attempt to use cryptoassets for attracting donations<sup>18</sup>.

Terrorist financing via cryptoassets poses a high terrorist financing risk, as they may be used for storing values, transferring values to recipients abroad and for specific use in terror-related activities<sup>19</sup>. It has also been possible to speculate in the fluctuating rate of exchange of cryptoassets leading to financial gains - or losses.

Terrorist financing via cryptoassets is attractive as the transactions can be made swiftly and across borders, as they are peer-to-peer transactions that are independent of the geographical locations of the users, and no correspondent banks are required.

A number of international examples confirm that terrorist groups such as Islamic State and al-Qaeda are able to

**17)** *The European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, pages 95-97.*

**18)** *CTA (2023): Assessment of the Terrorist Threat to Denmark, page 15.*


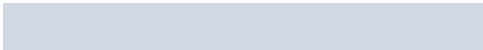
**19)** *See also Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism), page 80.*



receive transfers of cryptoassets. For instance, cryptocurrency exchange services have started business in the north-western part of Syria, and in addition to their legitimate purposes they are used for channelling funds to terrorist groups. In August 2020, the US Department of Justice identified the exchange service "BitcoinTransfer" in Idlib as a party in terrorist financing cases<sup>20</sup>.

It is of importance to the terrorist financing risk whether the users hold the private keys to their wallets (non-custodial wallets), or whether a third party has custody of the keys on behalf of the users (custodial wallets). The risk is higher when the users have the keys to their wallets (non-custodial wallets), as they are thus their own bank. The providers of custodial wallets in Denmark are subject to the Danish Anti-Money Laundering Act.

There is an important link between cryptoassets and the nonprofit sector. Cryptoassets increasingly enable terrorists and terrorist groups to carry out fundraising and crowdfunding fraud<sup>21</sup>, while maintaining high velocity and a certain degree of anonymity for donors and beneficiaries.



Internationally, there have been indications of a shift away from traditional money service businesses to cryptoassets since 2020, and this trend intensified in 2021. In EU member states, there have been cases concerning terrorist financing for users outside the EU by way of prepaid crypto vouchers of a value ranging from EUR 50 to EUR 250<sup>22</sup>.

Cryptoassets are also of importance to banks and payment service providers. A number of cryptoasset exchanges offer their users a debit card, for instance, via Visa or Mastercard, by which the users can make ordinary purchases in recognized currencies such as Danish kroner or US dollars.

The traceability of terrorist financing via cryptoassets varies depending on the transaction method. In general, traceability is high when the transaction is recorded on the blockchain (on-chain transactions) and is thus documented and implemented digitally. Blockchain is the technology underlying cryptoassets such as Bitcoin. Blockchain may be described as a "joint register" in which transactions in cryptoassets between accounts

---

**20)** *Chainalysis (2020): Chainalysis Intelligence Brief: How Syria-based Cryptocurrency Exchange BitcoinTransfer Facilitated Terror Financing Campaigns.*

**21)** *See also the European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, pages 54-57.*

**22)** *Europol (2022): Terrorism Situation and Trend Report (TE-SAT), page 19.*

linked to the blockchain are registered<sup>23</sup>. Conversely, traceability is low when the transaction takes place outside the blockchain (off-chain transactions), meaning that the transaction is not carried out or documented digitally, but is simply an agreement between two users. For instance, user A may transfer their wallet to user B by passing on their secret passwords. Thus, the terrorist financing threat is higher for off-chain transactions between two users than for on-chain transactions.

Mixers may also impact traceability. Mixers are financial service providers that cover up blockchain transactions by mixing, say, different cryptocurrencies.

It is a significant vulnerability that investigations into suspicious cryptoasset transactions require specialist competences and the potential exchange of information between national and international authorities and companies. This affects the risk of being detected and makes cryptoassets attractive for storage, transport and purchases. If an individual wanting to finance terrorism exchanges cryptocurrency into fiat currency, it will be attractive for this individual to choose a crypto exchange service in a country where the control level of the authorities is low. This is an important focus point.

It is a vulnerability that technological developments within cryptoassets happen fast and call for new regulation. An

example in point is privacy coins, which have become attractive to criminals due to the strong focus on encryption and anonymity. The cryptoasset Monero is an example of a privacy coin. Monero was introduced as a cryptoasset in 2014, and it was not withdrawn from the British cryptocurrency exchange service Kraken until 2021.

Globally, the financial regulation of cryptoassets has been weak since the introduction of the technology. The implementation in Denmark of the 5th EU Anti-Money Laundering Directive (AMLD V)<sup>24</sup> on 10 January 2020 was the first legislative step subjecting providers of exchange into cryptoassets and virtual wallets to a duty to notify under the Danish Anti-Money Laundering Act.

The Danish Financial Supervisory Authority exercises money laundering and terrorist financing supervision of providers of virtual wallets and currency exchange, but these businesses are still not subject to financial supervision by the Danish authorities, and the same applies to currency exchange services. However, this will change when the new EU Markets in Crypto-Assets Regulation (MiCA) has been implemented. This will enable the Danish Financial Supervisory Authority to perform financial supervision of providers of virtual wallets and exchange into cryptoassets. ■

---

**23)** Danish Financial Supervisory Authority (2022): *Blockchain technology may provide efficient infrastructure for payment service providers (Blockchain-teknologi kan udgøre en effektiv infrastruktur til betalingstjenester)*, page 2.

**24)** ACT no. 553 of 07.05.2019.

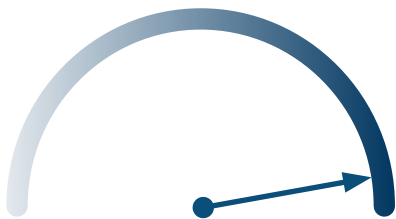


# 08

## The nonprofit sector

### Summary

PET assesses that the risk of terrorist financing is **high** within the nonprofit sector. The reason is PET's assessment that there are networks in Denmark with the capability and will to procure funds through, for instance, fundraising in support of terrorist organizations or terror-like activities. Further, there are a number of vulnerabilities within the nonprofit sector that make it attractive especially for the procurement of funds, but also for the transfer of funds.



This risk area covers the entire nonprofit sector, ranging from associations, nonprofit foundations and fundraising. Both associations and nonprofit foundations are organizations that may be used for terrorist financing<sup>25</sup>.


PET assesses that there is generally a high terrorist financing risk within the nonprofit sector and that this risk is particularly linked to the procurement of funds via fundraising or donations. PET assesses that the COVID-19 restrictions coupled with digital developments in recent years may have increased online fundraising in place of physical ones.

PET assesses that the nonprofit sector enables terrorist financing by way of raising both small amounts for specific purposes and more substantial and permanent funding for general purposes, channelled to terrorist organizations. Terrorist groups may benefit from donors, but it is also a vulnerable financing model for a terrorist organization if it depends on external funding only<sup>26</sup>. PET assesses that it is likely that terrorist organizations will increasingly use the nonprofit sector for launching modest fundraising for specific purposes rather than as a general source of financing their organizations.

