Money Laundering and Terrorist Financing – Tasks and Obligations of the Financial Sector in a Global System

Doctoral Dissertation

SWPS University of Social Sciences and Humanities
Faculty of Law

Submitted by

Carola Bader, LL.M.

November 15, 2023

Promoters: Prof. Dr. iur. Winfried Huck
Ostfalia University of Applied Sciences

Ph.D. Paweł Kowalski
SWPS University of Social Sciences and Humanities

List of Contents

List of Abbreviations

§(§)	Paragraph(s)
AFCA	Anti Financial Crime Alliance
AG	Aktiengesellschaft (Public Limited Company)
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLD	Anti-Money Laundering Directive
App	Application
Art.	Article
AWG	Außenwirtschaftsgesetz (Foreign Trade and Payments Act)
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority)
BKA	Bundeskriminalamt (Federal Criminal Police Office)
BSA	Bank Secrecy Act
CAD	Canadian Dollar
Cf.	Confer (compare)
CFT	Combating the Financing of Terrorism
COVID-19	Coronavirus Disease 2019
DeFi	Decentralized Finance
DNFBPs	Designated Non-Financial Businesses and Professions
E.g.	Exempli gratia (for example)
E.V.	Eingetragener Verein (Registered Association)
EBA	European Banking Authority
EBF	European Banking Federation
Email	Electronic mail
EU	European Union
EUR	Euro
Europol	European Police Office
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
Fintech	Financial Technology
FIU	Financial Intelligence Unit
G20	Group of Twenty

GbR	Gesellschaft bürgerlichen Rechts (Partnership under Civil Law)
GG	Grundgesetz für die Bundesrepublik Deutschland, Grundgesetz (Basic Law)
GmbH	Gesellschaft mit beschränkter Haftung (Private Limited Company)
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten, Geldwäschegesetz (Money Laundering Act)
GwGMeldV-Immobilien	Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich, Geldwäschegesetzmeldepflichtverordnung-Immobilien (Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act)
I.e.	Id est (that is)
Ibid.	Ibidem (in the same place)
ISIL	Islamic State in Iraq and the Levant
KryptoWTransferV	Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten, Kryptowertetransferverordnung (Crypto Asset Transfer Regulation)
KWG	Gesetz über das Kreditwesen, Kreditwesengesetz (Banking Act)
KYC	Know Your Customer
Lit.	Littera (letter)
LKA	Landeskriminalamt (State Criminal Police Office)
ML	Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism
MoPeg	Gesetz zur Modernisierung des Personengesellschaftsrechts, Personengesellschaftsrechtsmodernisierungsgesetz (Act to Modernize the Law on Civil Law Partnerships)
MVTS	Money or Value Transfer Services
NFT	Non-Fungible Token
NGO	Non-Governmental Organization
No.	Number
NPO	Non-Profit Organization
NRA	National Risk Assessment

OECD	Organization for Economic Co-operation and Development
PML	Professional Money Launderer
Rec.	Recital
RÜST GW/TF	Ressortübergreifender Steuerungskreis zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung (Interagency Steering Committee for Combating ML/TF)
SAR	Suspicious Activity Report
StGB	Strafgesetzbuch (Criminal Code)
TBML	Trade-Based Money Laundering
TF	Terrorist Financing
TFEU	Treaty on the Functioning of the European Union
TFS	Targeted Financial Sanctions
TFTP	Terrorist Finance Tracking Program
TraFinG	Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten, Transparenzregister- und Finanzinformationsgesetz (Transparency Register and Financial Information Act)
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
U.S.	United States (of America)
USD	United States Dollar
VASP	Virtual Asset Service Provider
VAT	Value-Added Tax
ZAG	Gesetz über die Beaufsichtigung von Zahlungsdiensten, Zahlungsdiensteaufsichtsgesetz (Payment Services Supervision Act)

1 Introduction

1.1 Research Background and Objective

Today, financial crime is a global challenge for business and society. In particular, money laundering (ML) and terrorist financing (TF) are major concerns for the financial system as well as for peace and security.[1]

One of the most famous early cases of ML was Al Capone, who hid the proceeds of his illegal business in laundromats in the early 20th century.[2] More recently, ML has received increased attention following incidents such as the Panama Papers and other high-profile investigations that revealed the role of offshore entities in global ML schemes.[3] In the context of TF, the issue has received increased public attention, particularly since the terrorist attacks in the United States (U.S.) in 2001 and the growing threat of terrorism in Europe in recent years.[4]

Financial crimes such as ML and TF pose a multidimensional threat that extends beyond the financial sector to broader socio-economic structures. These illicit activities not only undermine market integrity, but can also create dependencies between legitimate businesses and, for example, organized crime groups. By undermining a nation's economy, criminals can also gain significant political and financial influence over time, escalating levels of crime and corruption. The resulting loss of consumer confidence and increased public expenditures, such as for law enforcement, further strain societal resources. In addition, these crimes and related investments have a distorting effect on macroeconomic variables such as interest and exchange rates, and facilitate tax evasion, resulting in significant revenue losses for governments. Overall, the negative impact of this financial crime affects market dynamics, governance structures, and societal trust, and undermines overall economic stability.[5]

According to the United Nations Office on Drugs and Crime (UNODC), the annual volume of ML on a global scale is estimated to be between two percent and five percent of the world's gross domestic product, representing a financial range between United States Dollars (USD) 800 billion and USD 2 trillion, which results in various risks.[6]

[1] confer (cf.) European Council (Fight against ML and TF), 2023.
[2] cf. Levi & Soudijn, 2020, p. 580; Unger, 2011, p. 615.
[3] cf. Korejo, Rajamanickam & Said, 2021, p. 725.
[4] cf. Euskirchen, 2017, p. 7.
[5] cf. Ibidem (Ibid.), pp. 22-24.
[6] cf. United Nations Office on Drugs and Crime (Overview), n.d.

These risks arise from the increasing interdependence of financial flows, technological innovations such as virtual currencies, existing loopholes or gaps in the system, and the complex and evolving nature of criminals. As a result, the identification and prosecution of ML and TF activities, particularly cross-border activities, is becoming increasingly challenging.[7]

For this reason, efforts have been made at the international and national levels to combat these financial crimes. In this context, the tools developed by global bodies such as the Financial Action Task Force (FATF), the United Nations (UN), and the Organization for Economic Co-operation and Development (OECD) will be examined, as well as the frameworks in place in the United States, the European Union (EU), and Germany.

As Germany is particularly exposed to financial crime due to its leading economy, open borders, financial center, and large amount of cash in circulation, the fight against ML and TF requires robust measures.[8]

Therefore, the current landscape of ML and TF threats in Germany is examined and the weaknesses and shortcomings of the framework are identified. The aim of the dissertation is to provide a comprehensive understanding of the complexities involved and to recommend approaches and strategies for substantial improvements in the fight against financial crime. In this context, the Kotter Model is adapted, leading to sustainable change. The analysis is particularly relevant to policymakers, regulators, private entities, and academics concerned with strengthening financial systems against these destabilizing activities. As such, the findings and recommendations of this work are intended to be a central resource in ongoing efforts to combat ML and TF, thereby enhancing both economic integrity and societal trust.

1.2 Methodology

The methodology employed in this dissertation is designed to provide a comprehensive and critical understanding of the multi-layered complexities surrounding financial crime, with a particular focus on ML and TF.[9]

Therefore, the research is based on an extensive literature review of existing academic publications as well as laws, directives, regulations, conventions, resolutions, guidelines and recommendations at the national and international level to combat ML and TF. In addition,

[7] cf. European Council (Fight against ML and TF), 2023; Euskirchen, 2017, p. 8.
[8] cf. Financial Action Task Force, 2022, p. 21; Euskirchen, 2017, p. 8; International Monetary Fund, 2016, p. 7.
[9] Therefore, the scope of this dissertation extends beyond the financial sector to include a broader analysis of anti-money laundering and counter-terrorist financing strategies, taking into account the complexity and interconnectedness of these areas.

relevant reports or publications of international institutions, such as the FATF, the UN or the EU, and national institutions, including the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) in Germany or the Financial Intelligence Unit (FIU), which provide relevant insights into these phenomena, as well as actual case studies are taken into account.[10]

A comprehensive analysis and evaluation of the existing body of knowledge on ML and TF allows for a nuanced understanding of the subject matter and the identification of recurring threats, vulnerabilities, and current countermeasures across data sources. The approach thus supports the central objective of critically assessing the current ML and TF situation in Germany in order to fill these gaps by evaluating effective approaches against ML and TF.

The dissertation concludes with a presentation of findings and recommendations. As the analysis goes beyond the existing legal framework and explores potential improvements, the research culminates in a set of recommendations aimed at strengthening the existing legal framework, improving enforcement mechanisms, and enhancing cooperation among stakeholders involved in the fight against ML and TF.

By synthesizing and analyzing a wide range of data, this study aims to make a meaningful contribution to the existing body of knowledge and policy-making in the area of financial crime.

[10] The latest date for the literature and laws considered is June 30, 2023, due to further revision and completion of the dissertation.

2 Money Laundering and Terrorist Financing Definitions and Processes

2.1 Money Laundering Definitions

2.1.1 First Definitions

The first attempts to define ML originated in the U.S., where the first ML cases were uncovered. In the mid-1980s, the U.S. was the first country in the world to introduce an ML offense.[11] In this context, the *Presidents' Commission on Organized Crime* developed a phenomenological-descriptive working definition. At that time, the term *money laundering* described the process by which criminals convert their so-called dirty money, the illegal proceeds of criminal activity, into clean money in order to conceal the true origin of the money or to make it appear legitimate.[12] The concept of ML has evolved from general usage rather than being an original legal concept.[13] The 1985 definition was thus the catalyst for a dynamic international development and the precursor of more modern definitions of ML in both civil and common law.[14]

2.1.2 International and European Union Law Definitions

2.1.2.1 International Law

The first supranational description of ML, and thus the first step towards criminalizing ML under international law, was the *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*[15], adopted in Vienna in December 1988 and therefore known as the Vienna Convention.[16] The main objective was to prevent the illicit proceeds of crime from entering the legitimate economy, although the scope of the described criminal offenses was limited to the proceeds of drug crimes.[17]

[11] cf. 18 United States Code § 1956 - Laundering of monetary instruments (18 USC § 1956), 2001; 18 United States Code § 1957 - Engaging in monetary transactions in property derived from specified unlawful activity (18 USC § 1957), 2001.
[12] cf. President's Commission on Organized Crime, 1984, p. 7.
[13] cf. Schneider, Dreer & Riegler, 2006, p. 15.
[14] cf. Herzog & Achtelik, 2014, Introduction Rec. 58.
[15] United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), 1988.
[16] The term *money laundering* itself has already been used by the United States in the U.S. Money Laundering Control Act of 1986. In the Vienna Convention, however, the term *money laundering* is not explicitly mentioned (cf. Kersten, 2002, p. 50).
[17] cf. Korejo, Rajamanickam & Said, 2021, pp. 726-727.

In November 1990, the *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*[18], also known as the Strasbourg Convention, was opened for signature and for the first time defines not only criminal offenses but also ML offenses.

While Article (Art.) 6 subparagraph (1) reiterates basic elements of the Vienna Convention, it expands the scope of predicate offenses beyond drug trafficking.[19]

According to the Explanatory Report, the approach in the Strasbourg Convention is designed to combat the laundering of proceeds from a broader range of offenses than the Vienna Convention.[20] Thus, the predicate offenses are potentially limited only by the national law of the member states.[21]

Both the Vienna and Strasbourg Conventions are of particular importance because, under the German Basic Law (Grundgesetz, GG)[22], they are legally binding on their signatories as treaties under international law.[23] These definitional approaches are normative.[24]

2.1.2.2 European Union Law

The EU's First Anti-Money Laundering Directive (AMLD)[25] was adopted by the European Council of Ministers in June 1991.

The definition of ML in the First AMLD was originally taken from the Vienna Convention, with much of its content remaining unchanged to this day.[26] Even in the most recent Directive (EU) 2018/1673 to combat ML through criminal law[27], which was published on November 12, 2018, the definition of the acts that are considered as ML when committed intentionally in Art. 3 (1) is still identical in wording, with the sole exception that aiding and abetting, inciting and attempting to commit an offense under Art. 3 (1) are separately regulated in Art. 4.[28]

[18] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Strasbourg Convention), 1990.
[19] cf. Ibid., 1990, Art. 6 (1).
[20] cf. Council of Europe, 1990, p. 8.
[21] cf. Strasbourg Convention, 1990, Art. 6 (4).
[22] Grundgesetz für die Bundesrepublik Deutschland (GG), 2022.
[23] cf. Gürkan, 2019, p. 43; GG, 2022, Art. 25.
[24] cf. Gürkan, 2019, p. 43.
[25] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (Document 31991L0308), 1991.
[26] cf. Ibid., Art. 1.
[27] Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law (Document 32018L1673), 2018.
[28] cf. Ibid., Art. 3 (1), 4.

The legal requirements of the AMLDs are binding on the member states of the EU.[29] The implementation of the normative definitional approach into national law is the responsibility of the parliament of each member state.[30]

In contrast to the basic definition, the list of predicate offenses has changed over the years. The First AMLD only included drug offenses as a possible predicate offense to criminal activity with reference to the Vienna Convention. However, the recitals (Rec.) already indicate that ML predicate offenses include not only drug offenses but also the proceeds of other criminal activities such as organized crime or terrorism.[31]

In the Second AMLD[32], the concept of *criminal activity* is further defined in Art. 1 (E) as "any form of criminal involvement in the commission of a serious crime".[33] The concept of *serious crime* thus encompassed a separate, concrete catalog of potential predicate offenses.[34]

These predicate offenses were further expanded in the Third[35] and Fourth[36] EU AMLDs. The Fourth AMLD added tax offenses and any offense punishable by a custodial sentence of more than one year to the list of predicate offenses, reflecting a growing trend toward an *all-crimes approach*, in which almost all crimes are relevant as potential ML predicate offenses.[37]

The Fifth AMLD[38] builds on the Fourth AMLD. However, it also includes provisions to strengthen and extend the existing regime, as well as new regulatory measures for cryptocurrencies in the fight against ML and TF. Within this framework, a legal definition of virtual currencies has been introduced.[39] Directive (EU) 2018/1673 introduced a

[29] see for example: Document 31991L0308, 1991, Art. 18 or Document 32018L1673, 2018, Art. 16.
[30] cf. Gürkan, 2019, p. 44.
[31] cf. Document 31991L0308, 1991, Rec. 9, Art. 1 third indent; Vienna Convention, 1988, Art. 3 (1) lit. a; Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Document 32005L0060), 2005, Rec. 7.
[32] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (Document 32001L0097), 2001.
[33] Ibid., Art. 1 (E).
[34] cf. Ibid., Art. 1 (1) lit. e.
[35] Document 32005L0060, 2005.
[36] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Document 32015L0849), 2015.
[37] cf. Ibid., Rec. 11, 14, Art. 3 (4) lit. f.
[38] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Document 32018L0843), 2018.
[39] cf. Ibid., Art. 1 (2) lit. d Number (No.) 18.

harmonized definition of ML, in order to fill any gaps in the local legislation of EU countries. As part of this harmonization, additional predicate offenses have been added, such as environmental crimes, cybercrime, human trafficking and smuggling, and tax crimes.[40]

2.1.2.3 Financial Action Task Force

As the prevention of ML has become increasingly transnational, the efforts of national legislators have been and continue to be accompanied by guidelines and recommendations from transnational organizations and bodies. These include the FATF, an expert body that was established at the Group of Seven (G7) Summit in Paris in 1989. The purpose of the FATF is to develop a coordinated international approach to combating ML and TF.[41] In early 1990, the FATF first published *The Forty Recommendations of the Financial Action Task Force on Money Launderin*g (40 Recommendations), which set minimum standards for effective anti-money laundering (AML).[42]

According to the FATF's short definition, ML is the transformation of illicitly obtained proceeds into assets with the aim of concealing their criminal origin.[43] The non-binding list of predicate offenses in the 40 Recommendations contains various designated categories of offenses.[44] These predicate offenses include offenses that the FATF considers to be serious offenses. Initially, the focus was on drug offenses, in line with the UN.[45] However, the list of crime categories has been steadily expanded.[46] After the terrorist attacks of September 11, 2001, and the developments that followed, the FATF increasingly focused on the link between ML and international terrorism.[47] In 2003, the FATF again amended the list of predicate offenses in the 40 Recommendations, which has since been significantly expanded.[48]

The FATF was not created by an agreement under international law. Instead, member states have voluntarily committed themselves to comply with the FATF's Recommendations, but

[40] cf. Document 32018L1673, 2018, Art. 2-3.
[41] cf. Financial Action Task Force (FAQs), n.d.
[42] cf. Financial Action Task Force, 1990.
[43] cf. Financial Action Task Force (FAQs), n.d.
[44] cf. Financial Action Task Force (40 Recommendations), 2023, General Glossary: Designated categories of offences, pp. 123-124.
[45] cf. Gürkan, 2019, p. 46.
[46] In 1996, the list has been expanded for the first time (cf. Financial Action Task Force, 1996).
[47] The eight Special Recommendations on Terrorist Financing published in October 2001 and the ninth Special Recommendation supplemented in June 2004 constitute the *FATF IX Special Recommendations* (cf. Financial Action Task Force, 2001).
[48] cf. Financial Action Task Force, 2003, Recommendation 1 with reference to the definition of the designated categories of offences in the Glossary.

are not required to implement them into domestic law.[49] The Recommendations are therefore largely non-binding under international law.