In April 2020, PET published a separate risk assessment of terrorist financing within the nonprofit sector in Denmark, which largely remains up to date.

**25)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 04.7 concerning limited control of non-commercial funds.*

**26)** *Davis, Jessica (2021): Illicit Money: Financing Terrorism in the 21st Century, page 13.*



In October 2022, the Danish Financial Supervisory Authority published guidelines for companies governed by the Danish Anti-Money Laundering Act about how to assess associations with regard to the risk of money laundering and terrorist financing<sup>27</sup>. Both publications are key to the understanding of the risk factors relating to the nonprofit sector.

As appears from the risk assessment of the nonprofit sector, the risk posed by associations – and nonprofit foundations – may take various forms<sup>28</sup>. An organization may have been established with a view to financing terrorism, either with or without the knowledge and acceptance of the members and donors. Or an organization may have been established and be run for a legitimate purpose, often relief aid, but also with a concurrent illegal purpose where the funds or items of the organization are channelled to terrorist groups. In these cases, the funds channelled to illegal purposes will often be separated from other funds outside Denmark's borders, and the entire organization will not necessarily be aware of it. Finally, there may be a risk of terrorist financing through negligence in cases where an otherwise well-intentioned and well-run foundation or association cooperates with individuals or organizations that prove to be criminals<sup>29</sup>. The latter situation emphasizes that organizations in

Denmark must have a strong focus on assessing and controlling their local business partners.

The risk profiles of associations and nonprofit foundations differ significantly, and all obliged entities should be aware of this fact. In this connection, PET refers to the guidelines of the Danish Financial Supervisory Authority for companies governed by the Danish Anti-Money Laundering Act about how to assess associations with regard to the risk of money laundering and terrorist financing. The same guidelines are also generally relevant for the risk assessment of nonprofit foundations. It is important that obliged entities carry out a risk-based assessment to avoid that all associations are treated equally. Associations such as owners' associations, antenna associations and nonprofit housing associations generally pose a limited risk because their purpose is narrowly defined. At the other end of the risk scale, we see associations that have not been registered, have numerous cash activities and activities in conflict zones, etc.

As regards associations and nonprofit foundations with an elevated risk, obliged entities with a duty to notify should focus on any unusual organizational structures with actors such as independent private schools, mosques or sole proprietorships.

- 
- 27)** *The Danish Financial Supervisory Authority (2022): Vejledning til virksomheder omfattet af hvidvaskloven til vurdering af foreninger i forhold til risikoen for hvidvask og terrorfinansiering (guidelines to companies governed by the Danish Anti-Money Laundering Act on how to assess associations with regard to the risk of money laundering and terrorist financing). Finanstilsynet.dk.*
- 28)** *PET (2020): National risikovurdering af terrorfinansiering på NPO-området i Danmark (national risk assessment of terrorist financing within the NPO area in Denmark), page 14.*
- 29)** *The European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 239.*

International attention is increasingly directed at the consequences of the anti-money laundering standards, and exclusion of high-risk customers is an example in point (de-risking). An association or a foundation may represent a high risk for fully legitimate reasons, and it is a vulnerability that such customers risk being excluded from ordinary financial markets<sup>30</sup>.

Legitimate financial channels may be especially difficult to find in conflict zones and surrounding areas, which may tempt for instance Danish relief organizations to use methods such as hawala<sup>31</sup> and cash transports, which are characterized by a higher risk and a slim possibility of supervision and control.

Fundraising may take place in associations or nonprofit foundations, but also outside such organizations, and therefore this theme has been described separately in this publication. Fundraising is a classical way of procuring funds or items of value among extremist support networks in Denmark. Overall, a distinction should be made between fundraising with and without the authorization of the Danish fundraising board (Indsamlingsnævnet). Most fundraising methods require such authorization, but a number of exceptions are listed on the website of the fundraising board. The fundraising board, which reports to the Department of Civil Affairs, authorizes fundraising activities and oversees that the funds are applied for the purpose stated by the fundraiser. In this connection it is of utmost importance that the Department of Civil Affairs is able to collect the data required for controlling the fundraiser's information.

In cases involving fundraising, obliged entities should examine whether the fundraising activities have been authorized or have been exempted. The website of the Department of Civil Affairs lists recognized fundraising

activities<sup>32</sup>. Authorized fundraising activities are no guarantee that the funds are raised for legitimate purposes, and obliged entities should focus on the transfer and application of the funds, including whether the fundraising activities are a natural activity of the applicant and whether they are proportional to the purpose. For instance, there is an elevated risk if there is no transparency in the fundraising documentation, or if only some of the funds raised are passed to the documented recipients in or near conflict zones.

A recurring focus point in money laundering notifications involving suspected terrorist financing is behaviour resembling fundraising without authorization. This may happen where payments are made via the MobilePay payments application or in cash in a non-commercial context to accounts belonging to, say, an association, a private individual or a sole proprietorship. Unauthorized fundraising activities attract the attention of the authorities, and behaviour resembling fundraising should prompt further investigation.

Digital platforms account for a significant part of fundraising activities and have improved the opportunity to raise funds within a larger area at lower costs. But the implication is that the distance between the donor and the beneficiary may be large, and that the donor may have a very poor basis for making an informed decision on the donation and for controlling the application of the donation. The Norwegian authorities have also described how a number of known foreign and Norwegian extremist organizations and communities request financial support on social media<sup>33</sup>. Obligated entities are recommended to maintain a focus on fundraising authorizations, transparency and documentation regardless of the type of fundraising. ■

---

**30)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 04.6 and the European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 239.*

**31)** *See figure on page 37.*

**32)** *Godkendte indsamlinger (Authorized fundraising) (civilstyrelsen.dk)*

**33)** *Politiet/Politiets Sikkerhedstjeneste (2020): Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism), page 60.*





# 09

## Cash and high value goods

### Summary

PET assesses that the risk that cash and high value goods are used for terrorist financing is **high**. Cash and high value goods are attractive in several stages of terrorist financing, and the means of payment are characterized by a low risk of detection and low costs.





This chapter should be read in conjunction with similar chapters in National Risikovurdering af Hvidvask (national risk assessment of money laundering) published by the Danish FIU. It is recommended to read the chapter "Cash-related products" in the most recent risk assessment of the European Commission<sup>34</sup>.

Cash is still an obvious choice in all stages of terrorist financing. As to procurement, cash may be raised, stolen or earned both legally and illegally, and it may be exchanged into foreign currencies such as US dollars and euros. Banks and currency exchanges<sup>35</sup> should sharpen their focus on the exchange of Danish cash into US dollars and euros as regards the origin of the funds, the appearance and explanation of the customers as well as general customer due diligence. In relation to cash and high value goods, the risk of detection as well as the costs are assessed to be low. These aspects significantly increase the attractiveness of this area for terrorist financing.

The exchange of currency poses a risk of terrorist financing, as it covers up the origin of the funds and may enable the transport or transfer of the funds to another country. PET assesses that currency exchanges have a high inherent risk of money laundering and terrorist financing, and that this risk can only be higher in case of unregistered and thus illegal currency activities that are not supervised<sup>36</sup>.