Nevertheless, it cannot be generally assumed that the FATF's Recommendations are therefore of less importance than provisions that are binding under international or EU law. The FATF is a body that plays a decisive role in shaping the fight against ML and TF and has thus acquired a high reputation. For these reasons, the 40 Recommendations have at least a de facto binding force comparable to that of a convention.[50] In addition, the FATF Recommendations serve as a model for the member states' legislation[51], and EU legislation is regularly aligned with the 40 Recommendations.[52]

Furthermore, the FATF possesses diverse political and informal methods to exert pressure. One such example is mutual evaluations which involve comprehensive country reports for every member state. The primary objective is to scrutinize the nation's prevention measures against financial crime based on effectiveness and technical compliance. The report then provides recommendations to the respective country for further enhancing its AML and CFT efforts.[53] Similarly, the risk of reputational damage or international political pressure, exempli gratia (e.g.) if a state is blacklisted by the FATF, provides opportunities for sanctions against non-members.[54]

The question is whether sanctions resulting from political pressure are effective and actually lead to a change of attitude on the part of the credit institutions concerned. This is probably the case as long as the sanctions do not lead to a significant loss of profits. However, in the case of thriving offshore jurisdictions, this may be called into question at some point.[55]

2.1.3 Criminological Definition

There are several criminological-phenomenological definitional approaches that are, at least in essence, similar. According to them, ML is any legal or factual process that serves to effectively conceal the traces of the illegal origin of the proceeds of crime. The aim is to introduce the illegally obtained assets into the regular economic cycle as apparently legal assets.[56]

[49] cf. Herzog & Achtelik, 2014, Introduction Rec. 61.
[50] cf. Findeisen, 2009, § 70 Rec. 4.
[51] cf. Deutscher Bundestag, 2002, p. 81.
[52] cf. Mileusnic, 2023, p. 2.
[53] cf. Financial Action Task Force (Mutual Evaluations), n.d.
[54] cf. Herzog & Achtelik, 2014, Introduction Rec. 70.
[55] cf. Gürkan, 2019, p. 49.
[56] cf. Suendorf, 2001, p. 44.

It can be assumed that the above-mentioned phenomenological working definition of the *President's Commission on Organized Crime* served as a starting point to be confirmed by empirical-criminological methods. Thus, criminological definitions of ML have both phenomenological and empirical components.[57]

2.1.4 Generally Applicable Definition

The foregoing discussion illustrates that there are a variety of legal definitions of ML. What they all have in common is the goal of disguising the origin of funds, bringing them into the legitimate financial and economic system without leaving a trace, and thus avoiding prosecution.[58]

However, apart from the core elements of the definition, the individual approaches to the definition differ. Due to the large number of potential ML activities, it is difficult to precisely identify predicate offenses and thus to provide a generally applicable definition. Moreover, the phenomenology of ML has a transnational character. Global definitions of ML acts and predicate offenses differ according to the characteristics of each country, which also makes a general definition difficult.[59]

2.2 Money Laundering Cycle

Money laundering activities and the development of techniques depend on the ingenuity and experience or professionalism of money launderers, as well as the new technological capabilities available to criminals.[60] For this reason, and due to the high number of unreported cases, the following suggested methods are not guaranteed to be complete.[61]

The most common model of the ML process is divided into the following three stages:

- Placement
- Layering
- Integration[62]

2.2.1 Placement

In order to minimize the risk of detection, the origin of illegal proceeds must be concealed. Placement involves moving the funds into the financial system, such as depositing them in

[57] cf. Rebscher & Vahlenkamp, 1988, p. 110.
[58] cf. Schneider, Dreer & Riegler, 2006, p. 17.
[59] cf. Gürkan, 2019, p. 53.
[60] cf. Financial Intelligence Unit, 2022, p. 31; Levi & Soudijn, 2020, p. 584; Bussmann, 2018, pp. 137-138.
[61] cf. Alshantti & Rasheed, 2021, p. 13.
[62] cf. Levi & Soudijn, 2020, p. 582; United Nations Office on Drugs and Crime (Overview), n.d.

a bank, so that they no longer have a direct link to the criminal activity. Money launderers use a variety of techniques, the common feature of which is the conversion of cash into either other currencies or other assets.[63]

Conversion into Book Money

Crime generates profits for its perpetrators, often in the form of large sums of cash. Drug trafficking and TF in particular use cash as a means of payment, as opposed to white-collar crimes such as corruption or fraud.[64]

A key step in the ML cycle is the infiltration of the proceeds into the legitimate financial system. This can be done by converting cash into book money.[65]

Smurfing

Smurfing is a strategy used by money launderers to divide large sums of money into many smaller amounts. These amounts are calculated to remain below certain thresholds to avoid identification protocols or reporting requirements. The fragmented amounts are then deposited into various bank accounts or transferred by alternative methods. This dispersal obscures the inherent connection between these transactions, making it difficult to trace the origin and destination of the capital.[66]

Exploitation of the Underground Banking System

The underground banking system also provides a means for criminals to launder money and is particularly prevalent in South Asia. The so-called *hawala banking*, once a traditional method of money transfer, has evolved under the influence of globalization and technology. It is used primarily by migrant workers for family remittances, by criminal organizations for illicit financing and ML, and even by international aid organizations in regions with unstable financial infrastructures.[67]

Hawaladars are money transmitters associated with particular regions or ethnic groups who facilitate the transfer and receipt of money or its equivalent. Their unique characteristic, which distinguishes them from other money transmitters, is their reliance on non-bank methods of settlement, including trade and cash transactions, and extended settlement periods.[68]

[63] cf. Levi & Soudijn, 2020, p. 582; Schneider, Dreer & Riegler, 2006, p. 17.
[64] cf. European Commission, 2022, pp. 6-7; Levi, 2002, p. 183.
[65] cf. Suendorf, 2001, p. 162.
[66] cf. Usman Kemal, 2014, pp. 417, 420.
[67] cf. Rahimi, 2021, pp. 131-132.
[68] cf. Financial Action Task Force (The Role of Hawala), 2013, p. 9.

Over- and Under-Invoicing

Another ML technique is over- or under-invoicing. In this approach, money launderers purchase or export commercial goods abroad at highly inflated or below market prices in order to transfer value by misrepresenting the price. It is important that the importer and exporter work together.[69]

Cash Purchases

Larger amounts of illicit cash can also be used to purchase physical assets. These assets include jewelry, diamonds, gold, other precious stones and metals, luxury vehicles, and other valuable items. These purchases are not always intended for long-term retention. The money received by the criminals for the sale of the goods is then transferred to a bank account as a legal deposit.[70]

2.2.2 Layering

The next step is layering, where the money is moved around, for example, using multiple wire transfers and offshore banks. The goal is to disguise the origin of the money, cover the tracks, and thwart prosecution of the crime.[71]

International Financial Centers and Third Parties

One of the main approaches is to transfer of the book money to international financial centers. Offshore financial centers or tax havens play an important role in this context. These countries have non-standard, highly advantageous tax regimes to attract foreign capital. Furthermore, they offer additional services and excellent business and trade conditions, such as adequate infrastructure, a reliable financial and judicial system, including a secure legal environment, or generally low administrative constraints. Because of these favorable financial conditions, many reputable financial institutions maintain branches in these countries. Sometimes the advantages of offshore centers are used to evade taxes, but more and more criminals are using these areas for ML and TF.[72]

Legal Entities

Another technique in the layering process is the use of legal entities. Complex corporate structures or anonymous networks of shell companies and other arrangements, particularly

[69] cf. Financial Action Task Force/Egmont Group, 2020, p. 26; Financial Action Task Force/Organization for Economic Cooperation and Development, 2006, pp. 4-6.
[70] cf. Suendorf, 2001, p. 175.
[71] cf. Cassella, 2018, p. 495.
[72] cf. Lénártová, 2020, p. 2.

in jurisdictions with less stringent AML controls, are conducive to hiding the identity of the criminals behind the legal entity and laundering the illicit proceeds. In this way, money launderers are able to transfer large sums of money disguised as legitimate business transactions. In order to make the identification of the beneficial owner more difficult, straw men are often used to set up these networks.[73]

For example, consulting firms, especially those located in reputable jurisdictions, can be used for ML. Criminals establish or acquire these firms and then set up subsidiaries in various jurisdictions around the world. While providing genuine services, they also provide fictitious services, particularly to international clients, which are more difficult to verify, thereby channeling illicit funds. To bolster their legitimacy, these firms maintain extensive documentation of all transactions and may have features that highlight their supposed international expertise.[74]

Professional Secrecy

Professional secrecy, which applies to bankers and lawyers, for example, also allows money launderers to carry out financial transactions quickly and anonymously.[75]

2.2.3 Integration

In the final step, integration, the funds are integrated into the legitimate economy and are available to the criminal from supposedly clean sources to finance legitimate activities or to make investments.[76]

Loan-back Method

One of the approaches to integrate the money is the loan-back method. The criminals who want to launder the money decide, for example, to invest in a company for which they take out a loan. In effect, they are lending themselves their own dirty money by taking the loan from the bank where the dirty money is already stored. In this way, they are able to use their own account or that of an intermediary to whom the criminals have previously secretly given money in the amount of the loan.[77]

[73] cf. European Commission, 2022, pp. 8-9; Financial Action Task Force (Annual Report), 2023, p. 12; Teichmann, 2020, p. 243.
[74] cf. Teichmann, 2020, p. 243.
[75] cf. Levi, 2022, pp. 126-128, 130, 137.
[76] cf. Levi & Soudijn, 2020, p. 582; United Nations Office on Drugs and Crime (Overview), n.d.
[77] cf. Soudijn, 2016, p. 301.

Investment in Companies

As mentioned above, money launderers can also invest the dirty money in businesses in legitimate sectors that are not intended to be used for criminal purposes in order to avoid detection and even legally increase their income.[78]

Real Estate

Real estate can be used for all three stages of ML. Through cash payments, money launderers have opportunities for placement in both the acquisition and renovation of real estate, and for layering through the purchase and sale of real estate.

Above all, real estate is well suited for integration. After buying and renovating a property, it can be rented out. At this point, the incriminated money is fully integrated into the official economy and generates legitimate rental income.[79]

Cash-intensive Businesses

Businesses where customers typically pay in cash, such as bars, restaurants, kiosks, nightclubs, or even hair salons, are often used for ML. Especially when no bill is required, operators can claim much higher profits and make up the delta in the cash register with dirty money. It is almost impossible to prove this discrepancy months or years later.[80] Casinos also offer a variety of options. One technique is to exchange a sum of illegal cash for gambling tickets to win or lose a small portion of the same amount, and then exchange them for legal cash or checks after a few hours.[81]

2.2.4 Overall View of the Cycle

In reality, not all three stages of the ML cycle need have to be completed in the chronological order shown. Often the stages are combined or repeated several times to best cover the tracks. For example, placement and layering would occur simultaneously if cash proceeds from drug trafficking were deposited in small amounts into bank accounts through various intermediaries and then transferred to shell companies for payment of services.[82]

[78] cf. Organization for Economic Cooperation and Development, 2019, p. 15.
[79] cf. Teichmann (Real estate money laundering), 2018, p. 372.
[80] cf. Dienstbühl, 2022, p. 10; Transparency International Deutschland e.V., 2021, p. 16; Bundesministerium der Finanzen, 2019, pp. 26-27.
[81] cf. Fiedler, Krumma, Zanconato, McCarthy & Reh, 2017, p. 154; United States Department of the Treasury (ML Risk Assessment), 2022, p. 56; Bundesministerium der Finanzen, 2019, pp. 107-108.
[82] cf. Levi & Soudijn, 2020, p. 582; United Nations Office on Drugs and Crime (Overview), n.d.

In addition, within each stage, not only one technique is often used, but several techniques are combined. In this way, the success of concealment is more certain, since the investigating authorities may not have the necessary expertise to follow all the steps.[83]

Furthermore, criminals often use professional money launderers (PMLs), a type of third-party ML. According to the FATF, third-party ML is when a person, the PML, who was not involved in the original criminal activity from which the proceeds to be laundered originated, knowingly assists in or even completely takes over the ML process. For this service, the PML is compensated in an agreed-upon manner. In addition to providing ML services, PMLs may engage in other legitimate professional activities or use their expertise to identify opportunities, such as loopholes in the law, to help criminals keep or launder the dirty money. In general, PMLs are used in this way both to create the necessary distance between the perpetrator and the proceeds of crime and to provide the essential know-how for ML. Professional money launderers can be individuals, a professional ML organization, id est (i.e.) a structured group consisting of one or more individuals, or a professional ML network consisting of several partners and contacts who work together to facilitate ML or even partially subcontract their services.[84]

2.3 Terrorist Financing Definitions

2.3.1 Terrorism Definition

The term *terrorism* has a long history and has evolved significantly over the years. Its use dates back to the late 18th century, and its first appearance in Western public discourse was associated with the Jacobin reign of terror in France from 1793 to 1794. In this context, the word *terrorism* was used to describe the Jacobins' efforts to reshape human nature and society by eliminating the old regime and enforcing civic virtue. Revolutionary tribunals, which prosecuted so-called enemies of the people, played a key role in this process, with death as a common punishment.

The term came to have negative connotations associated with the abuse of power and fear-based tyranny. In the late 19th century, radical organizations disillusioned with conventional political methods turned to political violence, known as *propaganda by the deed*. This form of terrorism was largely discriminatory, often targeting royalty or high-ranking government officials.

[83] cf. Financial Action Task Force/Egmont Group, 2020, p. 40.
[84] cf. Financial Action Task Force, 2018, pp. 10-13.

Terrorism during the Russian Revolution and Civil War was an echo of the Jacobin era. Totalitarian regimes, such as Bolshevik Russia and Nazi Germany, and even some non-totalitarian states, used state terrorism to exert political control.

In the 20th and early 21st centuries, terrorism by insurgent organizations became prominent. These groups, fighting for liberation or against perceived oppressive systems, engaged in largely indiscriminate terrorism. As is often the case, they refrained from identifying themselves as terrorists because of the negative connotations of the term and their perceived supreme righteousness, often referring to their opponents as the terrorists.[85]

The definition of terrorism as it is used today encompasses legal, philosophical, political, economic, and sociological aspects. A common feature, however, is the goal, which is usually not in the interest of an individual, but within an ideological framework that creates an identity. In the case of transnational terrorism, this framework does not refer exclusively to a single state.[86] Another characteristic is the use of violent terrorist acts, which are usually intended to intimidate. The victims involved are therefore arbitrary; what is more important is that the terrorist attack is effective in terms of media coverage.[87]

Due to the complexity and depth of the concept of terrorism, an overview of legally relevant definitions and approaches to such definitions is provided below, which, however, cannot be presented in full. The definitions refer to the respective legal context and therefore have a relative meaning.[88]

International standards refer among themselves to different international definitional approaches. In particular, they refer, as does FATF Recommendation 5, to the definitional approaches and references of the 1999 *United Nations International Convention for the Suppression of the Financing of Terrorism*.[89] This in turn refers in Art. 2 (1) littera (lit.) a to the definitions of the other treaties listed in the Annex[90], but also provides a partial definition in Art. 2 (1) lit. b:

"Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the

[85] cf. Primoratz, 2022.
[86] cf. Albers & Groth, 2015, pp. 11-13.
[87] cf. Middel, 2007, pp. 46-48.
[88] cf. Albers & Groth, 2015, pp. 13-17.
[89] cf. Financial Action Task Force, 2016, p. 1; Financial Action Task Force (40 Recommendations), 2023, Recommendation 5.
[90] cf. International Convention for the Suppression of the Financing of Terrorism, 1999, Art. 2 (1) lit. a.

purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act".[91]

Furthermore, in Resolution 1566[92], the UN Security Council states "that criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism, are in no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or any other similar nature".[93]

Similarly, in the *Council Framework Decision of 13 June 2002*[94], the EU has already defined terrorism-related crimes as "offences under national law, which, given their nature or context, may seriously damage a country or an international organization where committed with the aim of seriously intimidating a population, or unduly compelling a Government or international organization to perform or abstain from performing any act, or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization".[95]

Following the definition of terrorism at the EU level, an almost identical formulation has been included in German law as an indirect definition of terrorism in Paragraph (§) 129a (2) of the German Criminal Code (Strafgesetzbuch, StGB).[96] According to this provision, the formation of a terrorist organization is punishable if the act "is intended to seriously intimidate the population, to unlawfully coerce an authority or an international organization by force or threat of force, or to destroy or significantly impair the fundamental political, constitutional, economic or social structures of a state or of an international organization and which, given the nature or consequences of such offences, may seriously damage a state or an international organization".[97]

Thus, similar definitions are used at the international, EU and German levels, although there is no binding definition under international law. It should be noted, however, that these

[91] International Convention for the Suppression of the Financing of Terrorism, 1999, Art. 2 (1) lit. b.
[92] Resolution 1566 (2004), 2004.
[93] Ibid., No. 3.
[94] Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA) (Document 32002F0475), 2002.
[95] Ibid., Art. 1 (1).
[96] cf. Strafgesetzbuch (StGB), 2023, § 129a (2); for unofficial English version see: German Criminal Code (Strafgesetzbuch - StGB), 2021.
[97] StGB, 2021, Section 129a (2).

approaches are partly in the context of criminal law. The relevance for other regulatory areas may therefore be limited.

Acts of terrorism may also be categorized as such by the international community's inclusion of associated organizations or individuals on terrorist lists, such as those of the UN, regional terrorist lists, such as those of the EU, and national terrorist lists.[98]

2.3.2 Terrorist Financing Definition

Terrorists and their organizations typically rely on money from third parties to finance the planning and execution of terrorist attacks and to support themselves in the interim. Therefore, TF encompasses both the methods and means used by terrorists.[99]

Because of its relationship to the definition of terrorism, a general definition of TF is also difficult.[100] In addition, there is the activity of financing, which is subject to constant change and can be carried out in different ways.[101]

The UN Security Council Resolution 1373 (2001)[102] describes TF as "the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts".[103]

Under German law, TF is defined in the German Money Laundering Act (Geldwäschegesetz, GwG)[104] as the provision or collection of property in the knowledge that it will be used or is intended to be used, in whole or in part, for the formation, incitement or support of a terrorist organization in Germany or abroad (§§ 129a-129b StGB) or for other terrorist offenses as defined in Directive (EU) 2017/541[105] as well as the commission of TF as perpetrator or accomplice punishable under § 89c StGB.[106] The inclusion of incitement and aiding and abetting indicates that the focus is not on individual perpetrators but on networks.[107]

[98] cf. Groth, 2016, pp. 28-29.
[99] cf. United Nations Office on Drugs and Crime (Overview), n.d.
[100] cf. Albers & Groth, 2015, pp.17-18.
[101] cf. Groth, 2016, p. 30.
[102] Resolution 1373 (2001), 2001.
[103] Ibid., Art. 1 (b).
[104] Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG), 2023; for unofficial English version see: Anti-Money Laundering Act (Geldwäschegesetz - GwG), 2020.
[105] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Document 32017L0541), 2017.
[106] cf. GwG, 2023, § 1 (2) No. 1 lit. a in conjunction with StGB, 2023, §§ 129a-129b; GwG, 2023, § 1 (2) No. 1 lit. b in conjunction with Document 32017L0541, 2017, Art. 3, 5-10, 12; GwG, 2023, § 1 (2) No. 2 in conjunction with StGB, 2023, § 89c; GwG, 2023, § 1 (2) No. 3.
[107] cf. Groth, 2016, p. 31; GwG, 2023, § 1 (2) No. 3.