- 
- 34)** *The European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 6.*
- 35)** *The Swedish authorities have a number of relevant observations about currency exchange in their most recent national risk assessment, The Swedish Police Authority (2021): National risk assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021, pages 71-77.*
- 36)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 06.11 on currency exchange activities.*



With respect to the storage of cash for terrorist financing, theft or detection poses a risk to criminals, which may be an incentive for them to keep the time of storage before the transfer relatively short. PET assesses that physical storage of cash does not constitute any practical challenge, as the amounts in terrorist financing are fairly modest. However, storage may be a practical challenge if a money launderer has to store many millions in cash – especially if the notes are not new. To illustrate this challenge, it should be noted that one million Danish kroner in new DKK 100 notes takes up slightly more space than an ordinary package of A4 printing paper and weighs almost 10 kg.

The transfer of cash poses a particular risk of terrorist financing. Cash can relatively easily be smuggled by hiding it on the body, in the luggage or other items on the journey. EUR 20,000 takes up about as much space as two mobile phones if they have been exchanged into new EUR 200 notes. This increases the possibility of smuggling for instance in connection with flights. The Danish customs authorities and the police should continue to focus on attempts at smuggling cash. The same applies to the origin and ownership of declared amounts.

Cash transports are also an attractive means of transferring funds to conflict zones, as it is often difficult to trans-

fer funds via a bank. Relief workers may also find it difficult to transfer funds to partners in or near conflict zones, and therefore they may use cash transports or a combined solution where funds are transferred electronically to for instance Türkiye or Lebanon, where they are withdrawn and transported in cash to the final destination. The obvious advantage of using cash is that it cannot be traced upon purchase. This is especially attractive in connection with attack financing in order to avoid monitoring of transactions and leaving a digital trail.

According to the national risk assessment of money laundering by the Danish FIU, the number of Danes using cash is declining<sup>37</sup>. However, PET assesses that cash will be increasingly attractive for terrorist financing, especially in connection with transfers to foreign countries.

High value goods have high risk potential because significant values may be easily hidden<sup>38</sup>. PET assesses that it will be particularly attractive to transfer funds by way of precious metals. For instance, a matchbox can almost hold one kg of 24 carat gold at a value of more than DKK 400,000. High value goods are also relevant for storing funds, but there is a risk of loss in value, detection or theft. ■

---

**37)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 02.2.*

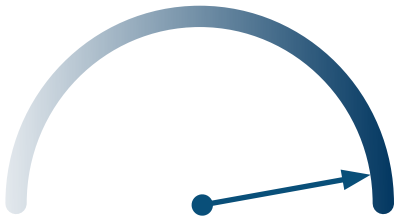
**38)** *The area is also covered by the European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, pages 164-170.*

# 10

## Illegal value transfer systems

### Summary

PET assesses that the risk of terrorist financing via illegal value transfer systems is **high**. Illegal value transfer systems are one of the few options to get money into conflict zones. The area holds a number of important vulnerabilities, as the money transfers are characterized by low costs, a high degree of anonymity, no registration and no possibility of supervision and regulation.



The risk area may be divided into two categories: “Illegal commercial transfers of funds via bank accounts” and “hawala”. Illegal commercial transfers of funds via bank accounts are characterized by an actor who uses the banking system to transfer funds on behalf of others against consideration without having been authorized by the Danish Financial Supervisory Authority. Generally, a specific account is used for transactions out of Denmark, and the funds are deposited in cash or are transferred from other accounts with Danish banks. The funds deposited into the account are aggregated into larger amounts in order to make one large transfer to a foreign country. The specific account may be linked to an association, a sole proprietorship or a private individual. The rationale for using the illegal method is to benefit from the often lower fee on a large aggregated transfer compared with many small transfers. Another advantage is that

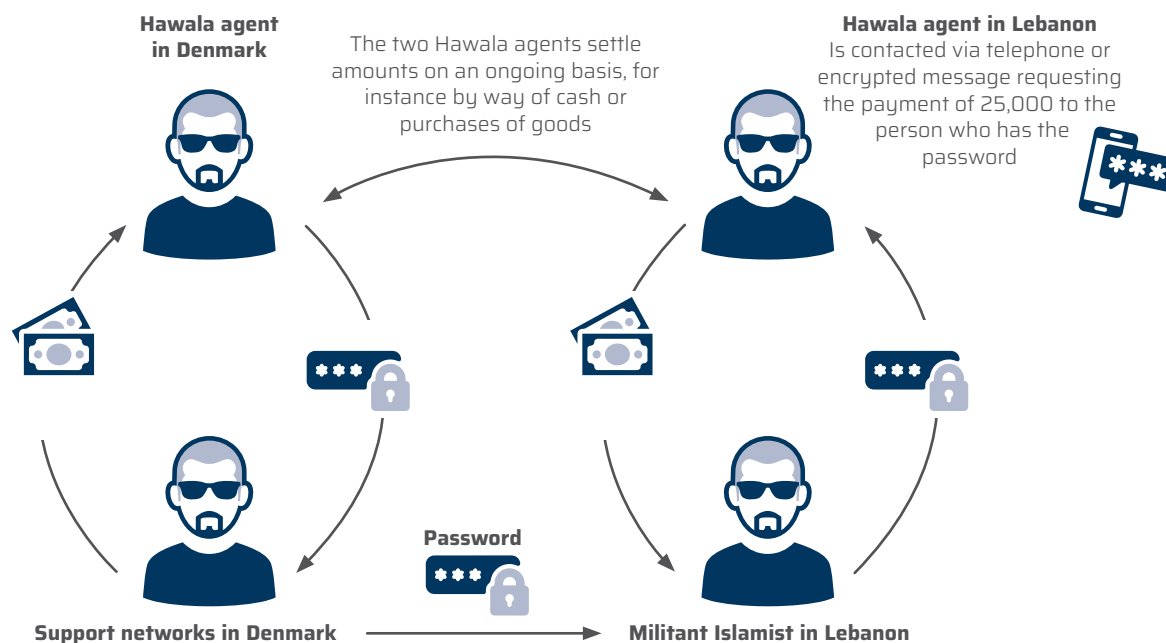
customer anonymity is higher because there are no established customer due diligence procedures and little chance of detecting the identity of the true customer. The method is based on the customers’ confidence that the actor will carry out the requested transactions.

In general, illegal value transfer systems are characterized by the absence of supervisory authorities that oversee compliance with the Danish Anti-Money Laundering Act. PET assesses that the low costs and the high degree of anonymity render unauthorized value transfer systems attractive for terrorist financing. This assessment is based on the fact that terrorist financing often involves smaller amounts than money laundering, which reduces the risk of detection.

The risk of detection mainly derives from banks’ monitoring of customers and transactions. In this connection, more focus should be placed on the behaviour described above, where amounts are aggregated to make one large transfer to a foreign country.

Illegal value transfers via hawala involve a significant element of trust, as there is often no documentation for the transfer of funds. The system exists in a number of versions, but a simple explanation is that a customer contacts a hawaladar (provider of hawala services) in their own country and passes on the amount to be transferred. A fee and a password for the release of the funds are agreed, and the amount is released by another hawaladar in the country where the funds are to be disbursed. Then the customer sends the password to the recipient, for instance via encrypted communication technology, while the hawaladar does the same to their colleague in the receiving country.

## EXAMPLE OF A HAWALA TRANSFER



The recipient contacts the hawaladar in the receiving country, provides the password and receives the funds. No funds are moved by the transfer, but a debt is created between the two hawaladars. This debt will generally vary over time, and it may be settled at physical meetings or via payment in gold, in goods with over/under-invoicing or in cash, wholly independently of the customer.

The implication of the method is no control by supervisory and other authorities, which impedes detection. Thus, there is a considerable risk of terrorist financing as the high degree of anonymity, the low risk of detection and moderate costs are attractive.

Illegal value transfer systems generally pose a high risk of terrorist financing<sup>39</sup>. The area is characterized by a sig-

nificant degree of anonymity, low costs and weak detection mechanisms.

PET assesses that illegal value transfer systems may be used by groups linked to Syria, Lebanon and Somalia. The threat relating to terrorist financing is high for these areas as the transfers are made across borders, the detection risk is low, and this method is one of the few channels that may bring funds into conflict zones.

Both law enforcement and supervisory authorities should look for potential hawala transactions when performing their duties. Hawala transactions are often seen together with other commercial activities relating to convenience stores, registered money service businesses, currency exchanges, etc.<sup>40-41</sup> ■

**39)** This also applies to Norway where the risk is particularly high. Politiet/Politiets Sikkerhedstjeneste (2020): *Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism)*, page 59.

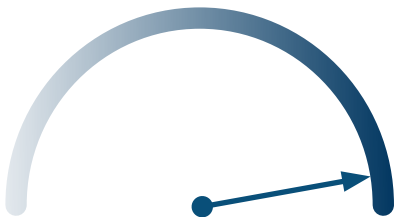
**40)** The Swedish national risk assessment also focuses on hawala as a risk area. It points out that in certain geographical regions, hawala may be the only way of transferring funds. The Swedish Police Authority (2021): *National risk assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021*, page 102.

**41)** See also the chapter "Illegal transfers of funds - Hawala" in the European Commission (2022): *Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, pages 81-85.

# Authorized money service businesses

## Summary

PET assesses that there is a high risk that authorized money service businesses are being abused for terrorist financing. The risk of terrorist financing is **high** because money service businesses are typically able to move funds closer to conflict zones and at lower cost than banks. Moreover, operators have difficulties distinguishing between criminal and legitimate customers and transactions, and the lower detection risk and failure to comply with rules increase the risk.




The risk area covers remittance through authorized money service businesses providing payments between individuals or businesses without creating an account in the name of the payer or the payee.

Money service businesses may be businesses which have remittance as their core service, or businesses which act as agents for major foreign money service businesses in connection with trade related to convenience stores or grocery stores.

Money service businesses are subject to supervision by the Danish Financial Supervisory Authority and to the obligations stipulated in the Danish Anti-Money Laundering Act. When money service businesses actively comply with the Anti-Money Laundering Act, including by applying customer due diligence measures and transaction monitoring, the risk of terrorist financing is lower.

For individuals who want to move funds out of Denmark, money service businesses offer an attractive alternative to banks because the costs are often lower, the transfer can be made faster and the requirements for customer affiliation are less strict. For example, refugees, immigrants or people staying in Denmark due to their work may find money service businesses to be an attractive option. Furthermore, money service businesses in many developing countries may be in a better position than the local banking sector to make funds available because they have a larger office representation.



Identifying a transfer related to financing terrorism places high demands on the controls performed by the money service business because numerous legitimate customer transactions of a similar size or with a similar destination may be conducted at the same time.

PET assesses that there is a significant risk that customer due diligence and other anti-money laundering measures are inadequate. This applies particularly to agents for which remittance is a secondary area of business<sup>42</sup>, and it enables the use of frontmen to carry out transactions through a money transfer provider.

The failure by many money service businesses to comply with the rules combined with the low risk of detection and the low costs<sup>43</sup> make money service businesses an attractive option for individuals who want to finance terrorism.

PET's assessment of money service businesses is in line with international assessments. In its Terrorism Situation and Trend Report 2022, Europol states that:

*"Jihadist actors commonly use money transfer services, such as MoneyGram and Western Union, or informal value transfer systems (IVTS), such as hawala".<sup>44</sup>* ■

---

**42)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 06.05 on payment services, and Norwegian Police/Norwegian Police Security Service (2022): Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism), page 78.*

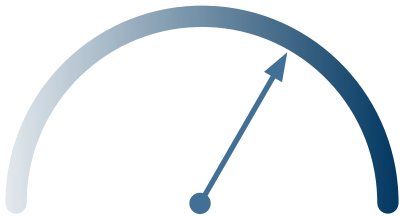
**43)** *The Norwegian authorities take the same view in their most recent national risk assessment (Norwegian Police/Norwegian Police Security Service 2022: Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering, page 6).*

**44)** *Europol (2022): Terrorism Situation and Trend Report (TE-SAT), page 18. See also the European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 76.*

# The banking sector

## Summary

PET assesses that there is a **significant** risk of terrorist financing in relation to the banking sector. Banking services are easily accessible and can be used at all stages of terrorist financing. Most banks have integrated a number of mitigating actions and invested in technical as well as human resources to mitigate risk.



Banks offer financial services targeting private as well as business customers, including associations and foundations. According to the good practice rules of the Danish Act on Payment Accounts, all consumers are entitled to have a basic deposit account at a bank.

In 2022, there were 89 banks altogether in the Danish Realm. Of these, 55 were located in Denmark, four were in the Faroe Islands and one was in Greenland, while the remaining 29 banks were branches of foreign banks with representations in the Danish Realm.

The Danish banking sector is generally characterized by a high concentration, which means that a few banks cover most of the market for financial products and services. The two largest Danish banks have a market share of 60%, and the four largest Danish banks have a combined market share of 88%<sup>45</sup>.

Banks can be used at all stages of terrorist financing. As they provide credit, banks can be used to procure funds, and a potential terrorist can keep money in a bank account, transfer money to other individuals or businesses and ensure payment of goods and services.

Furthermore, banks are characterized by high accessibility, and using them for terrorist financing requires no special knowledge or expertise. It is easy to open a bank account, and with online banking services available 24/7, instant transfers can conveniently be made between accounts and banks. Furthermore, banks offer access to international transactions via their correspondent banks.<sup>46</sup>

<sup>45</sup>) *Copenhagen Economics (2021): Konkurrencen i den danske banksektor (competition in the Danish banking sector)*

<sup>46</sup>) *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 06.1 on banks.*





The European Banking Authority (EBA) reports that 70% of European supervisory authorities find that there is a significant or very significant risk of money laundering and terrorist financing in the sector of payment institutions. Various factors account for the significant money laundering and terrorist financing risk in the payment institutions sector, including the cash-intensive nature of the services offered, the prevalence of occasional and sporadic transfers rather than regular transfers, the absence of established business relationships, the high speed of transactions, and the use of new technologies to facilitate on-line onboarding of customers<sup>47</sup>. EBA also notes that the institutions have a gatekeeper role in relation to money and customers entering the financial system<sup>48</sup>.