Paragraph 89c StGB defines TF as a series of acts that are financed for the purpose of terrorizing the public, exerting unlawful pressure on a public authority or an international organization by force or threats, or substantially disrupting or dismantling the political, constitutional, economic, or social framework of a state or an international organization. By their nature or consequences, these acts are capable of causing serious damage to a state or an international organization.[108] The provision is both a summary and a partial expansion of previous provisions on criminal liability for TF and is also linked to investigative measures. The preventive focus serves to meet international requirements.[109]

This is largely in line with the definitions in the more recent EU Directives 2018/1673 and 2019/1153[110], which also refer to the above definition in Directive (EU) 2017/541 on the concept of terrorist offenses.[111]

Combating TF involves both eliminating or curtailing illicit financing, for example by intercepting relevant financial flows, and preventing planned terrorist acts. Therefore, in accordance with the *follow the money* principle, the first step is usually to observe conspicuous and suspicious transactions in order to draw conclusions about the individuals and organizations behind them and their interdependencies.[112] The aim is to identify immediate threats of terrorist attacks and to prevent the planning and execution of such terrorist activities.[113]

2.4 Terrorist Financing Stages

While ML, as described above, is a circular process, the process of TF is usually linear. Accordingly, TF can typically be divided into the following four stages:

- Raise
- Store
- Move
- Use[114]

[108] cf. StGB, 2023, § 89c.
[109] cf. Sieber & Vogel, 2015, pp. 152-155, 162, 168-181.
[110] Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (Document 32019L1153), 2019.
[111] cf. Document 32018L1673, 2018, Art. 2 (1) lit. b; Document 32019L1153, 2019, Art. 2 No. 10.
[112] cf. Shetterly, 2006, pp. 327-348.
[113] cf. Groth, 2016, p. 35.
[114] cf. United Nations Office on Drugs and Crime (Overview), n.d.

2.4.1 Raise

The funds provided to terrorist organizations to plan and carry out terrorist activities can come from both legitimate and illegitimate, criminal sources. The following are typical financial resources and sources used by terrorists.[115]

Legal Commercial Companies

One way to legally obtain funds to finance terrorist activities is through legitimate businesses operated by potential terrorists and sleepers, or by individuals who support them. Several investigations have identified links between terrorist organizations and commercial enterprises, including restaurant franchises and used car dealerships.

In one specific case, used cars were being shipped to West Africa. A member of the Eastern and Southern Africa Anti-Money Laundering Group reported that dealers imported used cars from, for example, Japan or the United Kingdom and transferred the proceeds from the sale of the cars to terrorist organizations. The owners of the car dealerships were from countries or regions with a high risk of terrorism.[116]

Non-Governmental Organizations and Non-Profit Organizations

In addition, terrorist organizations often misuse or abuse non-governmental organizations (NGOs), non-profit organizations (NPOs) and charities. According to a FATF study, abuse can be divided into five types: First, it is possible for individuals in NPOs to funnel donations to terrorist organizations. Furthermore, NPO authorities are often exploited for the benefit of terrorists, programs are misused to support criminals, and bogus NPOs are created through fraud. Finally, NPOs also provide recruitment support to terrorist organizations.

The NPOs most affected by or at risk of these abuses provide services and tend to operate very close to the terrorist threat.[117] Moreover, NPOs that send funds to their counterparts in the terrorist organization's territory are often exploited. Appropriate and thorough due diligence of NPOs is therefore essential.[118]

Donations

Furthermore, organizations receive direct donations and grants from corporations or even individuals. An analysis of TF-related cases in the U.S. from 2001 to 2014 shows that

[115] cf. United Nations Office on Drugs and Crime (Overview), n.d.
[116] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 19.
[117] cf. Murrar (Non-profit organisations), 2022, pp. 19-21, 25-26; Financial Intelligence Unit, 2022, p. 31; Financial Action Task Force, 2022, p. 101; Financial Action Task Force (NPOs), 2014, pp. 36, 74.
[118] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 14.

terrorist networks received direct financial support from individuals in approximately 33 percent of these cases.[119]

Criminal Activity

In addition to legitimate sources, terrorists receive funds from criminal activities such as illicit trafficking. Smuggled goods such as alcohol, drugs, and cigarettes generate large revenues. The latter in particular is a growing threat to TF, for example in West Africa.[120] With respect to drug trafficking, a FATF study of financial flows related to the production and trafficking of Afghan opiates found that millions of U.S. Dollars in profits from the illicit trade were used to finance terrorist organizations. In one specific example, the UN Al-Qaeda & Taliban Sanctions Monitoring Team found that poppy trafficking funded one-third of the Taliban's total budget of USD 400 million in 2011 and 2012.[121] In most cases, terrorist organizations originate from areas where drug trafficking is not or not sufficiently prohibited, which facilitates their financing.[122]

Furthermore, the FATF Report on the *Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)* lists the smuggling and sale of antiquities and artifacts as a means of TF.[123]

The same report also cites tax crimes as a means of TF through the use of tax refunds or tax-related proceeds that are not declared as such.[124]

Another means of TF is insurance or credit fraud, as well as identity theft to obtain funds through credit card fraud.

Terrorists also finance themselves through bank robberies. Bank robbery has been a means of financing the Indonesian-based terrorist organization Jemaah Islamiyah, among others.[125]

Extortion of Populations and Businesses

Extortion of people and businesses in the immediate vicinity of terrorist organizations, as well as in the diaspora, is another method of raising funds for terrorist acts. The Taliban, for example, uses funds collected from the local population.[126]

---

[119] cf. United States Department of the Treasury (TF Risk Assessment), 2022, pp. 6-9, 13, 22; United States Department of the Treasury, 2015, p. 44.
[120] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 15.
[121] cf. Financial Action Task Force (Afghan opiates), 2014, p. 42.
[122] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 16.
[123] cf. Financial Action Task Force (ISIL), 2015, pp. 16-17.
[124] cf. Ibid., p. 23.
[125] cf. Bin Sulaiman, Schetinin & Sant, 2022, p. 55; John & Naaz, 2019, p. 1060; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 15.
[126] cf. Koseli, Ekici, Eren & Bitner, 2020, p. 215; Financial Action Task Force (Afghan opiates), 2014, p. 42.

Similarly, the Kurdistan Workers' Party uses funds from the taxation of illegal drugs, protection and arbitration fees, cigarette smuggling, and even human trafficking, among others, to fund terrorist acts.[127]

The Islamic State in Iraq and the Levant uses a similar method to extort money from the local population through supposed taxes: Government employees from ISIL territory are often required to travel to locations outside the controlled area to withdraw their salaries in cash and pay 50 percent of it to ISIL upon their return.[128] In addition, ISIL has imposed purported taxes on the movement of goods, withdrawals from private banks, and motor vehicles or fuel in the occupied territories. Involuntary donations in the form of protection money or school fees for children are also part of the financing of terrorist acts.[129]

Another method used in the past by the terrorist Liberation Tigers of Tamil Eelam to fund its operations was to extort money from members of the Tamil diaspora. In late 2005 and early 2006, the Liberation Tigers of Tamil Eelam raised large sums of money in Canada and parts of Europe by pressuring individuals and business owners in the diaspora[130] who refused to support the organization with donations to give the requested amount of money.[131]

Kidnapping for Ransom

Kidnapping for ransom is a growing source of funding for terrorist attacks.[132] Ransoms paid to terrorist organizations for the release of hostages are reported to average between Euros (EUR) 600,000 and EUR 8 million per kidnapping.[133] Thus, ransoms can represent anywhere from 5 percent to 50 percent of a terrorist organization's total annual budget, depending on factors such as the size of the group or local economic conditions.[134]

In the context of kidnapping for ransom, physical cash often plays an important role, transported by couriers to the terrorist organization after being handed over by the extortionists.[135] However, payments can also be made through financial institutions. For example, banks or alternative transfer systems such as hawala banking, lawyers, insurance companies, and bureau de change can be used.

[127] cf. European Union Agency for Law Enforcement Cooperation, 2019, p. 54.
[128] cf. Financial Action Task Force (ISIL), 2015, p. 17.
[129] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 17.
[130] According to Human Rights Watch the Tamil diaspora numbered around 600,000 to 800,000 worldwide in 2006. In Canada, the extortion amount ranged from Canadian Dollars (CAD) 2,500 to 5,000 for families and often exceeded that amount for businesses to as much as CAD 100,000 (cf. Human Rights Watch, 2006).
[131] cf. Ibid.
[132] cf. Koseli, Ekici, Eren & Bitner, 2020, p. 215; Financial Action Task Force, 2011, p. 26.
[133] cf. Financial Action Task Force, 2011, pp. 28, 31.
[134] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 18.
[135] cf. Financial Action Task Force, 2011, p. 33.

The fact that kidnappings may take place in a country other than the country where the ransom is paid makes it more difficult to trace the movement of funds.[136]

Furthermore, there are examples of relatives of the victim raising funds on the victim's behalf through loans, the sale of assets, or the use of trust funds to pay the ransom.[137]

State Support

Certain states also support terrorist organizations and their activities by providing the necessary logistics and infrastructure, offering sanctuary or assistance in planning and preparing attacks, or in some cases directly providing funds and weapons. This state support poses an immense threat to international security and peace, as well as to the political and financial stability of the region.[138]

According to the 2021 Country Reports on Terrorism published by the U.S. Department of State in 2023, Cuba, the Democratic People's Republic of Korea, Iran, and Syria are designated as state sponsors of terrorism, resulting in various sanctions.[139] In addition, Russia has been designated by the European Parliament as a state sponsor of terrorism and as a state using terrorist means in its current war against Ukrainian civilians, also resulting in various sanctions packages. Given the limitations of the EU in formally designating countries as state sponsors of terrorism, the EU Parliament advocates that the EU and its member states create an appropriate legal framework, which could potentially include the listing of Russia.[140]

Self-Funding

Small-scale terrorist attacks, in particular, often do not require large sums of money to finance them. Therefore, the savings and loans of individual terrorists and the support networks behind them, or the revenues of companies controlled by them, are usually sufficient.[141]

Since 2001, the proportion of terrorists who finance themselves has increased. One plausible explanation for this increase is the tighter regulations and controls introduced after the

[136] cf. Financial Action Task Force, 2011, p. 26.
[137] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 18.
[138] cf. Ibid., p. 20.
[139] cf. United States Department of State, 2023, pp. 212-216.
[140] cf. European Parliament, 2022.
[141] cf. Levy & Yusuf, 2021, p. 1169; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 19.

September 11 attacks, which make it more difficult for other terrorists to support terrorist cells.[142]

2.4.2 Store

If the terrorists cannot or will not use the funds immediately, or if the funds cannot be transferred immediately, they must be stored temporarily.

To avoid using as much money or even cash in this step, less regulated alternatives such as mobile payment services or commodities that retain their value over time are often used to store assets. Another advantage is that these commodities can easily be traded independently of the official international banking system. Metals and precious stones are particularly well suited for this purpose. Diamonds, for example, are unlike other commodities in that they are untraceable, light in weight and high in value, all of which benefit terrorists who smuggle them. In addition, diamond mines are usually located in remote areas without adequate border controls and rule of law. Finally, the international fragmentation of the diamond industry facilitates illicit transactions for TF.[143]

2.4.3 Move

In order to get the funds raised to where they are needed, i.e. to finance terrorist activities, they usually have to be transferred internationally. For this reason, all financial institutions are potentially at risk of TF through money transfers. The main mechanisms for such transfers are highlighted below.[144]

Banking Sector

Despite the measures already taken by the banking sector to combat ML and TF, financial institutions continue to be used by terrorists to transfer money internationally. The main advantages are the efficiency and reliability of the banking sector, which allows for easy and fast money transfers.

Due to the scope and size of the international financial sector, transactions conducted by terrorists or for terrorist purposes often go undetected. For example, it is possible for sympathizers or supporters of a terrorist organization to make structured cash deposits into bank accounts and then make international wire transfers. In addition, savings accounts are

[142] cf. Oftedal, 2015, p. 7.
[143] cf. Akartuna, Johnson & Thornton, 2022, pp. 11, 16; Hardouin, 2009, p. 206.
[144] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 20.

opened at banks and the associated debit cards are made available to members of terrorist organizations abroad. This allows terrorists to obtain cash abroad through cash withdrawals.

Another way to move funds internationally for terrorist activities is to use the bank accounts of international law firms and front companies or NPOs.[145]

Money or Value Transfer Services

Because money or value transfer services (MVTS), can also be used to transfer illicit funds, they are also vulnerable to TF, especially if they are unregulated, operate without a license, or are not subject to adequate oversight. Providers of such international MVTS are particularly important in regions controlled by terrorist organizations or where regular banking services are generally restricted. Families and migrant communities in and from these regions often rely on MVTS to receive funds from relatives abroad or to send it to their country of origin. This mixes legal and illegal transactions, making it difficult to detect transfers used for TF. The greatest threat is posed by employees of service provider who are supporters or sympathizers of terrorist organizations and who covertly and knowingly facilitate the transfer of illicit funds.

For example, hawala banking, which is often used for ML, has been shown to provide opportunities for TF due to the lack of adequate regulations and controls against ML and TF. At the same time, in countries where many terrorist organizations originate and are thus vulnerable to TF, hawala banking is often a legitimate and important MVTS for the population.[146]

Physical Transportation

Cash also plays an important role in TF. Even if funds are not initially obtained in cash, they are often converted into cash before being transferred internationally. National borders without adequate border controls, as well as unregulated and informal economies and the challenge of detecting the smuggling of small amounts of cash, contribute to the undetected illicit transfer of funds.[147]

[145] cf. Financial Action Task Force (Terrorist Financing in West Africa), 2013, p. 33; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 20-21.
[146] cf. Rahimi, 2021, p. 146; United States Department of the Treasury (TF Risk Assessment), 2022, pp. 18-19; Financial Intelligence Unit, 2022, p. 31; Financial Action Task Force, 2022, pp. 21-23, 31; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 21-22; Financial Action Task Force (The Role of Hawala), 2013, p. 41.
[147] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 23.

2.4.4 Use

Despite the many differences between the various terrorist organizations, there is always a need for funding for the common goal of carrying out terrorist plans. However, each organization prioritizes its expenditures differently. They may also evolve or change over time, for example, as the organization expands its capabilities, influence, or infrastructure. Essentially, the use of financial resources distinguishes terrorist organizations from small terrorist cells or lone actors.[148]

Terrorist Organizations

One aspect for which terrorist organizations require substantial financial resources is the recruitment of additional members and the raising of additional funds through propaganda. In this context, the Internet, including social media, is not very cost-intensive for the first steps, but there are usually additional costs for the subsequent steps. Large terrorist organizations also use more complex and costly propaganda operations to spread their ideology and worldview, sometimes publishing newspapers and magazines, managing websites, buying domain names, or even buying radio and television stations.

The willingness to sacrifice for the terrorist organization can be enhanced by financial security and incentives for both members of the organization and their families. For this reason, terrorist groups often require funding to pay salaries to leaders and members, and to support the families of arrested or deceased terrorists, sometimes on a long-term basis.

Often, governments in the countries where terrorist organizations originate neglect certain educational, health, or social services, leading to resentment among the local population. Terrorist groups exploit this by using the financial resources at their disposal to provide these very services by subsidizing or establishing social institutions. In this way, they not only gain popular support, but also facilitate recruitment.

For terrorist operations to be successful, both operatives and sympathizers must be adequately trained. This requires funding for training in weapons handling, bomb making, ideology, and clandestine communications. In addition to virtual online training, land and buildings are purchased for use as training camps and safe havens.

Additionally, terrorists need funds for both the preparation and execution of terrorist attacks. This includes travel to and from the target location, transportation such as vehicles,

[148] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 9-11.

machinery, and weapons. Terrorist groups also need to pay for basic living expenses, forged identity documents, and personnel, such as couriers.[149]

Small Terrorist Cells and Lone Actors

Small terrorist cells and lone actors have significantly lower funding needs because the cost of individual terrorist attacks is typically low and many other typical expenses of large terrorist organizations, such as those for controlling territory or recruiting activities, are eliminated.

Nevertheless, certain basic expenses must be covered. These include accommodation, food, means of transport and communications for the terrorists. In addition, financial resources are needed for the attack itself, such as weapons or explosives.[150]

A report by the Norwegian Defence Research Establishment, which assessed the expenses of 40 jihadi cells that carried out multiple attacks in Europe between 1994 and 2013, found that three-quarters of the attacks cost less than USD 10,000. Costs include all expenses directly related to the terrorist act, such as training, travel, explosives, transportation, or communications.[151]

2.5 Interrelationships of Money Laundering and Terrorist Financing

Although ML and TF are discussed and combated together, the origin of the funds and the ultimate use of the funds are different. While in the case of ML the source of funds is always illegal, the funds used to finance terrorist activities can be of both legal and illegal origin. The opposite is true for the ultimate use of the funds. In the case of TF, the funds are always used for illegal purposes, while the funds introduced into the regular economic cycle through ML may be used for both legal and illegal purposes.[152]

With respect to ML in the context of terrorism, it should also be noted that in the case of TF, the funds are laundered prior to the terrorist act and not afterwards as in other criminal activities. In addition to concealing the criminal origin of the funds, another purpose of ML may be to conceal the intended criminal use of the funds.[153]

[149] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 9-10.
[150] cf. Ibid., pp. 10-11.
[151] cf. Oftedal, 2015, pp. 7, 24.
[152] cf. Jakobi, 2015, pp. 67-68; United Nations Office on Drugs and Crime (Overview), n.d.
[153] cf. Reuter & Truman, 2004, p. 139.

3 Tools to Combat Money Laundering and Terrorist Financing

3.1 International and Transnational Instruments

Because ML and TF activities often cross international borders, a global approach is important to effectively combat these crimes.

A global approach allows countries to share information and resources, which can be critical in identifying and prosecuting individuals and organizations involved in ML and TF. Furthermore, it helps ensure that consistent standards and regulations are in place.[154]

3.1.1 Financial Action Task Force

At the global level, the FATF is one of the most important bodies in the fight against ML and TF. Originally established to combat ML, the FATF expanded its mandate in 2001 to include combating the financing of terrorism (CFT).

The FATF sets international standards for combating ML and TF and monitors the implementation of these standards by its member countries. In this context, the FATF has developed the aforementioned FATF 40 Recommendations and the FATF IX Special Recommendations on the prevention of organized crime, terrorism and corruption. They are regularly reviewed and strengthened in response to new criminal techniques.[155]

Moreover, the FATF provides technical assistance to countries seeking to improve their capacity to combat these crimes. In addition to its work with governments, the FATF also works with the private sector and civil society organizations to raise awareness of the risks of ML and TF, and to promote best practices for preventing these crimes.[156] Furthermore, new developments in the technology and prevalence of ML and TF are presented in regular reports to ensure effective prevention. The use of self-assessment questionnaires and mutual evaluations allows countries to be compared in their implementation of the FATF Recommendations.[157]

The intergovernmental organization now has 39 members and a global network of nine FATF Style Regional Bodies. More than 200 jurisdictions and countries around the world,

[154] cf. Financial Action Task Force (FAQs), n.d.
[155] cf. Financial Action Task Force (About), n.d.
[156] cf. Financial Action Task Force (Private Sector), n.d.
[157] see last report: Financial Action Task Force (Annual Report), 2023.

including the U.S. and Germany, have committed to implementing the FATF standards. They have also been incorporated into EU law as part of the AMLDs.[158]

Forty Recommendations

Recommendations 3 and 5 in particular provide guidance on the criminalization of ML and TF.[159]

Specifically, Recommendation 3 states that ML should be criminalized to the extent provided for in the Vienna and Palermo[160] Conventions. Furthermore, "[c]ountries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences".[161]

The criminalization of TF is set forth in Recommendation 5. Accordingly, countries should criminalize TF as described in the Terrorist Financing Convention[162], as well as the financing of terrorist organizations and individuals. In addition, acts related to TF should be considered predicate offenses to ML.[163]

The principle for deriving and implementing national AML and CFT measures should be the risk-based approach. Accordingly, appropriate measures will be taken after the risk exposure has been determined.[164]

In Recommendations 6, 7 and 35, the FATF outlines that financial sanctions should be applied to persons or entities that pose a risk, such as politically exposed persons (see Recommendation 12). In this context, the funds and assets of such persons and entities should be frozen immediately and no further funds or assets should be made available to them.[165]

Furthermore, countries should ensure that financial institutions carry out appropriate due diligence, for example, to identify beneficial owners (see Recommendation 24) or verify the identity of customers. This customer due diligence is particularly necessary in the case of new business relationships or certain situations and transactions that raise doubts or suspicions (see Recommendation 10). Suspicious transactions must also be reported

[158] cf. Financial Action Task Force (Countries), n.d.
[159] cf. Financial Action Task Force (40 Recommendations), 2023, Recommendations 3, 5.
[160] United Nations Convention against Transnational Organized Crime (Palermo Convention), 2000.
[161] Financial Action Task Force (40 Recommendations), 2023, Recommendation 3.
[162] International Convention for the Suppression of the Financing of Terrorism, 1999.
[163] cf. Financial Action Task Force (40 Recommendations), 2023, Recommendation 5.
[164] cf. Ibid., Recommendation 1.
[165] cf. Ibid., Recommendations 6-7, 12, 35.

immediately to the relevant FIU (see Recommendation 20). In addition, special due diligence requirements apply to high-risk countries (see Recommendation 19).

The FATF also issued Recommendations on how to deal with new technologies and wire transfers, in part to address the growing use of cryptocurrencies around the world (see Recommendations 15-16).[166] In this context, the FATF also published its guidance for a risk-based approach to virtual assets and virtual asset service providers (VASPs) in 2021.[167]

Moreover, the Recommendations explicitly emphasize that countries should ensure international cooperation (see Section G). For example, according to Recommendation 37, countries should provide the widest possible range of mutual legal assistance constructively and effectively in investigations, prosecutions and related judicial proceedings in ML and TF matters.[168]

3.1.2 United Nations

3.1.2.1 United Nations Offices and Council

The UN, through its various agencies and programs, also plays a key role in the fight against ML and TF.

United Nations Office on Drugs and Crime

The UNODC plays an important role in the international fight against corruption, organized crime, drugs and terrorism, including ML and TF.[169] In particular, through the Global Programme against Money Laundering, Proceeds of Crime and the financing of Terrorism, the UNODC promotes international approaches, acts as a coordinator and provides assistance to the UN member states in developing and implementing effective AML and CFT regimes.[170]

The International Money Laundering Information Network, also called IMoLIN, was established by the UN in 1998 and is maintained by UNODC in partnership with international AML organizations. This global network assists governments, organizations and individuals in combating financial crimes such as ML and TF by providing a range of

[166] cf. Financial Action Task Force (40 Recommendations), 2023, Recommendations 10, 15-16, 19-20, 24.
[167] cf. Financial Action Task Force (Virtual Assets), 2021.
[168] cf. Financial Action Task Force (40 Recommendations), 2023, Section G, Recommendation 37.
[169] cf. United Nations Office on Drugs and Crime (About), n.d.
[170] cf. United Nations Office on Drugs and Crime (GPML), n.d.

resources, including a database of AML laws and regulations, an electronic library, a case law database and a calendar of AML events.[171]

Moreover, UNODC has established the Terrorism Prevention Branch, which assists member states in implementing international legal instruments to combat terrorism.[172] It focuses on raising awareness and promoting ratification of these instruments, providing legislative assistance and capacity building. This includes areas such as countering the use of the Internet for terrorism; assisting victims of terrorism; combating chemical, biological, radiological, and nuclear terrorism; responding to transportation-related crimes; protecting human rights while countering terrorism; and CFT. In addition, the Terrorism Prevention Branch works to strengthen international cooperation in criminal matters related to terrorism. It has field experts in various regions of the world who provide regional expertise and support for the implementation of counterterrorism activities in recipient countries. The organization also works in partnership with other UN entities and international organizations to coordinate and cooperate in the delivery of assistance.[173]

United Nations Office of the Coordinator for Counter-Terrorism

The United Nations Office of the Coordinator for Counter-Terrorism is responsible for coordinating the UN system's efforts to counter terrorism and its financing. To strengthen the coordination and coherence of these efforts, the UN Global Counter-Terrorism Coordination Compact was launched in 2018. This framework includes 38 UN entities, the World Customs Organization and the International Criminal Police Organization, also known as Interpol. Additionally, the UN Counter-Terrorism Centre and Special Projects and Innovation Branch provides technical assistance and capacity-building support to member states through a range of programs and projects, focusing on regions and countries most at risk of terrorism, particularly in Africa, Central and South Asia and the Middle East.[174]

United Nations Security Council

The United Nations Security Council is an organ of the UN responsible for the maintenance of international peace and security. Its powers include the ability to investigate and mediate disputes, send peacekeeping forces, and impose economic sanctions, arms embargoes, and even military action if necessary. In this context, it has adopted several resolutions related

[171] cf. International Money Laundering Information Network, n.d.
[172] For more details on the 19 international legal instruments and additional amendments related to the prevention and suppression of international terrorism, see: United Nations Office of Counter-Terrorism (Legal Instruments), n.d.
[173] cf. United Nations Office on Drugs and Crime (TPB), n.d.
[174] cf. United Nations Office of Counter-Terrorism (What we do), n.d; United Nations Office of Counter-Terrorism (Compact), n.d.

to ML and TF, including measures to freeze the assets of designated individuals and entities and to impose financial sanctions on countries and entities that support terrorism.[175]

The Security Council is composed of 15 member states, of which China, France, Russia, the United Kingdom and the U.S. are permanent members and ten are elected by the General Assembly for two-year terms.[176]

3.1.2.2 United Nations Legal Instruments against Money Laundering

United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988

The 1988 Vienna Convention, which entered into force in November 1990, is designed to prevent ML from illicit drug trafficking. Its purpose is to promote cooperation among the parties in order to combat more effectively the various international manifestations of illicit traffic in narcotic drugs and psychotropic substances. To this end, the parties are obliged to take the necessary legislative and administrative measures to implement the Convention. In this context, implementation must take into account the fundamental characteristics of each national legal system.[177]

The Vienna Convention provides for fundamental measures, such as the comprehensive criminalization of drug trafficking (Art. 3) and extensive jurisdiction (Art. 4). It also aims to create extensive possibilities for the confiscation of assets derived from the offenses referred to in Art. 3 (Art. 5) and extradition possibilities (Art. 6) with regard to these crimes. Furthermore, a general improvement of mutual legal assistance between the contracting parties is to be achieved (Art. 7).

It is important to note that the Convention establishes only minimum standards. Article 24 explicitly states that the parties may adopt more stringent measures than those set forth in the Convention.[178]

According to Art. 3 (1) lit. b of the Vienna Convention, the following acts, when committed intentionally, shall be defined as criminal offenses by the parties:

"b) i) The conversion or transfer of property, knowing that such property is derived from any [drug trafficking] offence […], or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit

[175] cf. United Nations Security Council (Security Council), n.d.
[176] cf. United Nations Security Council (Current Members), n.d.
[177] cf. Vienna Convention, 1988, Art. 2 (1).
[178] cf. Ibid., Art. 3-7, 24.

origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;

ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from [any drug trafficking] offence […] or from an act of participation in such an offence or offences;"[179]

Moreover, Art. 3 (1) lit. c (i) adds the following acts:

"c) […] i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from [any drug trafficking] offence or from an act of participation in such offence or offences;"[180]

The Convention's definition of ML is very broad. Article 3 (1) lit. b (i) largely covers all possible financial transactions. For other acts that do not directly involve property but conceal or disguise its true nature or source, Art. 3 (1) lit. b (ii) applies. In addition, Art. 3 (1) lit. c (i) prohibits the acquisition, possession and use of such assets.[181] However, the latter provision (Art. 3 (1) lit. c (i)) is subject to national constitutional principles in order to provide sufficient protection to a purchaser acting in good faith.[182] According to Art. 3 (1) lit. b and c, it is a prerequisite that the offender knows that the property is derived from one or more "offences established in accordance with subparagraph a)".[183] Furthermore, Art. 3 (1) lit. b (i) requires an intentional act.[184] At the same time, Art. 3 (3) states that "[k]nowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances."[185] This is not intended to change the substantive or formal requirements for the presentation of evidence as structured by the domestic law of each party. On the contrary, the Convention does not prevent such evidence.[186]

The wording of the Convention is largely based on U.S. criminal law.[187] Two important differences are, first, that ML under Art. 3 (1) lit. b and c relates exclusively to assets derived from drug offenses, and secondly, the Convention does not establish an obligation to

[179] Vienna Convention, 1988, Art. 3 (1) lit b.
[180] Ibid., Art. 3 (1) lit c (i).
[181] cf. Ibid., Art. 3 (1) lit. b-c.
[182] cf. Werner, 1996, p. 42; Vienna Convention, 1988, Art. 3 (1) lit c (i).
[183] Vienna Convention, 1988, Art. 3 (1) lit b (i), b (ii), c (i).
[184] cf. Ibid., Art. 3 (1) lit. b (i).
[185] Ibid., Art. 3 (3).
[186] cf. Werner, 1996, p. 43.
[187] cf. 18 USC § 1956, 2001; 18 USC § 1957, 2001.

substantiate reporting requirements for certain financial transactions, the circumvention of which is subject to sanctions.[188]

Pursuant to Art. 5 (2) of the Convention, parties shall take appropriate measures to assist their respective competent authorities in identifying, seizing, and confiscating the proceeds of, and property and instrumentalities derived from, drug trafficking. In this context, courts and authorities shall be allowed to request or even seize banking, financial and commercial records (Art. 5 (3)). It is important to note that under Art. 5 (3), banking secrecy should not be invoked in such cases, even if mutual legal assistance is provided for such investigations (Art. 7 (5)).[189]

United Nations Convention against Transnational Organized Crime 2000

The Palermo Convention is a legally binding multilateral treaty and the first binding international instrument in this area. It was adopted by the UN General Assembly in 2000 and entered into force in 2003 with the aim of enhancing cooperation among states preventing and combating transnational organized crime.[190]

The Palermo Convention expands the scope of proceeds beyond drug-related proceeds (Art. 2 lit. e). Article 6 (2) lit. a requires that the offense of ML be applied to the broadest possible list of predicate offenses. In any event, this means including all offenses punishable by a penalty of at least four years' imprisonment, as well as participation in organized criminal groups, corruption and obstruction of justice (Art. 6 (2) lit. b).[191] According to the relevant additional protocols, trafficking in human beings and smuggling of migrants also fall within this scope.[192]

With the exception of the predicate offenses, the requirements for the offense of ML are the same as under the Vienna Convention.

Unlike the Vienna Convention, the Palermo Convention does not limit the ML offense to the subject matter of the Convention. The fight against ML is no longer a means of fighting organized crime, but ML itself is a part of organized crime. Although the crimes to be created under this Convention are possible predicate offenses to ML, the mandatory inclusion in the

[188] cf. Werner, 1996, p. 42; Vienna Convention, 1988, Art. 3 (1) lit. b-c.
[189] cf. Vienna Convention, 1988, Art. 5 (2)-(3), 7 (5).
[190] cf. United Nations Office on Drugs and Crime (Palermo Convention), n.d.
[191] cf. Korejo, Rajamanickam & Said, 2021, pp. 729-730; Palermo Convention, 2000, Art. 2 lit. e, 6 (2) lit. a-b.
[192] cf. United Nations (Protocol against the Smuggling of Migrants), 2000; United Nations (Protocol to Prevent, Suppress and Punish Trafficking in Persons), 2000.

catalog of possible predicate offenses is based on the level of punishment (Art. 6 (2) lit. b). The higher weighting can also be derived from Art. 7 of the Palermo Convention.[193]

Another new feature compared to the Vienna Convention is the requirement to establish national AML systems. However, the specifications and requirements do not go beyond those of the European level or the FATF. In particular, the regulation and supervision of the financial sector and the creation of identification, documentation and suspicious activity reporting obligations are prescribed.[194] In this respect, the content of Art. 6 and 7 is largely based on the FATF Recommendations.[195] In particular, Art. 7 (3) refers to the FATF without explicitly mentioning it.[196]

The Palermo Convention is a comprehensive agreement that provides a framework for addressing issues related to ML and the proceeds of crime. However, the Convention has some shortcomings, for example, it is not clear what exactly constitutes a serious crime. Other gaps exist in relation to corruption and corruption offenses.[197]

United Nations Convention against Corruption 2003

The *United Nations Convention against Corruption*[198], also known as the Merida Convention, is also a legally binding multilateral treaty that was adopted by the UN General Assembly in 2003 and entered into force in 2005 (Art. 67).

The Merida Convention retains the concept of *predicate offense* from the previous Convention, but significantly expands the scope of ML offenses. In this context, any offense from which proceeds of ML offenses were obtained is considered a predicate offense. In addition, the Convention further expands the scope of ML by requiring states to include the widest possible range of predicate offenses, both within and outside the jurisdiction (Art. 2 lit. h, 23).

Furthermore, Art. 24 expands the offense to include the concealment or ongoing possession of property when the individual involved knows that the property is derived from any of the offenses covered by this Convention, without having participated in the predicate offense itself.

A further step in the fight against ML is the requirement in the Convention that states establish a holistic domestic regulatory and supervisory mechanism for both financial and

[193] cf. Scholz, 2020, p. 15; Palermo Convention, 2000, Art. 6 (2) lit. b, 7.
[194] cf. Pintaske, 2014, pp. 210-212.
[195] cf. McClean, 2007, pp. 71, 93-94; Palermo Convention, 2000, Art. 6-7.
[196] cf. McClean, 2007, p. 105; Palermo Convention, 2000, Art. 7 (3).
[197] cf. Korejo, Rajamanickam & Said, 2021, p. 731.
[198] United Nations Convention against Corruption, 2003.

non-financial institutions (Art. 14 (1) lit. a). Similarly, regional and bilateral cooperation, including cooperation among regulatory, law enforcement and judicial authorities, should be encouraged (Art. 14 (1) lit. b).

Despite the broadening of the scope of AML in this Convention, it does not contain relevant descriptions for the inclusion of the *all serious crimes* approach in the definition of ML offenses.[199]

3.1.2.3 United Nations Legal Instruments against Terrorist Financing

International Convention for the Suppression of the Financing of Terrorism 1999

The *International Convention for the Suppression of the Financing of Terrorism*[200] was adopted by the UN General Assembly in 1999 and entered into force in 2002. Its purpose is to facilitate the prosecution of persons accused of involvement in TF activities. This was prompted by a growing recognition of the importance of the financing of such activities and the potential involvement of apparently legitimate money transfers in the preparation of terrorist acts.[201] In this regard, Art. 2 (1) states:

"1. Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or

(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."[202]

The Convention defines the circumstances under which TF is punishable and is therefore one of the most important instruments in force to provide a definition of terrorism. In this regard, proven intent to facilitate the commission of a terrorist act may be prosecuted under

[199] cf. Korejo, Rajamanickam & Said, 2021, p. 731; United Nations Convention against Corruption, 2003, Art. 2 lit. h, 14 (1), 23-24, 67.
[200] International Convention for the Suppression of the Financing of Terrorism, 1999.
[201] cf. Klein, 2009, p. 1; International Convention for the Suppression of the Financing of Terrorism, 1999, Preamble.
[202] International Convention for the Suppression of the Financing of Terrorism, 1999, Art. 2 (1).

the Convention, even if the funds were not actually used to commit an act as defined in Art. 2 (1) (Art. 2 (3)). It is also an offense to attempt, organize, participate as an accomplice in or intentionally contribute to the commission of such acts (Art. 2 (4)-(5)). However, the Convention applies only to offenses involving a foreign element (Art. 3).