However, the terrorist financing risk varies across banks, as it depends on the banks' business models and customer segments as well as on the markets and financial products and services offered. Overall, the risk may be assessed in terms of the two major categories of bank customers: private customers and business customers. Subsequently, the risk may be broken down according to the products offered to each of the two customer groups.

The terrorist financing risk associated with financial services offered to private customers, such as the granting

of consumer credit and issuance of payment cards, is high. The reason for the high exposure of the banking sector is the very large volume of customers, and the fact that even by making small amounts available, banks are at risk of being abused for money laundering. The risk of asset-based loans is assessed to be lower than the risk of cash loans as asset-based loans typically involve a re-sale option, which makes them less attractive.

Cash withdrawals and the use of ATMs are among the services involving the highest risk of exposure for banks. According to the most recent supranational risk assessment from the European Commission, terrorist groups often place funds in deposit accounts with terrorist financing in mind. However, as is also stated in the European Commission report, it requires knowledge and planning to make the funds appear legitimate. In conflict zones, cash withdrawals through ATMs may be complicated by a slow or disrupted underlying payment infrastructure<sup>49</sup>.

It is difficult to remain anonymous at a bank, and this partly reduces the attractiveness for private individuals of using banks for terrorist financing. However, individuals involved in terrorist financing may obtain partial anonymity by using frontmen.

---

**47)** *European Banking Authority (2021): Opinion of the European Banking Authority on the risks of money laundering and the terrorist financing affecting the European Union's financial sector, page 34.*

**48)** *European Banking Authority (2021): Opinion of the European Banking Authority on the risks of money laundering and the terrorist financing affecting the European Union's financial sector, page 11 and pages 26-32.*

**49)** *European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 38.*

Historically, there have been examples of relatives, in particular, acting as frontmen for militant extremists.

When banks (or payment institutions or e-money institutions) have no face-to-face contact with their customers, for example in the case of online onboarding, this places high demands on their customer due diligence measures as these play an important role in preventing terrorist financing. Actors who have no interaction with customers are less able to form an impression of the customer and are forced to rely more on transaction monitoring. The fact that non-Danish actors are often involved adds further to the distance between the customer, the financial company and society.

In its national risk assessment of money laundering, the Danish FIU notes an increase in the number of multi-bank customers, i.e. private individuals or businesses that are customers of multiple banks<sup>50</sup>. This trend makes it more difficult for the primary bank as well as the secondary banks to detect any suspicious activities because none of the banks are able to assess the full range of a customer's activities.

One of the reasons for the multi-bank trend is that bank customers have been forced to pay negative interest, leading them to spread their savings across several banks. However, spreading one's transactions can also be an attractive option for criminal actors. A risky customer using, for example, five different banks may not necessarily appear risky for the individual bank. All else being equal, this means that the individual bank does not get the full financial picture, and, overall, this increases the risk for the banks involved<sup>51</sup>.

Multi-bank customers can use their different accounts to hide and disguise the existence and transit of funds transferred to cryptoasset markets, for example. If non-Danish financial companies are involved, it becomes more difficult and time-consuming for Danish authorities to obtain relevant information and to assess the scope and nature of suspicious factors.

The terrorist financing risk in relation to business customers is moderate. The European Commission's Supranational Risk Assessment Report 2022 mentions in relation to business customers and institutional investments that various risk factors such as products, customers, geography and service channels make the services unattractive for terrorists. In many cases, people who want to engage in terrorist financing do not have the expertise required to get access to the sector.

The primary risk of terrorist financing in relation to business customers concerns small businesses, commercial foundations or associations. The risk can be linked to fundraising, donations, revenue from sole proprietorships or similar. See the chapter on the nonprofit sector for further details. The risk may also relate to transfers via Danish or foreign payment service providers or cryptocurrency exchanges. Identifying suspicious activities may be extremely difficult, and focus should therefore be on indications of conflict zone involvement, criminal activity or affiliation with extremist communities, or on actors who may give rise to terrorist financing suspicion.

Asset management, including investment advice, for both business and private customers is an area assessed by PET to be associated with a low terrorist financing

---

**50)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 06.1.*

**51)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 06.5.*

risk. Asset management is a service targeting wealthy customers who wish to generate a long-term return on their assets. PET sees no indications that assets managed by banks or on the basis of investment advice have been used for terrorist financing.

To counter the inherent terrorist financing risk, banks have generally integrated mitigating actions into their business procedures, and they have invested in transaction monitoring and human resources. PET assesses that these efforts have reduced the threat related to terrorist financing because individuals who wish to engage in such activity are often aware of the control measures and customer due diligence procedures adopted by banks. The higher risk of detection that these measures and procedures entail may discourage the use of services offered by banks.

Banks are generally characterized by a considerable risk awareness in relation to terrorist financing, but at the same time, they face a difficult task when it comes to translating risk awareness into concrete risk-reducing measures, for example by calibrating transaction monitoring to ensure detection of relevant transactions.

According to the European Commission's Supranational Risk Assessment Report, banks tend to handle the terrorist financing risk in the same way that they handle the risk of money laundering<sup>52</sup>. PET assesses that this vulnerability is also present in a Danish context, as we have seen examples of banks failing to differentiate adequately between the two different types of risk, although the differences between them may be substantial as is also reflected in the two national risk assess-

ments of money laundering and terrorist financing, respectively.

Another vulnerability in relation to terrorist financing is that banks are not allowed to share adequate information about their customers with other banks. Consequently, if a bank refuses to carry out a transaction or asks critical questions about a customer's request to transfer funds to a high-risk country, the customer may turn to another bank, which has no knowledge about the customer's history. In its 2021 status report on anti-money laundering measures, Finance Denmark states that:

*"Banks are only able to see what is happening in their own business. This means that individual banks may not be able to see that transactions form part of a larger network involving numerous banks, and consequently, it may not be clear to the bank that a transaction is suspicious."<sup>53</sup>*

Previously, banks accounted for a considerable share of all financial transactions, but today, providers of financial services also include payment service providers and e-money institutions, which also carry out or initiate transactions. This makes it more difficult for the individual bank to gain a full picture of their customers' behaviour. Although this trend may benefit the individual customer, it complicates banks' monitoring of their customers' activities. There is nothing to suggest that this fragmentation trend will decrease going forward. ■

---

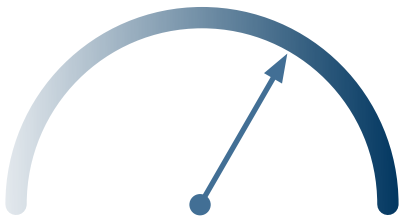
**52)** European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 39.