The Convention requires member states to establish the offenses referred to therein as criminal offenses under their domestic law and to provide for penalties commensurate with the gravity of the offenses (Art. 4). Unusually, the Convention makes both legal and natural persons liable, but not criminally liable, for the conduct covered by the Convention (Art. 5). The commission of such offenses cannot be justified by political, ideological, philosophical, racial, religious, ethnic or other similar considerations (Art. 6). To ensure effective prosecution, member states must establish jurisdiction over these crimes. In this regard, the Convention provides a particularly broad basis for jurisdiction (Art. 7). In addition to prosecuting the perpetrators, states parties must take appropriate measures to investigate, detect, and freeze or confiscate all funds used or made available for the commission of the aforementioned crimes, as well as the profits derived from such crimes, in order to enable their confiscation, if necessary (Art. 8).

Furthermore, it requires states to prosecute or extradite such persons to another state that has established jurisdiction to prosecute them (Art. 10). In this regard, several provisions are aimed at simplifying the process of extradition and mutual legal assistance between states (Art. 11-12).

In addition, the 1999 Convention requires member states to take various measures to increase the transparency of financial transactions and to improve the monitoring of financial transactions and flows (Art. 18).[203]

Resolution 1373 (2001)

Following the attacks of September 11, 2001, the UN Security Council adopted Resolution 1373[204] on September 28, 2001. The premise of Resolution 1373 was that any act of international terrorism is a threat to security and peace. Since under Chapter VII of the UN Charter the Security Council has the primary responsibility for dealing with threats to international security and peace, the Security Council assumed responsibility for all efforts to prevent international terrorism.

[203] cf. International Convention for the Suppression of the Financing of Terrorism, 1999, Art. 2 (1), (3)-(5), 3-8, 10-12, 18.
[204] Resolution 1373 (2001), 2001.

The Resolution imposed obligations on all states to criminalize the preparation, planning, support, financing, and execution of acts of international terrorism, to deny asylum to terrorists, and to freeze all assets related to international terrorism, among other important measures.

Resolution 1373 as a whole thus creates a unique framework of obligations that states are required to implement through both general legislation and enforcement measures. The special character of the Resolution, which distinguishes it from other Security Council Resolutions on international terrorism, is particularly evident in the combination of its general nature, its binding effect, and the exclusive procedure for its adoption.[205]

Because the Security Council has formulated its provisions in a binding, permanent, general and abstract manner, some have criticized the Council for engaging in legislative activity through Resolution 1373, the legality of which has at times been questioned under the Charter. Moreover, the Council has been criticized for its perceived bias in choosing to include certain aspects of the 1999 Convention regime in Resolution 1371 while excluding other elements. Ultimately, there has been a significant improvement in the global legal regime addressing the issue of TF.[206]

Resolution 1377 2001

Since no state met all the requirements of Resolution 1373, it placed an enormous burden, particularly on states with less capacity and resources.

As a result, in November 2001, the Security Council adopted Resolution 1377[207] with a statement recognizing the lack of capacity of some states to fully implement Resolution 1373, adopted earlier in the year, and declaring their need for assistance.

Resolution 1377 directed the Counter-Terrorism Committee to assist countries in addressing their capacity shortfalls related to Resolution 1373. The Counter-Terrorism Committee works with assistance providers to identify each country's priority needs and coordinates assistance programs to take advantage of synergies. Most countries needed assistance in drafting legislation and training personnel. To ensure that countries receive this assistance, regional and international institutions and organizations, as well as states in a position to help, were invited to assist members in implementing Resolution 1373. This underscores the

[205] cf. Husabø & Bruce, 2009, pp. 3-4; Resolution 1373 (2001), 2001.
[206] cf. Klein, 2009, p. 4.
[207] Resolution 1377 (2001), 2001.

objective of strengthening the capacity and importance of international cooperation to enable states to combat terrorism effectively.[208]

3.1.3 Egmont Group of Financial Intelligence Units

The Egmont Group of FIUs is an international network of national FIUs designed to promote the exchange of financial intelligence among its members and has become a central body for international cooperation in the fight against ML and TF. It was established in 1995 and now includes 167 FIUs from around the world.[209]

Financial Intelligence Units are specialized government agencies that receive, analyze, and disseminate suspicious activity reports (SARs)[210] and other financial intelligence from reporting entities, such as financial institutions. They also work with law enforcement and intelligence agencies to identify and investigate cases of ML and TF.[211]

The Egmont Group's activities include operating a secure platform that enables its member FIUs to exchange financial intelligence and information confidentially and securely, capacity building, technical assistance and training, including support for the establishment of new FIUs in countries that do not yet have them. It also organizes regular meetings and workshops where its member FIUs can discuss issues related to financial intelligence, ML and TF, providing an opportunity for member FIUs to share best practices and learn from each other.[212]

Finally, the Egmont Group works closely with other international organizations involved in the fight against ML and TF, such as the UNODC and the FATF.[213] This helps to ensure that the efforts of the various organizations are coordinated and complementary.

3.1.4 Organization for Economic Co-operation and Development

The OECD is an international organization that strives to develop effective policies that promote economic growth and development, as well as opportunity, equality and well-being for all, in order to improve people's lives.[214]

[208] cf. Ward, 2003, pp. 289, 300; Resolution 1377 (2001), 2001.
[209] cf. Fülbier, Aepfelbach & Langweg, 2006, § 5 Rec. 9; Egmont Group of Financial Intelligence Units (FAQs), n.d.
[210] Sometimes also referred to as suspicious transaction reports (STRs).
[211] cf. Egmont Group of Financial Intelligence Units (FIUs), n.d.
[212] cf. Egmont Group of Financial Intelligence Units (FAQs), n.d.
[213] see, for example, the Egmont Group and FATF joint publication on *Trade-Based Money Laundering - Trends and Developments* from December 2020 (cf. Financial Action Task Force/Egmont Group, 2020).
[214] cf. Castellano, De Bernardo & Punzo, 2023, pp. 141-144; Aydan, Bayin Donar & Arikan, 2022, pp. 436-437; Organization for Economic Cooperation and Development (About), n.d.

Within this framework, the OECD addresses economic crime, including tax fraud and corruption. In particular, the OECD has been instrumental in developing international standards for tax transparency and promoting the exchange of tax-related information between countries to help detect and prevent ML and tax evasion. The leading international body in this area is the Global Forum on Transparency and Exchange of Information for Tax Purposes.[215] In addition, the OECD conducts research and analysis and shares this information and related recommendations, such as the *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, published in 2019.[216]

Furthermore, the OECD's work to combat bribery, particularly through the *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* and its monitoring process, contributes to the fight against ML by targeting predicate offenses.[217] The Convention requires signatories to take measures to combat money laundered from bribery of foreign public officials and establishes a peer review system to ensure effective implementation of the OECD's anti-bribery instruments, including review of the effectiveness of AML systems.[218]

Another tool for reducing the risk of ML and TF is the Group of Twenty (G20) and OECD *G20/OECD Principles of Corporate Governance*, which provide guidelines for improving corporate governance practices. This, in turn, can enhance transparency and accountability in the financial sector.[219]

Additionally, the OECD is working with other international anti-financial crime organizations, such as the FATF, to improve cooperation between AML and tax authorities and to enhance the ability of governments to combat these crimes. In this regard, FATF member and observer countries and the OECD share experiences and conduct surveys on their activities in combating these criminal activities and on how AML and tax authorities can share and exchange information.[220]

3.1.5 Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision[221] is a committee of 45 member institutions from 28 jurisdictions around the world, established to strengthen global financial stability

[215] cf. Organization for Economic Cooperation and Development (Global Forum), n.d.
[216] cf. Organization for Economic Cooperation and Development, 2019.
[217] cf. Organization for Economic Cooperation and Development, 1997.
[218] cf. Financial Action Task Force (OECD), n.d.
[219] cf. Amonovna & Feruzbek, 2023, p. 539; Organization for Economic Cooperation and Development, 2015.
[220] cf. Financial Action Task Force (OECD), n.d.
[221] Initially named the Committee on Banking Regulations and Supervisory Practices (cf. Bank for International Settlements, n.d.).

and the integrity of the international banking system, and to enhance cooperation among its members.[222]

The 1988 Basel Committee's Statement on the *Prevention of criminal use of the banking system for the purpose of money-laundering* provides that credit institutions generally refrain from transactions with a criminal background and contribute to the detection and combating of such transactions. According to the Committee, banking supervisors must prevent the misuse of the banking system for illicit purposes in order to ensure public confidence in banks and thus their stability. Supervisors should therefore promote ethical principles among banks and other financial institutions.[223]

The Committee has established a number of international standards for banking supervision. Of particular importance in this context are the capital adequacy accords, commonly known as Basel I, Basel II and Basel III.[224]

3.1.6 International Monetary Fund

As a collaborative institution, the International Monetary Fund makes an important contribution to the international fight against ML and TF. The Fund facilitates the international exchange of information, the development of common approaches, and the promotion of necessary standards and policies. In addition, the International Monetary Fund assesses countries' compliance with international AML and CFT standards and develops programs to help members address deficiencies.

The current focus of work is on the above assessments, policy development, and technical assistance. Any assessment of compliance with the FATF 40 Recommendations and the FATF IX Special Recommendations conducted under the Financial Sector Assessment Program and the Offshore Financial Centers Program must include an evaluation of each country's AML and CFT regime. These assessments are based on an agreed methodology, which is also used by the FATF and the World Bank in their assessments.

In this context, the near-universal membership of the International Monetary Fund and its extensive experience in conducting financial sector assessments, monitoring member economies, and providing technical assistance are an advantage.[225]

[222] cf. Bank for International Settlements, n.d.
[223] cf. Bank for International Settlements, 1988.
[224] cf. Bank for International Settlements, n.d.
[225] cf. Hunter & Biglaiser, 2022, p. 505; International Monetary Fund, n.d.

3.1.7 World Bank Group

The World Bank Group is made up of five institutions that promote prosperity and sustainable development. It is one of the world's largest sources of financing and knowledge for developing countries. Two of the institutions are the International Bank for Reconstruction and Development and the International Development Association, which together make up the World Bank. The World Bank provides financing, technical assistance, and policy advice to developing countries. While the International Development Association focuses on the poorest countries, the International Bank for Reconstruction and Development assists middle-income or creditworthy poorer countries.[226]

As part of its work, the World Bank also addresses ML and TF issues. For example, the Financial Integrity unit helps countries build capacity and capability to detect, prosecute, and prevent criminal financial flows to strengthen the integrity of the financial system. Its three main areas of responsibility are technical assistance through knowledge products, training, and practical tools; policy development; and in-country AML and CFT regulatory assessments. The latter are used to assess the effectiveness of regulations and identify potential risks, which in turn determine the need for technical assistance and policy development.

Cooperation exists both with the authorities responsible for combating ML and TF in the client countries and with regional organizations or civil society organizations. At the international level, the unit works with the FATF, the OECD, the Egmont Group and the UNODC, among others. Of particular note is the partnership between the World Bank Group and the UNODC, the Stolen Asset Recovery Initiative, which was established to promote international cooperation with developing countries and financial centers and to eliminate safe havens for corrupt funds.[227]

3.2 United States Instruments

The U.S. plays a significant role in the international fight against ML and TF because of its leading role in the global economy, including the financial market that can be used for illicit purposes. Additionally, the U.S. has a long history of enacting legislation and implementing regulatory measures to combat ML and TF. The U.S. approach, unlike, for example, the German approach, has therefore already been the subject of a wide range of academic studies, both in the United States and internationally, including some comparative law

[226] cf. World Bank (Who we are), n.d.
[227] cf. World Bank (Financial Integrity), n.d.

studies. The consideration of U.S. instruments thus promotes a more global perspective on AML and CFT.[228]

3.2.1 United States Institutions

Department of the Treasury

In the United States, the U.S. Department of the Treasury is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States. The Department works with governments and financial institutions around the world. Its sanctions and AML programs play a critical role in the U.S. government's overall efforts to combat illicit finance and protect the integrity of the financial system.[229]

The Treasury Department's Office of Terrorism and Financial Intelligence develops and implements the U.S. strategy for combating ML and TF at home and abroad. It consolidates the Treasury Department's intelligence and enforcement functions to both protect the financial system from illicit use and to combat national security threats such as money launderers and terrorists.[230]

Furthermore, the Office of Terrorism and Financial Intelligence oversees several component offices and bureaus, such as the Office of Foreign Assets Control, which administers and enforces trade and economic sanctions against designated countries, regimes, and individuals that pose a threat to the national security, economy, or foreign policy of the United States. Sanctions are based on U.S. foreign policy and national security objectives.[231]

In addition, the Financial Crimes Enforcement Network is responsible for promoting global information sharing and assisting international partners in the fight against ML and TF. Among other things, the U.S. FIU responds to requests from foreign FIUs and acts as a liaison between them and domestic law enforcement agencies. Moreover, the Financial Crimes Enforcement Network provides strategic products to law enforcement and FIUs on issues of international concern and works with foreign governments to combat transnational crime.[232]

The Terrorist Finance Tracking Program (TFTP) was established after the September 11 terrorist attacks to identify and track terrorists and their networks. By identifying illicit

[228] cf. Groth, 2016, pp. 151-152.
[229] cf. United States Department of the Treasury (Role of the Treasury), n.d.
[230] cf. United States Department of the Treasury (Terrorism and Financial Intelligence), n.d.
[231] cf. Preble & Early, 2023, pp. 1, 19-20; United States Department of the Treasury (OFAC), n.d.
[232] cf. Financial Crimes Enforcement Network (International Programs), n.d.

financial flows and terrorists, the U.S. Treasury Department helps track terrorist networks at home and abroad.[233]

The EU-US TFTP Agreement[234] was concluded in 2010 and covers the exchange of financial information for the purpose of detecting and tracing TF.[235]

Department of Justice

As the principal enforcer of federal laws, the Department of Justice plays a key role in the fight against financial crime by ensuring public safety, upholding the rule of law, and protecting civil rights.[236]

Among other things, Department of Justice's law enforcement agencies such as the Drug Enforcement Administration and the Federal Bureau of Investigation (FBI) play an important role in the fight against financial crime. As for the FBI, one of its top priorities is to prevent terrorist attacks in the United States, and its AML efforts are housed in the Money Laundering, Forfeiture, and Bank Fraud Unit of the Criminal Investigative Division.[237]

The Department of Justice's Money Laundering and Asset Recovery Section is responsible for overseeing the Department's AML and asset forfeiture efforts. Its role includes the prosecution and coordination of complex, sensitive ML and asset forfeiture investigations and litigation across multiple districts and international borders. The Money Laundering and Asset Recovery Section also provides policy and legal support and conducts training programs for local, state, and federal prosecutors and law enforcement officials, as well as for foreign governments, and assists departmental and interagency policymakers in formulating and evaluating regulatory, legislative, and policy initiatives. Additionally, the Money Laundering and Asset Recovery Section overseas the Department's Asset Forfeiture Program, which includes the distribution of forfeited assets and funds to appropriate domestic and foreign law enforcement agencies and community groups in the United States. Furthermore, it is responsible for deciding petitions for remission or mitigation of forfeited assets.[238]

[233] cf. United States Department of the Treasury (TFTP), n.d.
[234] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 2010.
[235] cf. Groth, 2016, p. 161.
[236] cf. United States Department of Justice (Our Work), n.d.
[237] cf. Lindsay, 2023, p. 167; United States Department of Justice (Agencies), n.d.
[238] cf. United States Department of Justice (MLARS), n.d.

3.2.2 United States Legal Instruments

The primary AML and CFT laws are the *Currency and Foreign Transactions Reporting Act* of 1970, commonly referred to as the Bank Secrecy Act (BSA), and the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001,* which are discussed below.[239]

Bank Secrecy Act

The BSA[240] is a federal law in the U.S. that imposes compliance obligations on financial institutions operating in the United States.[241] It is administered by the Financial Crimes Enforcement Network, which describes it as one of the most important tools in the fight against ML and TF.

The purpose of the BSA is to facilitate the detection of the origin, quantity, and movement of currency and other financial instruments transported, transmitted, deposited, or withdrawn within the U.S. or through financial institutions. It requires banks, other financial institutions, and individuals to report suspicious financial transactions and maintain records of such transactions to assist law enforcement in detecting and investigating ML and TF.

Specifically, banks are required to report currency transactions above a certain threshold by filing a Currency Transaction Report. The threshold for reporting currency transactions is currently set at USD 10,000. Furthermore, customer due diligence is required to properly identify all persons conducting transactions. In addition, financial institutions are required to maintain records of certain financial transactions by maintaining appropriate documentation.

To date, several laws have been enacted to amend and expand the BSA to provide regulators and law enforcement with the most effective tools against ML and TF.[242]

[239] Other relevant legislation, which will not be discussed further in this paper, includes: Money Laundering Control Act (1986), Anti-Drug Abuse Act (1988), Annunzio-Wylie Anti-Money Laundering Act (1992), Money Laundering Suppression Act (1994), Money Laundering and Financial Crimes Strategy Act (1998), Suppression of the Financing of Terrorism Convention Implementation Act (2002), Intelligence Reform and Terrorism Prevention Act (2004), Anti-Money Laundering Act (2020).
[240] Currency and Foreign Transactions Reporting Act (Bank Secrecy Act), 1970.
[241] cf. Financial Crimes Enforcement Network (Bank Secrecy Act), n.d.
[242] cf. Financial Crimes Enforcement Network (History), n.d.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001

In the wake of the September 11, 2001 terrorist attacks, the USA PATRIOT Act[243] was passed in October 2001.

The USA PATRIOT Act criminalizes TF, increases civil and criminal penalties for ML, and strengthens customer identification procedures, which expands the existing BSA framework. It also extends AML program requirements to all financial institutions and requires financial institutions to implement due diligence procedures. Enhanced due diligence procedures apply to foreign correspondent and private bank accounts, and financial institutions are prohibited from doing business with foreign shell banks. Moreover, the U.S. government and financial institutions are required to exchange and share information, and the Secretary of the Treasury is authorized to impose special measures against countries, institutions, and transactions of particular ML significance. Additionally, access to records has been facilitated and banks are required to respond to government requests for information within 120 hours. When reviewing applications for business combinations, such as bank mergers or acquisitions, the banking agencies must consider a bank's AML record.[244]

The terrorist attacks of September 11 generally favored greater acceptance of, or justification for, possible relatively far-reaching restrictions on individual rights implied by measures to combat TF and other terrorist activities, such as the expansion of government powers.[245] In the literature, this impairment of individual rights by the USA PATRIOT Act is criticized, as are numerous individual aspects such as the designation of terrorist organizations.[246] Moreover, there is criticism that investigative powers can also reduce the overall effectiveness of the pursuit of security interests when suspicions are low.[247] In 2004, a federal court ruled that parts of the USA PATRIOT Act relating to private actors' obligations to provide data were unconstitutional.[248]

On the positive side, it is argued that the USA PATRIOT Act has provided the homeland security, law enforcement, and intelligence with the tools, guidance, and resources to prevent

[243] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 2001.
[244] cf. Financial Crimes Enforcement Network (History), n.d.
[245] cf. Duncan Jr., 2004, pp. 1-3.
[246] cf. Syring, 2012, pp. 600-605.
[247] cf. Macdonald, 2009, pp. 528-529.
[248] cf. Groth, 2016, p. 385.

another attack similar to September 11 and that, while in need of some revision, it is a successful combination of principles and technical capabilities to protect democracy.[249]

3.3 European and European Union Instruments

Europe and the EU also play an important role in the global fight against ML and TF. The EU, in particular, has developed a comprehensive framework of instruments and regulations to combat ML and TF. This chapter examines European and EU instruments and considers their impact on AML and CFT.

3.3.1 European and EU Institutions

European Parliament

The European Parliament plays a crucial role in the fight against ML and TF. It is the law-making body of the EU, with legislative, budgetary and supervisory powers, and is directly elected every five years by EU citizens who are eligible to vote. In its legislative role, the European Parliament is responsible for adopting EU laws, deciding on enlargements and international agreements, scrutinizing the European Commission's strategic agenda and calling on the Commission to propose legislation. In its supervisory role, it has the power to elect the President of the Commission and to approve the Commission as a body, to exercise democratic control over the EU institutions and to grant discharge. Furthermore, it initiates inquiries and considers citizens' petitions, observes elections, debates with the European Central Bank on monetary policy, and questions the European Council and the Commission. With regard to the third main role, the Parliament draws up the EU budget and approves its long-term budget.[250]

One of the key examples of the European Parliament's role in AML and CFT efforts is the development and adoption of the AMLDs. These Directives establish a harmonized and comprehensive set of measures to prevent the financial system from being misused for illicit purposes. In addition, the implementation of the FATF Recommendations, by incorporating them into EU legislation, ensures a consistent approach to combating financial crime in all member states.[251]

European Commission

The European Commission assesses risks to identify and respond to threats to the EU. It supports the adoption of global solutions to respond to these threats at the international level.

[249] cf. Dinh, 2004, pp. 462, 466-467.
[250] cf. European Union (Parliament), n.d.
[251] cf. European Commission, n.d.

The Commission also ensures that the EU's AML and CFT legislation is effectively implemented, by monitoring compliance with EU rules and working with the relevant authorities.[252] In 2017, it established the EU Global Facility on Anti-Money Laundering and Countering the Financing of Terrorism as a tool to provide assistance to third countries when needed due to deficiencies in their AML and CFT regulations.[253]

Recent developments[254] by the European Commission include the publication of an action plan in May 2020[255] for a comprehensive EU policy to prevent ML and TF based on six pillars. Measures of particular interest include the establishment of a single EU AML and CFT regulatory framework and EU-level AML and CFT supervision.[256] The action plan was adopted by the European Parliament in July 2020.[257]

As a result, in July 2021, the European Commission proposed a comprehensive legislative package to strengthen the EU's AML and CFT regime. It aims to protect the EU financial system and citizens from ML and TF by strengthening the identification of suspicious activities and transactions and closing the loopholes used by criminals. Specifically, the package proposes the creation of a new EU Anti-Money Laundering Authority; a new regulation on AML and CFT, including customer due diligence, beneficial ownership and EU-wide cash limits; a Sixth AMLD, including rules on national FIUs and national supervisors; and a revision of Regulation 2015/847/EU[258] to allow for the traceability of crypto-asset transfers.[259]

European Council

The European Council is a key EU body that brings together the leaders of the EU member states to decide on the EU's political direction and priorities within the EU's political agenda. It also deals with certain issues that need to be resolved at the highest level of intergovernmental cooperation between EU member states and defines the EU's common security and foreign policy. Additionally, the European Council is responsible for

[252] cf. European Commission, n.d.
[253] cf. European Union AML/CFT Global Facility, n.d.
[254] The *Communication entitled 'Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework'* (2019), the *report assessing whether Member States have duly identified and made subject to the obligations of Directive (EU) 2015/849 all trusts and similar legal arrangements governed under their laws* (2020), and the *trainers' manual and its corresponding user's manual* (2022) will not be considered further in the context of this work (cf. European Commission, n.d.).
[255] cf. European Commission (Communication from the Commission), 2020.
[256] cf. European Commission (Action plan), 2020.
[257] cf. European Parliament, 2020.
[258] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (Document 32015R0847), 2015.
[259] cf. European Commission, 2021.

nominating and appointing candidates for certain high-level EU posts. However, the European Council has no legislative powers.[260]

In 2019, the European Council adopted the Strategic Agenda 2019-2024, which sets the framework for the work of the institutions to protect citizens' way of life and promote their interests, societies and businesses. Its main priorities are the protection of citizens and freedoms, the development of a strong and dynamic economic base, the creation of a climate-neutral, social and fair Europe, and the promotion of European values and interests at the global level. Within this framework, particular emphasis is placed on the fight against cross-border crime and terrorism by strengthening common instruments, information exchange and cooperation.[261]

Council of the European Union

The Council of the EU is made up of government ministers from each EU member state and acts as the voice of those states. The ministers meet regularly to discuss, amend and adopt of EU laws and to coordinate EU policies. The Council works closely with the European Parliament, and together they are the main decision-makers in the EU. Together with the EU Parliament, the Council of the EU is responsible for negotiating and adopting EU laws proposed by the European Commission and approving the EU's annual budget. Moreover, the Council develops the EU's security and foreign policy based on guidelines from the European Council, coordinates EU policies, and concludes agreements on behalf of the EU with other states or organizations.[262]

For example, in 2019, the Council of the EU set strategic priorities in the context of further AML and CFT reforms in response to the European Council's Strategic Agenda 2019-2024. In 2020, the Council discussed the Commission's plans to strengthen its efforts to combat ML and TF, committed to supporting further coordination and oversight at the EU level, and adopted conclusions to guide the European Commission's future legislative proposals. Later, in June 2022, the Council of the EU published the agreement on its partial position on the new Anti-Money Laundering Authority proposed by the Commission as part of the 2021 legislative package. More recently, in December 2022, the Council agreed its position on a new AML and CFT directive and regulation, including the extension of its application to the

[260] cf. European Council, n.d.
[261] cf. European Council, 2019.
[262] cf. European Union (Council), n.d.

entire crypto sector, and in May 2023 adopted rules to make crypto-asset transfers traceable.[263]

Council of Europe

Through its role as a pan-European political organization, the Council of Europe offers a unique added value in supporting reforms related to corruption, ML and TF. In this context, the Council has a three-pronged approach to combating these crimes: It sets standards in the form of treaty law and soft law instruments, provides technical assistance and support to address gaps in the legal and institutional framework, and promotes capacity building through its Economic Crime Co-operation Unit. Furthermore, it monitors compliance with these standards through monitoring mechanisms such as the Group of States against Corruption, also referred to as GRECO, and the Committee of Experts on the Evaluation of Anti-Money Laundering and the Financing of Terrorism (MONEYVAL).[264]

MONEYVAL uses a dynamic methodology, including peer reviews, peer evaluations and regular follow-up, to make recommendations to national authorities to improve their systems and strengthen their capacity to effectively combat ML and TF. The MONEYVAL Statute was adopted in 2010, making it an independent monitoring mechanism within the Council of Europe, reporting directly to the Committee of Ministers, and further amended in 2013 and 2017. By monitoring and improving national AML and CFT efforts, MONEYVAL contributes to maintaining the integrity of the financial system and fighting crime.[265]

European Banking Federation

With regard to the European banking sector in particular, the European Banking Federation (EBF) is actively involved in the fight against financial crime in order to protect the stability and integrity of the international financial system. It brings together several European national banking associations.

The EBF has reviewed the EU's AML and CFT regulatory framework and identified four specific areas for improvement: harmonization of the framework, better and more efficient cooperation, use of effective tools and new technologies, and strengthening of the relevant EU bodies, including strengthening the role of the European Banking Authority (EBA) and better coordination of the relevant supervisory authorities. In March 2020, the EBF published a proposal of 20 recommendations based on these suggestions for improvement.

[263] cf. European Council (Timeline), 2023.
[264] cf. Council of Europe (Economic Crime and Cooperation Division), n.d.
[265] cf. Council of Europe (MONEYVAL), n.d.

Additionally, the EBF is a member of the Global Coalition to Fight Financial Crime and the European Police Office (Europol) Financial Intelligence Public-Private Partnership.[266]

European Banking Authority

The EBA is the EU financial supervisory authority responsible for ensuring the integrity, orderly functioning and transparency of financial markets and for preventing the use of the financial system for ML and TF.

To achieve this objective, the EBA carries out various activities, such as developing and supporting the implementation of effective policies to combat ML and TF, promoting close cooperation and exchange of information between all competent authorities and financial institutions in the EU, and monitoring the implementation of EU AML and CFT standards and policies.

The EBA follows a risk-based approach and aims to achieve consistent results in the fight against ML and TF.[267]

Europol

Europol, the EU's law enforcement agency, has a significant impact on the fight against ML and TF. It unites the four centers: European Serious and Organised Crime Centre, European Cybercrime Centre, European Counter Terrorism Centre and European Financial and Economic Crime Centre.[268]

Specifically, the European Counter Terrorism Centre was established in 2016, following a series of terrorist attacks in Europe in 2015, as an operations center and center of expertise to promote EU-level cooperation in national counter-terrorism efforts and to provide a comprehensive response to terrorism in the EU. It is the first center of its kind to be established under the EU Security Policy to combat terrorism and develops counter-terrorism tools in line with new requirements and facilitates the networking of relevant authorities and the exchange of information and intelligence between EU member states. Its main task is to provide tailored operational support to counter-terrorism authorities. In order to meet these requirements, the European Counter Terrorism Centre includes, among others, the Counter Terrorism Joint Liaison Team, which serves as a platform for the rapid exchange of

[266] cf. European Banking Federation (Tackling Financial Crime), n.d.
[267] cf. European Banking Authority, n.d.
[268] cf. European Union Agency for Law Enforcement Cooperation (Centres), n.d.

information and intelligence, and the Counter Terrorism Program Board, which serves as a steering instrument among the member states.[269]

The European Financial and Economic Crime Centre was established in 2020 to combat threats such as ML, corruption, counterfeiting, fraud and tax evasion, and to improve the confiscation of criminal assets. It combats and prevents financial and economic crime in the EU by conducting financial investigations and seizing assets, cooperating with public and private bodies, and assisting law enforcement authorities in the field of international financial crime. Moreover, the European Financial and Economic Crime Centre manages the Europol Financial Intelligence Public-Private Partnership, the first transnational information exchange mechanism ever established in the field of combating ML and TF.[270]

In general, Europol plays an important role in the fight against ML by providing intelligence and forensic support to member states. Among other things, the Europol Criminal Assets Bureau assists in tracing the proceeds of crime worldwide when assets have been hidden outside their jurisdiction. The Europol Criminal Assets Bureau also houses the secretariat of the Camden Asset Recovery Inter-Agency Network, which focuses on the recovery of criminal proceeds. Finally, the Financial Crime Information Center provides a secure web platform for law enforcement, and the European Multidisciplinary Platform Against Criminal Threats provides an integrated approach to EU internal security with a focus on financial crime.[271]

3.3.2 European and EU Legal Instruments

The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime

The 1990 Strasbourg Convention of the Council of Europe largely incorporates the ML provisions of the FATF Recommendations, without explicitly referring to them, and removes the link between ML and drug-related crime (Art. 1 lit. e in conjunction with Art. 6 (4) and also proposes to the signatory states to criminalize negligent ML (Art. 6 (3) lit. a).

Initially, the Convention does not limit the range of predicate offenses that can lead to ML charges, but Art. 6 (4) allows signatory states to limit this range independently by means of a reservation. Thus, the Convention adopts the FATF recommendation to separate ML from drug-related offenses, but goes beyond it in its specific wording. The Convention's scope of

[269] cf. European Union Agency for Law Enforcement Cooperation (ECTC), 2023.
[270] cf. European Union Agency for Law Enforcement Cooperation (EFECC), 2023.
[271] cf. European Union Agency for Law Enforcement Cooperation (Money Laundering), n.d.; European Union Agency for Law Enforcement Cooperation, 2022.

ML offenses is broad, while the proposal to criminalize negligent ML is not further elaborated and relies on the evidence facilitation of the Vienna Convention on Narcotic Drugs.

With regard to the measures to be taken at the national level, Art. 3 contains a general obligation to enable the identification of property subject to confiscation and to prevent any further processing of such property.

Article 4 (1) also requires each party to provide for the power of authorities or courts to order the provision or seizure of financial, banking and commercial documents for the purposes of the measures referred to in Art. 2-3, whereby banking secrecy shall not constitute an obstacle to the execution of such measures. Furthermore, pursuant to Art. 4 (2), the use of investigative methods that facilitate the detection of proceeds and the gathering of evidence in this regard shall be made possible.[272]

Council Directive 91/308/EEC of 10 June 1991

The First EU AMLD is based on the requirements of the Vienna Convention and the Strasbourg Convention and obliges the signatory states to transpose them into national law. The specifications for a national criminal offense of ML (Art. 1 third indent) are based on the above-mentioned international legal instruments.[273]

Although, according to the prevailing view, the European Community did not have the power to set binding minimum standards in the area of criminal law at the time of adoption (see now Art. 83 of the Treaty on the Functioning of the European Union (TFEU)[274]), the prohibition of ML was based on the power to harmonize laws in order to harmonize the internal market (see now Art. 114 TFEU).[275]

The Directive refers to Art. 3 (1) lit. a of the Vienna Convention[276] on predicate offenses, but extends it to "any other criminal activity designated as such for the purposes of this Directive by each Member State".[277] Although the Directive does not link ML to drug-related crime or other specific forms of organized crime and leaves member states free to define the range of predicate offenses as they see fit, it explicitly states that the scope is intended to be broader than that of the Vienna Convention. In this sense, the Directive corresponds to the Strasbourg Convention.

[272] cf. Strasbourg Convention, 1990, Art. 1 lit. e, 2-4, 6 (3) lit. a, (4); Council of Europe, 1990, pp. 7-10.
[273] cf. Document 31991L0308, 1991, Art. 1 third indent.
[274] cf. Treaty on the Functioning of the European Union (Document 12012E/TXT), 2012, Art. 83.
[275] cf. Ibid., Art. 114.
[276] cf. Vienna Convention, 1988, Art. 3 (1) lit. a.
[277] Document 31991L0308, 1991, Art. 1 ninth indent.

In contrast to the FATF Recommendations, negligent ML is not included in the requirements.

The specifications regarding the potential precursors of ML are as imprecise as those regarding the recipients of the economic regulatory obligations to combat ML. Article 12 leaves it to national legislators to impose additional AML requirements on professions and categories of businesses.

In Art. 3-11, the Directive essentially follows the relevant FATF Recommendations. Of particular importance is the obligation to report suspicious ML transactions set out in Art. 6 (1) first indent.[278]

Council Framework Decision of 26 June 2001[279] (2001/500/JHA)

In 2001, the Council of the EU adopted Framework Decision 2001/500/JHA with reference to the Strasbourg Convention. In particular, this Decision limits the possibility of reservations within the EU with respect to Art. 2 and 6 of the Strasbourg Convention (Art. 1). In this context, Art. 1 lit. b of the Framework Decision explicitly adds serious crimes to the list of predicate offenses for ML. This categorization includes offenses punishable by deprivation of liberty for a maximum of more than one year or a minimum of more than six months.[280]

Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001[281]

The EU's Second AMLD supplements the First AMLD by expanding the range of possible predicate offenses for ML to include activities of criminal organizations, corruption, serious fraud, and other high-yield offenses that are severely punished under national law. These offenses, together with the narcotics offenses of Art. 3 (1) lit. a of the Vienna Convention, constitute the concept of serious crimes under Art. 1 No. 1 (E).

The scope of persons subject to AML supervision is also expanded. The term *financial institution* is extended to include bureaux de change and investment firms (Art. 1 No. 1 (B)), and non-financial entities such as legal professionals, tax advisors, real estate agents, casinos and persons dealing in high-value goods are included (Art. 1 No. 2).