**53)** Finance Denmark (2021): Hvidvaskindsats, Status 2021 (2021 status on anti-money laundering measures), page 13.

## Terrorist financing based on organized economic crime

### Summary

PET assesses that the risk of terrorist financing based on proceeds from economic crime is **significant**. The reason is that there may be extremist sympathies in criminal networks and that some of the barriers to terrorist financing have already been overcome as economic crime by professionals contains elements of anonymity and cross-border transactions, large amounts and the acceptance of financial costs.



Terrorist financing, in particular financing of organizations, may be related to general economic crime, especially tax and VAT fraud, which is a highly profitable area of crime. For more information on tax and VAT fraud, we refer to section 05.1 of the national risk assessment of money laundering published by the Danish FIU. Another reason why this area is relevant in relation to terrorist financing is that PET has identified a risk of criminal proceeds being channelled to terrorist groups in or near conflict zones.

An example of a modus operandi could be a criminal network in Denmark generating criminal proceeds, e.g. from fraudulent chains or VAT carousel fraud, and transferring these funds to recipients abroad. If the organizers behind the criminal activities have extremist sympathies, part of the criminal proceeds may end up in the hands of militant Islamist groups in the form of donations or religious indulgences. Identifying this form of terrorist financing can be extremely difficult for obliged entities as well as for public authorities because it involves criminal proceeds already concealed abroad and then chan-

nelled, in part, to terrorist groups. Thus, it is important that public authorities as well as obliged entities assess whether the person under suspicion could have links to known extremist groups.

We have seen examples of organized crime being committed via professional advisers, e.g. on tax, legal and accounting matters<sup>54</sup>. Denmark's 2022-2025 national strategy for combating money laundering and terrorist financing focuses, among other things, on this form of complex and organized crime, including the use of professional advisers and facilitators<sup>55</sup>. It is important that

both law enforcement authorities and supervisory authorities focus on identifying advisors who knowingly assist criminals. Moreover, lawyers, auditors and other professionals should give more attention to whether their advisory services are in fact to be used in criminal activities, for example to create a specific company or foundation structure<sup>56</sup>. With regard to terrorist financing, this could be relevant in relation to companies in or near conflict zones or the creation of unusual corporate structures when establishing mosques, independent private schools, foreign donations or nonprofit foundations. ■

---

**54)** *The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), page 110 on professional advisers.*

**55)** *The Danish Government (2022): National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025 (Denmark's 2022-2025 national strategy for combating money laundering and terrorist financing), page 13.*

**56)** *European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 187.*

DEN EUROPÆISKE UNION  
DANMARK

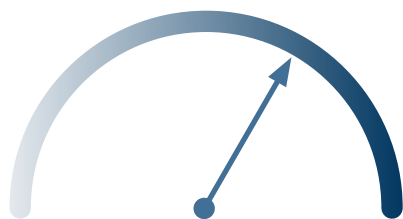


PAS

# Identity misuse and derived crime

## Summary

PET assesses that identity misuse and derived crime represent a **significant** risk of terrorist financing. This area is attractive for illegal procurement of funds, and the risk of detection may be reduced, because this type of crime may appear legal as true digital identities are used.



The risk area covers identity misuse and identity theft as well as derived property crime. Identity misuse is a general term covering offences involving the misuse of a (digital) identity for property crime. Most often, identity misuse takes place online as it would be considerably more risky to appear in person, e.g. at a bank. Identity misuse may involve theft or the fraudulent takeover of a digital identity, but also situations in which a person willingly hands over their identity to others, knowing that it will be used for criminal purposes<sup>57</sup>. The takeover typically gives access to the personal data, passport or driver's licence and MitID (an electronic personal identification system) of the person involved.

In relation to terrorist financing, identity misuse is mainly relevant for the procurement of funds or items. Misusing another person's identity offers a range of possibilities to commit economic crime. This includes purchasing goods without paying for them, trading on online sites such as second-hand websites, taking out consumer loans online and establishing businesses to evade tax and/or VAT.

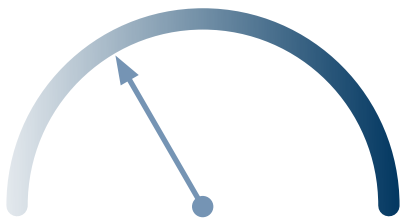
The risk associated with identity misuse places great demands on the customer due diligence and ongoing monitoring carried out by obliged entities, as activities may appear legitimate due to the use of a valid digital identity and identification. Identity misuse exploits a vulnerability in the data sharing between public authorities and private companies. For example, a business offering consumer loans may make a positive credit assessment based on a customer's digital identity, even though other data suggests that the loan application should be rejected. Similarly, if an identity wants to establish a company, and public data suggests that there is a considerable risk that the company will engage in criminal activity, this may not be detected. Overall, the higher the number of data sources available to public authorities and private companies when verifying an identity and assessing the risk of a certain behaviour, the lower the risk of criminal activity. ■

**57)** See also the European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, pages 107-110.

# Benefit fraud

## Summary

PET assesses that there is a **moderate** risk that benefit fraud may be used for terrorist financing. Benefit fraud is assessed to be attractive among individuals in extremist communities, but the considerable focus on the threat by the authorities as well as by obliged entities is assessed to mitigate the risk.






The risk area covers all forms of social security benefits knowingly claimed by a recipient with no entitlement. In terms of terrorist financing, benefit fraud can be divided into three categories: travelling to conflict zones while receiving benefits, travelling to other destinations while receiving benefits and benefit fraud in Denmark.

PET has seen examples of people travelling to conflict zones while still receiving benefits such as student grants and unemployment benefits. These cases received media attention, and PET informed the media that 39 incidents had been reported to the Danish Agency for Labour Market and Recruitment<sup>58</sup>. As mentioned previously, the number of foreign fighters has not increased since 2016, but the modus operandi of receiving social security benefits despite having travelled to conflict zones or other destinations should remain a focus area for obliged entities, especially if this trend returns.




PET assesses that the authorities as well as obliged entities have a strong focus on benefit fraud, also with regard to benefits paid to individuals who have travelled to destinations other than conflict zones. This could be neighbouring countries or countries near Syria, Iraq, Somalia, Lebanon, Afghanistan and Palestine. Typical characteristics of these cases include long-term stays outside Denmark, flight ticket purchases, no payment of fixed expenses in Denmark and considerable changes in finan-

**58)** Consultation at the Danish Parliament about foreign fighters receiving social security benefits (30 August 2018, FT.dk)





cial behaviour after leaving Denmark. Obligated entities are likely to experience uncertainty as to whether a suspicion concerns possible terrorist financing or ordinary benefit fraud/other criminal activity.



The former category includes benefit fraud in Denmark, with channelling of fraudulently obtained funds to individuals or groups involved in terrorism or terrorist-like activities. The funds may serve to finance attacks or organizations, with the former type of financing usually being linked to an individual, or a person or group close to an individual, to whom funds, items or services are provided for the purpose of carrying out an attack. Organizational financing may involve small transfers directly to individuals abroad, for example via a money service business to an intermediary in or near a conflict zone. Furthermore, funds may be transferred or donated in cash, intentionally or unintentionally, to associations, nonprofit foundations, fundraising collections or similar bodies supporting a terrorist organization<sup>59</sup>.