[278] cf. Document 31991L0308, 1991, Art. 3-12; Scholz, 2020, pp. 13-14.
[279] Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA) (Document 32001F0500), 2001.
[280] cf. Document 32001F0500, 2001, Art. 1; Strasbourg Convention, 1990, Art. 2, 6.
[281] Document 32001L0097, 2001.

The further differentiation of the requirements for the prevention obligations with regard to the extended group of addressees is set out in Art. 1 Nos. 3-10.[282]

Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)[283]

The *Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)* is a key legal instrument aimed at harmonizing the definition, penalties and prosecution of terrorism-related offenses throughout the EU. The definition of terrorist offenses includes acts committed with the intent of "seriously intimidating a population, or unduly compelling a Government or international organisation to perform or abstain from performing an act, or seriously destabilising or destroying the fundamental political, constitutional, economic, or social structures of a country or an international organization".[284]

Article 5 of the Framework Decision establishes minimum penalties for terrorist offenses. For example, the penalty for directing a terrorist group is at least 15 years' imprisonment, while the penalty for participating in the activities of a terrorist group is at least eight years' imprisonment. Furthermore, the Framework Decision establishes rules of jurisdiction for the prosecution of terrorist offenses (Art. 9), such as when the offense is committed on their territory (Art. 9 (1) lit. a), when it is committed by one of their nationals (Art. 9 (1) lit. c), or when it is committed against their nationals or institutions (Art. 9 (1) lit. e), in order to prevent safe havens for terrorists and to ensure effective prosecution of terrorism-related offenses. In addition, Art. 10 requires member states to ensure that victims of terrorism have access to support services and are provided with information on their rights and available assistance.[285]

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism[286]

The *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism*, or the Warsaw Convention, adds

[282] cf. Document 32001L0097, 2001, Art. 1 Nos. 1-10; Vienna Convention, 1988, Art. 3 (1) lit. a; Later in 2001, *Council Regulation (EC) No. 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism* was adopted, which will not be discussed further in this dissertation as it focuses on specific restrictive measures rather than providing a comprehensive framework for combating terrorist financing.
[283] Document 32002F0475, 2002.
[284] Ibid., Art. 1 (1).
[285] cf. Ibid., Art. 5, 9-10.
[286] Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention), 2005.

procedural measures in Art. 9 (5)-(7) to the offenses, which are essentially taken from the Vienna and the Strasbourg Conventions. These measures are intended to ensure effective prosecution of ML.[287] Moreover, this instrument seeks to expand the scope of the Strasbourg Convention to include TF and is thus a useful complement to the 1999 *International Convention for the Suppression of the Financing of Terrorism*.[288]

Signatory states undertake to ensure that a previous conviction of a third party for the principal offense is not a prerequisite for a conviction for ML (Art. 9 (5)). In addition, criminal liability for ML will not require that the illegally obtained assets be attributable to a specific predicate offense (Art. 9 (6)), and acts committed abroad may also be considered predicate offenses for ML, provided that they constitute an offense abroad and are considered predicate offenses under national law (Art. 9 (7)).[289]

Furthermore, the proposal to criminalize negligent ML is included in Art. 9 (3) lit. b. However, the explanatory report to the Convention explicitly justifies this proposal by stating that the recognizing court may infer negligence from objective circumstances at trial.[290]

Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005[291]

The Third EU AMLD introduced a number of new provisions in response to the threat that ML poses to the integrity, solidarity and stability of financial and credit institutions and to confidence in the financial system (Rec. 2).

In addition to the fight against ML, the Directive also includes the fight against TF as an objective (Art. 1 (1)).[292] Terrorist financing is defined in Art. 1 (4) as "the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism".[293] In this context, the scope of predicate offenses to ML was expanded in Art. 3 (5) lit. a and lit. f to include terrorist acts

[287] cf. Warsaw Convention, 2005, Art 9 (5)-(7); Council of Europe, 2005, pp. 16-17.
[288] cf. Klein, 2009, p. 5.
[289] cf. Warsaw Convention, 2005, Art 9 (5)-(7).
[290] cf. Warsaw Convention, 2005, Art 9 (3) lit. b; Council of Europe, 2005, p. 16.
[291] Document 32005L0060, 2005.
[292] cf. Ibid, Art. 1 (1), Rec. 2.
[293] Ibid, Art. 1 (4).

and crimes punishable by imprisonment for a minimum of more than six months or a maximum of more than one year under national law.

Most of the changes relate to the requirements for preventive duties, which are now structured on a risk-based basis (Rec. 22). Accordingly, several passages, such as Art. 8 (1) lit. b, (2), Art. 9 (6) and Art. 13 (1), (4) lit. a, contain the terms *risk-based* or *risk-sensitive*.

The customer due diligence requirements are expanded to include the identification of the beneficial owner (Art. 8 (1) lit. b).[294] Article 3 (6) defines the beneficial owner as "the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted".[295]

As part of the enhanced due diligence requirements, politically exposed persons have also been introduced as a risk category in support of international anti-corruption efforts (see Rec. 25).[296] Politically exposed persons are defined in Art. 3 (8) as "natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons".[297]

In addition, Chapter V, Section 1, describes in more detail the requirements for internal procedures, training and feedback (Art. 34-35).[298] Similarly, Art. 39 (1) specifies the obligation to impose sanctions for violations of AML requirements, which must be "effective, proportionate and dissuasive".[299]

The role of private actors in the prevention of criminal activity is being redefined by the EU's Third AMLD. The risk-based approach is intended to provide more flexibility for obligated parties in this context.[300] However, the implementation of this approach is accompanied by new responsibilities, as terms such as risk-sensitive have to be defined independently by the obligated parties. At the same time, the requirements for a national prevention system also include sanctions that penalize failure to take appropriate responsibility.[301]

In this context, the importance of the *Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the member states in*

[294] cf. Document 32005L0060, 2005, Rec. 22, Art. 3 (5) lit. a, f, Art. 8 (1) lit. b, (2), Art. 9 (6), Art. 13 (1), (4) lit. a.
[295] Ibid., Art. 3 (6).
[296] cf. Document 32005L0060, 2005, Rec. 25.
[297] Ibid., Art. 3 (8).
[298] cf. Ibid., Art. 34-35.
[299] Ibid., Art. 39 (1).
[300] cf. Ibid., Rec. 47.
[301] cf. Scholz, 2020, pp. 17-18.

respect of exchanging information[302] for the development of the Third AMLD should be mentioned. Immediately prior to the adoption of the Third AMLD, *Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offenses*[303] was also adopted.

In 2006, an Implementing Directive to the Third AMLD[304] was adopted, setting out technical criteria for simplified due diligence requirements and exemptions from them, as well as a more precise definition of politically exposed persons.[305]

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006[306]

The 2006 Regulation of the European Parliament and the Council of the EU on information on the payer accompanying transfers of funds is binding in its entirety and directly applicable in all member states (Art. 20).

The Regulation highlights the threat to society and the financial system posed by the concealment of illicit funds and the financing of terrorist activities (Rec. 1). It therefore specifies the information to be provided to the payer for the purposes of preventing, investigating and detecting ML and TF (Art. 1). Money laundering is defined as any act which, when committed intentionally, constitutes ML within the meaning of Art. 1 (2) or (3) of the Third AMLD (Art. 1 (1) No. 2).

Full traceability of transfers of funds is extremely important and helpful in the fight against ML or TF under the Regulation. In order to ensure the smooth processing of information on the payer during the payment transaction, a system should be put in place requiring the payer's payment service providers to provide accurate and meaningful information on the payer when transferring funds (Rec. 6).

In this context, Art. 4 of the Regulation contains the full information on the payer, which includes the name, address and account number (Art. 4 (1)). The address may be replaced by the payer's date and place of birth, customer number or national identity number (Art. 4

[302] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the member states in respect of exchanging information (2000/642/JHA), 2000.
[303] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, 2005.
[304] Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis, 2006.
[305] cf. Groth, 2016, pp. 155-156.
[306] Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds (Document 32006R1781), 2006.

(2)). If the payer does not have an account number, the payer's payment service provider shall replace it by a customer identification number allowing the transaction to be traced back to the payer (Art. 4 (3)).[307]

Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015[308]

Regulation (EU) 2015/847 aims to prevent, detect and investigate ML and TF by improving the traceability of funds transferred within and outside the EU.

The main elements of the Regulation include the obligations of the payer's payment service provider to obtain and send information on the payer and the payee, such as name and account number (Art. 4-6). In addition, the obligations of the payee's payment service provider and of intermediary payment service providers are described, such as verification and detection of missing information on the payer or the payee (Art. 7, 10-11) and obligations if they cannot obtain the required information on the payer and the payee or detect discrepancies (Art. 8 (2), 12 (2)). The risk-based approach and the obligations for internal controls and risk assessments within financial institutions are set out in Rec. 23 and Art. 8 and 12. Article 13 also covers the responsibility of financial institutions to monitor wire transfers for potential risks, and Art. 16 requires financial institutions to keep records of payer and payee information for a period of five years. Cooperation and exchange of information between EU member states and their competent authorities is explicitly mentioned in Art. 17-19. Moreover, Art. 25 mandates the European Supervisory Authorities to develop guidelines for competent authorities and payment service providers on the implementation of specific measures, in particular in relation to Art. 7-8 and 11-12.[309]

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015[310]

The Fourth AMLD on combating ML and TF introduced a number of innovations, particularly in the area of preventive obligations.

The Commission (Art. 6) and the member states (Art. 7) are required to analyze the geographical risks of ML and TF, and the obligated parties (Art. 8) are required to analyze their own risks of abuse in this context. These risk analyses should serve as a basis for further

[307] cf. Document 32006R1781, 2006, Rec. 1, 6, Art. 1, 4, 20; Document 32005L0060, Art. 1 (2)-(3).
[308] Document 32015R0847, 2015.
[309] cf. Ibid., Rec. 23, Art. 4-8, 10-13, 16-19, 25.
[310] Document 32015L089, 2015.

improvement of the prevention system. In the case of obligated parties, this analysis should also serve as a basis for supervision by the competent authority (Art. 48 (6)).

Article 9 in conjunction with Art. 64 empowers the Commission to draw up a black list of third countries with an increased risk of ML on the basis of the national prevention systems.

There have been no significant changes to the customer due diligence requirements (Chapter II). For the first time, the European legislator has provided member states with concrete guidelines for the identification of ML risks (Annexes I-III). According to Art. 30, member states are required to establish a central register containing basic information on the beneficial owners of companies and other legal entities. A legitimate interest is sufficient for access to the register (Art. 30 (5) lit. c).

The Fourth AMLD also contains explicit provisions on data protection and the processing of personal data (Art. 40-41). In addition, there are provisions on international cooperation, in particular between (national) FIUs (Art. 51-57).

In addition to a more stringent catalog of sanctions (Art. 59), the legal consequences also include the disclosure of violations committed at the national (Art. 60) and European (Art. 62) levels. Furthermore, in addition to suspected cases of ML and TF, violations of national regulations enacted on the basis of the Directive by other obligated parties must also be reported (Art. 61).[311]

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017[312]

Directive (EU) 2017/541 is an important step in the EU's efforts to combat terrorism and its financing. It aims to harmonize criminal law provisions in the EU member states, facilitate cooperation and improve preventive measures in the fight against terrorism.

Article 3 establishes a common definition of terrorist offenses, including acts that intentionally cause death or serious injury, hostage-taking and extensive destruction of public or private property. Furthermore, the Directive criminalizes participation in the activities of a terrorist group, as well as providing support or resources to such a group with the intent to contribute to the commission of terrorist offenses (Art. 4). Title III defines offenses related to terrorist activities, including TF (Art. 11). Article 17 establishes the liability of legal entities for terrorist offenses and offenses related to TF committed for their benefit or by persons acting on their behalf. In addition, the Directive requires EU member

[311] cf. Document 32015L089, 2015, Art. 6-9, 30, 40-41, 48 (6), 51-57, 59-62, 64, Chapter II, Annexes I-III.
[312] Document 32017L0541, 2017.

states to impose effective, dissuasive and proportionate sanctions and penalties on those found guilty of terrorist offenses and related offenses, including TF (Art. 15, 18). Articles 19-20 provide guidelines for establishing jurisdiction and encourage cooperation in the investigation and prosecution of the described offenses. Provisions on assistance, protection and rights of victims are contained in Title V.[313]

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018[314]

Directive (EU) 2018/843, the EU's Fifth AMLD, includes rules for virtual currencies, also known as cryptocurrencies. There is a particular focus on dealing with high-risk countries and identifying politically exposed persons. The Directive also strengthens FIUs and increases transparency regarding beneficial owners:

As electronic wallets are used to store and transfer virtual currencies (Art. 1 (2) lit. d (19)), electronic wallet providers are included among the obligated parties for the first time (Art. 1 (1) lit. c).

Moreover, the Directive tightens the due diligence requirements for business relationships with third countries with a high risk of ML (Art. 1 (11)) and for transactions involving prepaid cards (Art. 1 (7)). Member states are required to publish lists of relevant public authorities (Art. 1 (13)) to help obliged parties determine whether a business partner is a politically exposed person.

Transparency obligations for trusts and similar legal arrangements are strengthened and member states' central registers must be interconnected (Art. 1 (16)). In addition, FIUs are given enhanced information powers (Art. 1 (15), (20)) and the exchange between FIUs of member states is facilitated (Art. 1 (30)-(36)).

Like the Fourth Directive, the Fifth Directive seeks to strengthen the risk-based approach, thereby broadening the scope of the risk-based approach and making it easier for obligated persons to implement risk-based ML prevention. Although only one year has passed since the Fourth EU AMLD was transposed into national law, the need for improvement has led to the adoption of a supplementary Directive, confirming the enormous importance attached to combating ML and TF at the international level.[315]

[313] cf. Document 32017L0541, 2017, Art. 3-4, 11, 15, 17-20, Titles III, V.
[314] Document 32018L0843, 2018.
[315] cf. Scholz, 2020, pp. 20-21; Document 32018L0843, 2018, Art. 1.

Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018[316]

Regulation (EU) 2018/1672 focuses on the control of cash entering or leaving the EU, thereby contributing to the prevention, detection and investigation of ML and TF activities. Cash is defined broadly to include currency, bearer negotiable instruments, certain highly liquid and valuable goods, and prepaid cards (Art. 2 (1) (a)).

The Regulation ensures that cash sums of EUR 10,000 or more crossing the EU's borders are duly declared to the competent authorities (Art. 3-4). In this context, Art. 5 emphasizes the need for customs authorities to carry out risk-based controls on cash. In cases where cash is not declared, is incorrectly declared or is linked to criminal activities, the competent authorities may temporarily detain the cash (Art. 7).

Furthermore, the Regulation provides for the provision of information to the FIU (Art. 9), the need for competent authorities to cooperate with other competent authorities and the Commission to facilitate the exchange of information (Art. 10), and provisions on the protection of personal data and the retention of cash and disclosure reports by competent authorities and the FIU for a period of five years (Art. 13).[317]

Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018[318]

The EU AMLD 2018/1673 sets minimum standards for the criminal prosecution of ML. According to Art. 2 (1), all offenses are considered as potential precursors of ML that are punishable by a custodial sentence of a minimum of six months and a maximum of one year. Additionally, there is a list of precursors that must be included.

Similar to Art. 9 of the Warsaw Convention, Art. 3 describes the minimum requirements for national ML offenses. However, the obligation in Art. 3 (5) to prosecute self-laundering, i.e. ML by the predicate offender, is new.

Article 5 (2) provides for a maximum sentence of at least four years' imprisonment for the offenses described in Art. 3. Attempts and participation are also subject to sanctions under Art. 4. Furthermore, there are *aggravating circumstances* for a ML offense (Art. 6), such as the commission within the framework of a criminal organization (Art. 6 (1) lit. a) or by a

[316] Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (Document 32018R1672), 2018.
[317] cf. Ibid., Art. 2 (1) lit. a, 3-5, 7, 9-10, 13.
[318] Document 32018L1673, 2018.

perpetrator who is active in one of the sectors referred to in Art. 2 of the Fourth AMLD and acting in the course of his or her professional activity (Art. 6 (1) lit. b), as well as the laundering of assets of considerable value (Art. 6 (2) lit. a) and of certain predicate offenses (Art. 6 (2) lit. b).

Article 7 provides that legal persons may also be held liable for ML committed as a result of a lack of control or committed by their organs for the benefit of the legal person. The legal consequences are defined in Art. 8 as fines or penalties and other sanctions that may affect the economic activity of the legal person.[319]

Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019[320]

Directive (EU) 2019/1153 lays down rules on the use of financial information to combat ML, financial crime and other serious crime. It aims to improve cooperation between FIUs and competent public authorities and to facilitate access to and exchange of financial information.[321]

Some of the key elements include the power of competent authorities to access and search centralized registers of bank accounts in order to carry out their AML and CFT responsibilities (Art. 4).[322] According to Art. 2 (1), centralized bank account registries are "the centralised automated mechanisms, such as central registries or central electronic data retrieval systems, put in place in accordance with Article 32a(1) of Directive (EU) 2015/849".[323]

Furthermore, there are provisions on cooperation and exchange of information between different FIUs and competent authorities (Art. 7-8), exchange of financial information between FIUs within the EU (Art. 9) and between competent authorities of EU member states (Art. 10) and exchange of information with Europol (Chapter IV) in order to enhance cross-border cooperation in combating ML and TF.[324]

3.4 German Instruments

As one of Europe's leading economies and a member of the EU, Germany, with its well-established financial sector, occupies a prominent position in the international fight against

[319] cf. Scholz, 2020, pp. 21-22; Document 32018L1673, 2018, Art. 2 (1), 3-4, 5 (2), 6-8; Document 32015L084, 2015, Art. 2; Warsaw Convention, 2005, Art. 9.
[320] Document 32019L1153, 2019.
[321] cf. Ibid, Rec. 1-2.
[322] cf. Ibid, Art. 4.
[323] Ibid., Art. 2 (1).
[324] cf. Ibid., Art. 7-10, Chapter IV.

ML and TF. This section examines Germany's efforts, including its AML and CFT institutions and legal instruments.