Overall, PET assesses that the collaborative effort and joint focus of the authorities on combating benefit fraud in relation to relevant communities, combined with the stronger focus of companies and individuals on reporting any suspicion of benefit fraud, reduce the risk of terrorist financing. ■

---

**59)** See also PET (2020): *National risikovurdering af terrorfinansiering på NPO-området i Danmark (national risk assessment of terrorist financing within the NPO area in Denmark)*, pages 13-14 on negligence.

# Other risk areas

## Repatriation benefits and return allowances

PET assesses that there is a **moderate** risk that repatriation benefits and return allowances may be used for terrorist financing. Repatriation refers to a person's voluntary return to their home country or previous country of residence with a view to settling there permanently. According to the Danish Repatriation Act, municipalities may provide support for repatriation, and if all members of a family receive repatriation benefits, the total amount may run to several hundred thousand Danish kroner. In some cases, the payment of repatriation benefits and return allowances has been complicated by the fact that Danish banks have not been able to transfer funds to countries such as Iran and Syria. Consequently, in April 2022, new rules were introduced on flexible payment of repatriation benefits or return allowances to Syria and Iran to ensure that the benefits could be paid in cash upon departure from Denmark. The rules apply to cases from 1 May 2022 or later. In the assessment of PET, this increases the risk of intentional or unintentional terrorist financing when in transit and upon arrival in countries in or near conflict zones, for example in the form of taxes or fees being collected in connection with screenings at border crossings. Generally, the higher the amount, the greater the risk.

When obliged entities investigate a terrorist financing suspicion, radicalization or violation of the repatriation

agreement should be considered possible indications of terrorist financing. Furthermore, the municipality deciding on payment of repatriation benefits etc. must obtain a statement from the police if there is reason to assume that the applicant intends to participate in activities abroad that could put national security at risk, or increase such risk - in Denmark or elsewhere - or that could pose a serious threat to public order.

## Leasing

PET assesses that there is a **low** risk that leasing activities are used for terrorist financing. Leasing remains a risk area with limited data available to assess the risk of terrorist financing. The risk associated with leasing relates primarily to procurement of funds through an illegal sale of a leased car and the use of the procured funds to support terrorist activities. There have also been cases where a leased car has been transported illegally to a conflict zone to be used in the conflict. The risk of this modus operandi has been reduced as the situation in Syria and Iraq is now characterized by considerably more isolated zones with very difficult access.

The vulnerabilities related to leasing primarily concern the possibilities of verifying and checking the customer's identity, ability to pay and right of residence.

### Art and spoils of war

PET assesses that there is a **low** risk that art and spoils of war in Denmark are used for terrorist financing. The risk area concerns terrorist financing through trade in works of art, antiquities and artefacts. In an FATF context, this area is referred to as AACO (Art, Antiquities and other Cultural Objects). PET divides the area into two categories.

The first category concerns the risk of funds being stored or transferred by means of high value works of art or similar items. More specifically, funds are invested in a work of art, which is then sold or otherwise disposed of close to the location at which the funds will be used for terrorist financing. Compared with other methods available, PET does not assess this method to be attractive for terrorist financing in a Danish context; neither for storing nor transferring money<sup>60</sup>. The Danish FIU notes that the

subjective valuation of art can render it difficult to assess whether the funds transferred in a given transaction exceed the actual value of the work of art traded<sup>61</sup>. However, PET assesses that the risk is limited in a Danish terrorist financing context.

The other category concerns the risk of sale of spoils of war, including works of art, jewellery, coins, etc., that have fallen into the hands of a terrorist group in connection with a specific conflict. An example of this is the looting by Islamic State in Syria and Iraq. Spoils of war can be moved out of the conflict zone and sold on the legal as well as the illegal art market, thereby serving as a method of procuring substantial funds. Items may be sold with or without certificates of origin, and the certificates may be false or they may have been issued by illegitimate actors, such as Islamic State. ■

---

**60)** See also the European Commission's risk assessment for "High value goods - artefacts and antiquities" in European Commission (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, page 153.

**61)** The Danish Financial Intelligence Unit (2022): Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering), section 06.13 on art.

# Empirical data and literature

## Empirical data

This risk assessment is widely based on the same empirical and methodological approach as the risk assessment from 2019.

As regards identification of financial vulnerabilities, the risk assessment has been prepared in close cooperation with the Danish FIU, as there is substantial overlap between the financial vulnerabilities related to money laundering and to terrorist financing. The Norwegian risk assessment of money laundering and terrorist financing from 2022 is based on a similar cooperation<sup>62</sup>.

PET's assessment of the terrorist financing risk takes a holistic perspective as recommended by the Financial Action Task Force (FATF)<sup>63</sup>. This means that qualitative as well as quantitative data from different sources make up the empirical basis of the terrorist financing risk assessment, and the origin of knowledge may be both national and international.

Investigations and criminal cases related to terrorist financing in a national as well as an international context constitute important qualitative data sources for understanding the modus operandi of terrorist financing.

However, investigations and criminal cases cannot be used to determine whether a certain aspect reflects a trend in terrorist financing, as individual cases are not necessarily representative. Knowledge about national terrorist financing investigations and criminal cases mainly originates from PET and the Danish police districts, whereas knowledge about international investigations and criminal cases has been gathered from FATF and Counter ISIS Finance Group (CIFG), among others. Furthermore, PET is part of a strong Scandinavian collaboration focusing on risk assessments and exchanging knowledge on terrorist financing.

PET has made quantitative analyses based on reports on terrorist financing suspicions from the Danish FIU and PET's subsequent processing of the reports. Other empirical sources include PET's collaboration with Danish authorities on involving companies and trade organizations in the identification of threats and financial vulnerabilities. Analyses and risk assessments from international organizations also form part of the empirical basis, including the European Commission's assessment of the risk of money laundering and terrorist financing as well as analyses and assessments by Europol. ■

**62)** *Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism), page 5.*

**63)** *FATF (2019): Terrorist Financing Risk Assessment Guidance 2019, page 20.*

## Literature

Centre for Terror Analysis (2023): *Assessment of the Terrorist Threat to Denmark*. PET.dk.

Chainalysis (2020): *Chainalysis Intelligence Brief: How Syria-based Cryptocurrency Exchange BitcoinTransfer Facilitated Terror Financing Campaigns*. Chainalysis.com.

Copenhagen Economics (2021): *Konkurrencen i den danske banksektor (competition in the Danish banking sector)*. Finansdanmark.dk.

Davis, Jessica (2021): *Illicit Money: Financing Terrorism in the 21st Century*, Lynne Rienner Publishers.

Davis, Jessica (2022): *New Technologies but Old Methods in Terrorism Financing*, The CRAFT Research Briefing Series 2020-2022.

The court of Roskilde, Denmark (2022): *Decision in the criminal case against three members of ASMLA*. Domstol.dk

European Banking Authority (2021): *Opinion of the European Banking Authority on the risks of money laundering and the terrorist financing affecting the European Union's financial sector*. Eba.europa.eu.

European Commission (2022): *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to crossborder activities*. Europa.eu.org. COM(2022) 554 final.

European Commission (2022): *Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*. Europa.eu.org. SWD(2022) 344 final.

Europol (2022): *Terrorism Situation and Trend Report (TE-SAT)*. Europol.europa.eu.

FATF (2019): *Terrorist Financing Risk Assessment Guidance*. FATF-GAFI.org.

Finance Denmark (2021): *Hvidvaskindsats, Status 2021 (2021 status on anti-money laundering measures)*. Finansdanmark.dk

The Danish Financial Supervisory Authority (2022): *Blockchain-teknologi kan udgøre en effektiv infrastruktur til betalingsstjenester (blockchain technology may provide efficient infrastructure for payment services)*. Finanstilsynet.dk

The Danish Financial Supervisory Authority (2022): *Vejledning til virksomheder omfattet af hvidvaskloven til vurdering af foreninger i forhold til risikoen for hvidvask og terrorfinansiering (guidelines for companies governed by the Danish Anti-Money Laundering Act about how to assess associations with regard to the risk of money laundering and terrorist financing)*. Finanstilsynet.dk.

The Danish Financial Intelligence Unit (2022): *Den Nationale Risikovurdering af Hvidvask (national risk assessment of money laundering)*. Anklagemyndigheden.dk.

PET (2020): *National risikovurdering af terrorfinansiering i Danmark 2019 (national risk assessment of terrorist financing in Denmark 2019)*. PET.dk.

PET (2020): *National risikovurdering af terrorfinansiering på NPO-området i Danmark (national risk assessment of terrorist financing within the NPO area in Denmark)*. PET.dk.

Politiet/Politets Sikkerhedstjeneste (2020): *Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism)*. PST.no.

Politiet/Politets Sikkerhedstjeneste (2022): *Nasjonal risikovurdering. Hvitvaskning og terrorfinansiering (national risk assessment of money laundering and financing of terrorism)*. PST.no.

The Danish Government (2022): *National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025 (Denmark's 2022-2025 national strategy for combatting money laundering and terrorist financing)*. Justitsministeriet.dk.

Reimer & Redhead (2022): *Bit by Bit - Impacts of New Technologies on Terrorism Financing Risks*. Project CRAFT, RUSI Occasional Paper, April 2022.

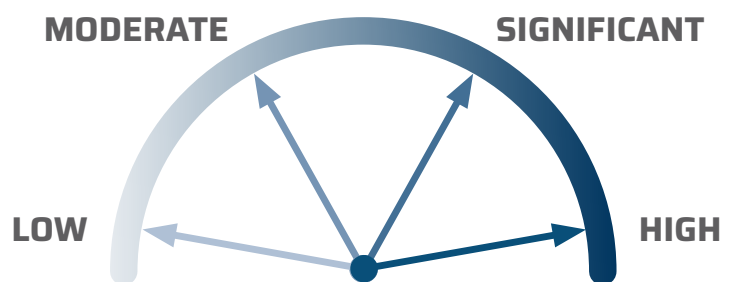
Consultation at the Danish Parliament about foreign fighters receiving social security benefits, 30 August 2018. FT.dk

The Swedish Police Authority (2021): *National risk assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021*. FI.se.

# Appendix 1

## Model for assessment of special risk areas

The model on the right, which appears in a similar version in the national risk assessment of money laundering published by the Danish FIU, is used to assess specific terrorist financing risk areas. Each of the areas is characterized by various services and means of payment posing various degrees of risk. The vulnerabilities related to these services and means of payment are at the core of the vulnerability analysis.



DANISH SECURITY AND INTELLIGENCE SERVICE  
NATIONAL RISK ASSESSMENT OF TERRORIST FINANCING  
YEAR OF PUBLICATION: 2024  
PHOTOS: ADOBE STOCK

		LIMITED RISK	MODERATE RISK	SIGNIFICANT RISK	HIGH RISK
THREAT	Scope	Services and means of payment etc. are only known to be used by a small group of people in extremist communities or are not known to be used at all.	Services and means of payment etc. are considered attractive for terrorist financing in extremist communities to a moderate degree.	Services and means of payment etc. are considered attractive for terrorist financing in extremist communities to a significant degree.	Services and means of payment etc. are considered attractive for terrorist financing in extremist communities to a high degree.
	Accessibility	Services and means of payment etc. are difficultly accessible and require considerable planning, knowledge and/or technical expertise.	Services and means of payment etc. are relatively accessible and require moderate planning, knowledge and/or technical expertise.	Services and means of payment etc. are accessible and require little or no planning, knowledge and/or technical expertise.	Services and means of payment etc. are easily accessible and require little or no planning, knowledge and/or technical expertise.
VULNERABILITY	Volume, transaction size and speed of transactions	<p>The total number of transactions is low.</p> <p>The provider is unsuitable for high-volume terrorist financing.</p> <p>The transactions are not executed at a fast pace.</p>	<p>The total number of transactions is moderate.</p> <p>The provider is moderately suitable for high-volume terrorist financing.</p> <p>The transactions are executed at a moderate pace.</p>	<p>The total number of transactions is significant.</p> <p>The provider is suitable for high-volume terrorist financing to a significant degree.</p> <p>The transactions are executed at a significant pace.</p>	<p>The total number of transactions is high.</p> <p>The provider is highly suitable for high-volume terrorist financing.</p> <p>The transactions are executed at a high pace.</p>
	The potential to move funds in and out of Denmark (cross-border transactions)	<p>Services and means of payment etc. provide limited scope for foreign transactions.</p> <p>Moving values in and out of Denmark is not easy.</p>	<p>Services and means of payment etc. provide moderate scope for foreign transactions.</p> <p>Moving values in and out of Denmark is moderately feasible.</p>	<p>Services and means of payment etc. provide significant scope for foreign transactions.</p> <p>Moving values in and out of Denmark is relatively easy.</p>	<p>Services and means of payment etc. provide extensive scope for foreign transactions.</p> <p>Moving values in and out of Denmark is easy.</p>
	Costs	<p>The costs associated with terrorist financing are high.</p> <p>Using services and means of payment for terrorist financing is expensive / the risk of losses is high.</p>	<p>The costs associated with terrorist financing are significant.</p> <p>Using services and means of payment for terrorist financing is relatively expensive / the risk of losses is significant.</p>	<p>The costs associated with terrorist financing are moderate.</p> <p>Using services and means of payment for terrorist financing is relatively inexpensive / the risk of losses is moderate.</p>	<p>The costs associated with terrorist financing are low.</p> <p>Using services and means of payment for terrorist financing is inexpensive, and/or the risk of losses is low.</p>
	Anonymity/probability of criminal activity being detected	Attempts at terrorist financing are likely to be detected.	Attempts at terrorist financing are less likely to be detected.	Attempts at terrorist financing are relatively difficult to detect.	Attempts at terrorist financing are difficult to detect.