3.4.1 German Institutions

Federal Financial Supervisory Authority (BaFin)

The German Federal Financial Supervisory Authority (BaFin) is responsible for the supervision of the financial sector, including banks, insurance companies, financial service providers as well as securities trading. The autonomous public-law institution under the supervision of the Federal Ministry of Finance (Bundesministerium der Finanzen) is managed by an Executive Board and funded by the institutions and undertakings it supervises.[325]

Preventing the misuse of the financial system for ML, TF and other criminal activities is one of BaFin's main objectives. Its AML supervision covers institutions in the financial sector, which, in addition to those mentioned above, also includes life insurance companies, financial investment management companies or persons and companies that distribute or convert electronic money. The only competent authority in this area is BaFin, which ensures that the institutions and persons it supervises comply with the legal obligations imposed on them. These obligations result from the GwG, the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz, ZAG)[326], the Banking Act (Kreditwesengesetz, KWG)[327], the Capital Investment Code (Kapitalanlagegesetzbuch, KAGB)[328] or the Insurance Supervision Act (Versicherungsaufsichtsgesetz, VAG)[329].[330]

Federal Criminal Police Office (BKA)

The German Federal Criminal Police Office (Bundeskriminalamt, BKA) was established in 1951 by the *Law on the Establishment of a Federal Criminal Police Office*. The development, expansion and orientation of the BKA have always been closely linked to national and international crime trends and the role of the BKA within the security architecture in Germany, Europe and the world.

In addition to advances in information and communication technology, which criminals use to their advantage, the fight against international terrorism is currently a global challenge.

[325] cf. Bundesanstalt für Finanzaufsicht (About), n.d.
[326] Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz – ZAG), 2023.
[327] Gesetz über das Kreditwesen (Kreditwesengesetz – KWG), 2023.
[328] Kapitalanlagegesetzbuch (KAGB), 2023.
[329] Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz - VAG), 2023.
[330] cf. Bundesanstalt für Finanzaufsicht (Prevention), n.d.

The resulting reorganization of the BKA's State Security Division significantly strengthens the investigative potential in connection with international terrorism. Furthermore, the Joint Counter-Terrorism Centre (Gemeinsames Terrorismusabwehrzentrum) was established in 2004 to collect and evaluate information on international terrorism on an interagency basis.[331] It therefore plays an important role in the cooperation between police and intelligence services.[332]

Financial Intelligence Unit

The German FIU was established as an administratively oriented central unit for financial transaction investigations (Zentralstelle für Finanztransaktionsuntersuchungen) within the General Directorate of Customs (Generalzolldirektion). The FIU is of great importance at the regulatory level and is responsible for receiving, analyzing and disseminating SARs from financial institutions and other designated reporting entities. In this context, all available relevant data from financial, administrative and law enforcement authorities are used in the assessment. If the assessment results in a suspicion of ML or TF, the assessed reports are forwarded to law enforcement agencies and other relevant authorities.[333]

Anti Financial Crime Alliance

The Anti Financial Crime Alliance (AFCA) is a public-private partnership founded in September 2019 by the FIU, BaFin and BKA together with representatives of major German banks. It aims to establish a sustainable strategic cooperation in the field of combating ML and TF in Germany and has therefore developed various papers on ML typologies and risks, which are available to all reporting entities. The initiative started with a pilot phase in the financial sector and has been extended to the non-financial sector. Additionally, it includes public authorities and non-obligated parties. In principle, any group affected by the GwG can participate in the AFCA.[334]

Other Private Actors

At the level of private actors, Deutsche Bank is a member of the Wolfsberg Group.[335] In total, 13 global banks belong to the Wolfsberg Group, which has set itself the goal of developing frameworks and guidelines for dealing with the risks associated with financial crime. The focus is on Know Your Customer (KYC), AML and CFT.[336]

[331] cf. Bundeskriminalamt (BKA), n.d.
[332] cf. Groth, 2016, pp. 164-165.
[333] cf. Zoll (FIU), n.d.
[334] cf. Zoll (AFCA), n.d.; Zoll (Public Private Partnership), n.d.; Financial Action Task Force, 2022, p. 47.
[335] cf. Deutsche Bank, 2023, p. 1.
[336] cf. Wolfsberg Group, n.d.

In addition, interpretation and application guidelines are issued by the German Banking Industry Committee (Deutsche Kreditwirtschaft).[337]

3.4.2 German Legal Instruments

Money Laundering Act (GwG)

In Germany, the main legislation against ML and TF is the GwG. Essentially, financial services institutions are required to comply with certain due diligence obligations when processing their customers' financial transactions. Key principles include the KYC principle (§§ 10-11 GwG) and the risk-based approach (§ 3a GwG). In addition to the due diligence obligations, there is a duty to report suspicious transactions to the FIU (§§ 27, 32 GwG) and a duty of disclosure (e.g. § 52 GwG).

In most cases, BaFin is responsible for supervising compliance with these obligations (§ 50 GwG).[338]

The GwG was first introduced in 1993.[339] It was completely revised in 2008 as part of the implementation of the Third EU AMLD. The rules-based approach was replaced by a risk-based approach and the consideration of politically exposed persons was introduced.[340]

After further adjustments and changes, significant improvements were made in 2017 with the implementation of the Fourth EU AMLD, such as the strengthening of the risk-based approach.[341]

Further significant extensions and tightening were set out in 2020 as part of the implementation of the Fifth EU AMLD. Another new regulation under this amendment concerns the transparency register, which is to be made as publicly accessible as possible.[342]

In this context, the Transparency Register and Financial Information Act (Transparenzregister- und Finanzinformationsgesetz, TraFinG)[343], which came into force in 2021, also entails amendments to the GwG. Among other things, there are amendments and

[337] cf. Groth, 2016, p. 165.
[338] cf. Groth, 2016, pp. 40-41; GwG, 2023, §§ 3a, 10-11, 27, 32, 50, 52.
[339] Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG), 1993.
[340] cf. Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz – GwBekErgG), 2008, Art. 2.
[341] cf. Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen, 2017, Art. 1.
[342] cf. Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, 2019, Art. 1.
[343] Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenzregister- und Finanzinformationsgesetz), 2021.

new provisions with regard to the extended due diligence obligations of obligated parties (§ 10 GwG), extended requirements for the transparency register (§§ 18-23 GwG), including public access to the transparency register (§ 23 GwG), extended reporting obligations of obligated parties (§§ 43, 45 GwG) and sanctions and fines (§§ 56-57 GwG).[344]

Transparency Register and Financial Information Act

The TraFinG implements Directive (EU) 2019/1153 and transforms the transparency register in Germany from a collection register to a full register. This allows direct and immediate access to the beneficial owners of all legal entities in Germany. In particular, the aim is to increase the practical and digital usability of the register and to create the conditions for the European networking of the transparency register. In addition, the BKA and the Federal Office of Justice (Bundesamt für Justiz) are designated for access to the account retrieval procedure, and the BKA is designated for access to the FIU data exchange. The powers for the subsequent data exchange with Europol are standardized accordingly.[345]

Criminal Code (StGB)

The definition of ML is contained in § 1 (1) of the GwG, which states that ML is a criminal offense under § 261 StGB.[346] This paragraph was last fundamentally revised in 2021 and thus leads to a significant expansion of criminal liability for ML. The expansion of the definition of ML by dispensing with a selective list of predicate offenses and including all criminal offenses as predicate offenses is intended to facilitate the presentation of evidence. However, the court must still be convinced of the criminal origin of the money laundered.[347]

Paragraph 261 of the StGB states that punishable is:

"(1) Whoever, in respect of an object derived from an unlawful act,

1. hides it
2. exchanges, transfers or takes it with the intent of preventing it being found, confiscated or its origin being investigated,
3. procures it for themselves or a third party or
4. keeps or uses it for themselves or a third party if they were aware of its origin at the time of obtaining possession of it […]

[344] cf. GwG, 2023, §§ 10, 18-23, 43, 45, 56-57; TraFinG, 2021, Art. 1.
[345] cf. Bundesministerium der Finanzen, 2021.
[346] cf. GwG, 2023, § 1 (1).
[347] cf. Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche, 2021, Art. 1.

(2) Whoever hides or conceals facts which may be of relevance to an object as referred to in subsection (1) being found, confiscated or its origin being investigated […]"[348]

Criminal activities covered by § 261 (1)-(2) StGB shall be punishable by imprisonment of up to five years or a fine.[349]

According to § 1 (2) GwG, TF means the following:

"[…] 1. providing or collecting property in the knowledge that such property will or is intended to be used, entirely or in part, for the purpose of committing one or more of the following criminal offences:

a) an offence under section 129a [Forming terrorist organisations] of the Criminal Code, also in conjunction with section 129b [Foreign criminal and terrorist organisations; confiscation] of the Criminal Code or

b) any other offences as described in [Article 3 Terrorist offences, Article 5 Public provocation to commit a terrorist offence, Article 6 Recruitment for terrorism, Article 7 Providing training for terrorism, Article 8 Receiving training for terrorism, Article 9 Travelling for the purpose of terrorism, Article 10 Organising or otherwise facilitating travelling for the purpose of terrorism and Article 12 Other offences related to terrorist activities] of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism […],

2. committing an offence under section 89c [Financing of terrorism] of the Criminal Code or

3. instigating or aiding and abetting an offence within the meaning of no. 1 or 2."[350]

The penalties for the offenses are set forth in particular in §§ 89c and 129a of the StGB:

According to § 89c StGB, the offenses described in subparagraphs (1)-(2) are punishable by imprisonment from six months to ten years.

If the assets that are the subject of the offense under § 89c (1) or (2) StGB are of low value, the term of imprisonment shall be from three months to five years (§ 89c (5) StGB).

[348] StGB, 2021, Section 261 (1)-(2).
[349] cf. StGB, 2023, § 261 (1)-(2).
[350] GwG, 2020, Section 1 (2).

Pursuant to § 89c (6)-(7) StGB, the court may, under certain conditions, reduce the penalty or even refrain from imposing a penalty.[351]

Pursuant to § 129a StGB, the offenses described in subparagraphs (1)-(2) are punishable by imprisonment for a term of one to ten years. Under certain conditions, the term of imprisonment may begin at six months (§ 129a (5) StGB).

Subparagraph (3) of § 129a StGB prescribes a term of imprisonment of between six months and five years if the objectives or activities of the organization are aimed at threatening the commission of any of the offenses referred to in subparagraph (1) or (2). Under certain circumstances, the term of imprisonment may be up to ten years (§ 129a (4) StGB). Furthermore, under § 129a (5) StGB, a fine is appropriate under certain conditions.

The subparagraphs (6)-(7) of § 129a StGB allow the court to reduce the penalty or even not to impose it under certain circumstances.

In addition to a term of imprisonment of not less than six months, the court may also disqualify the person from holding public office and from being elected in public elections in accordance with § 129a (8) StGB.

Furthermore, in the cases referred to in § 129a (1)-(2), (4) and (5) StGB, the court may order supervision of conduct in accordance with § 129a (9) StGB.[352]

National Security Law on Countering the Financing of Terrorism

Germany prioritizes the fight against terrorism and has integrated global frameworks such as UN Security Council Resolutions, FATF Recommendations and international conventions on the suppression of TF into national law.

It is important to the German government that law enforcement measures be taken against actual and potential terrorist threats while upholding the rule of law and human rights in order to prevent radicalization. In addition to severely punishing any activity that financially supports terrorism under criminal law, deradicalization efforts are made in prison. Moreover, all available investigative tools are used and the authorities consider any information to deter or disrupt illegal activities that cannot be prosecuted.

The offenses under §§ 89c, 129a, and 129b StGB and § 18 of the German Foreign Trade and Payments Act (Außenwirtschaftsgesetz, AWG)[353] cover the risk categories for TF as defined by the FATF, including the attempts under § 129a (1)-(2) StGB and § 18 (1) No. 1 a)

[351] cf. StGB, 2023, § 89c (1)-(2), (5)-(7).
[352] cf. Ibid., § 129a.
[353] Außenwirtschaftsgesetz (AWG), 2022.

alternative 8 and No. 1 b) AWG. Violations of embargoes imposed by the EU, including the provision of assets to persons or organizations suspected of terrorism, may also be prosecuted under § 18 (1) No. 1 a) AWG. The law requires only that the donor be aware of the economic restrictions imposed on the recipient.[354]

[354] cf. Bundesministerium der Finanzen, 2019, pp. 22-23; StGB, 2023, §§ 89c, 129a-129b; AWG, 2022, §18 (1) No. 1 a)-b).

4 Current Threats and Vulnerabilities in Germany and Specific Countermeasures

4.1 Relevance of the Analysis of Germany

This chapter focuses on a critical examination of Germany's threats and vulnerabilities to ML and TF. As a leading European economic power, Germany's strategic location, large economy, open borders, open financial center, and extensive international connections make it a key player in the fight against financial crime.

The country's vulnerability to ML and TF is exacerbated by its large informal sector, the widespread use of cash and crimes such as tax evasion, and the presence of foreign terrorist organizations, sympathizers, and fighters.[355] In addition, Germany has by far the largest number of credit institutions in the Euro Area and foreign branches compared with other EU member states.[356] Its major commercial banks offer a wide range of international financial services. Furthermore, Germany is home to one of the world's largest stock exchanges, the Frankfurt Stock Exchange, and has a large insurance sector that is closely linked to the banking sector.[357] Moreover, the Euro is recognized globally as one of the most prevalent currencies.[358]

Germany ranks seventh on the 2022 Financial Secrecy Index, indicating a clear vulnerability to ML and TF.[359]

In light of these factors, it is essential to conduct an analysis of the country's situation in terms of ML and TF threats in order to derive appropriate measures to combat and mitigate these crimes.

4.2 Recent Reports and Assessments

FATF Mutual Evaluation Report

The 2022 FATF Mutual Evaluation Report[360] provides a comprehensive analysis of the AML and CFT protocols as they were in effect at the time of the evaluation in November

[355] cf. Financial Action Task Force, 2022, p. 21; International Monetary Fund, 2016, p. 7.
[356] cf. Statista Research Department (Credit institutions), 2023; European Banking Federation (Structure of the Banking Sector), n.d.
[357] cf. International Monetary Fund, 2016, p. 7; Statista Research Department (Frankfurt Stock Exchange), 2023.
[358] cf. Financial Action Task Force, 2022, p. 21.
[359] cf. Tax Justice Network, 2022.
[360] Financial Action Task Force, 2022.

2021. The report assesses Germany's adherence to the FATF 40 Recommendations, the effectiveness of its AML and CFT infrastructure, and suggests areas for further improvement.

The examination was based on the FATF Recommendations from 2012, employing the 2013 methodology.[361] Furthermore, the analysis used data provided by Germany, as well as reports from public sources, input from various countries, and data collected by the assessors during the on-site visit.[362]

German National Risk Assessment

Germany's first National Risk Assessment (NRA) in 2019[363] was instrumental in advancing the understanding and control of ML and TF risks. Under the coordination of the Federal Ministry of Finance, 35 federal and state agencies were involved.

The assessment was based on the European Commission's supranational risk assessment and several sector-specific assessments using an adapted World Bank methodology.[364] In accordance with the FATF Recommendations, it assessed Germany's potential threat and vulnerability to ML/TF in order to effectively address existing and future risks.

In this context, the expertise of the law enforcement agencies, relevant supervisory authorities, experienced, intelligence services, and the FIU was critical. In particular, the conclusions resulted from expert dialogues among federal and state specialists, supported by statistical and academic research, consultations with the private sector, and engagement with civil society. Achieving a comprehensive understanding of the various data sets was a key component of the NRA process. Despite certain limitations, the combination of academic input and historical data analysis served to identify risk trends and is an important element of future risk assessments.[365]

German FIU Report

According to the German GwG, one of the tasks of the FIU is to prepare and publish an annual report on the operational analyses carried out. It contains statistical information on the main results and tasks of the FIU’s work.[366]

[361] see for example: Financial Action Task Force (Methodology), 2023.
[362] cf. Financial Action Task Force, 2022, pp. 17-18.
[363] Bundesministerium der Finanzen, 2019.
[364] see for example: World Bank, 2015.
[365] cf. Financial Action Task Force, 2022, p. 8; Bundesministerium der Finanzen, 2019, pp. 9-11, 14-15.
[366] cf. GwG, 2023, § 28 (1) Sentence 2 No. 11; Zoll (Jahresberichte), n.d.

In order to increase the effectiveness of control and prioritization efforts, the analysis process for the 2021 Report[367] has been refined and aligned with the key risk areas introduced in previous years, particularly with respect to typologies and trends. Within this framework, the FIU has analyzed the SARs and suspicious financial transaction information received in relation to ML and TF. In this context, all reports and information received by the FIU during the reporting year from fiscal and supervisory authorities, and reporting entities are relevant and subject to a multi-level operational analysis using a risk-based methodology. The significant increase in the number of SARs to almost 300,000 is an indication of the breadth of the data base for this analysis.[368]

Transparency International Study

Transparency International Deutschland eingetragener Verein (e.V.) is the German branch of Transparency International, a global anti-corruption network with more than 100 national chapters. Its primary goal is public awareness of the negative effects of corruption and the strengthening of integrity systems.[369]

In a study published by Transparency Germany in July 2021[370], Germany is linked to a number of ML scandals in recent years involving billions of Euros in illicit financial flows, highlighting the problem of ML and the associated risk, as well as the lack of adequate measures in Germany. In this context, the study has identified key areas that are particularly susceptible to ML risk and provides specific recommendations.[371]

4.3 Money Laundering Threats and Vulnerabilities and Specific Countermeasures

Money laundering and TF trends can vary over time and across different regions of the world. In recent years, certain methods or strategies have been identified as recurring and particularly important in the fight against ML and TF. The following section examines the threats and vulnerabilities that pose the greatest risks to Germany, in part because of their widespread nature or the monetary volume and damage of individual cases. As a result, there are other threats and vulnerabilities that are beyond the scope of this dissertation and will not be discussed further.[372]

[367] Financial Intelligence Unit, 2022.
[368] cf. Ibid., pp. 7, 14.
[369] cf. Transparency International Deutschland e.V. (Who we are), n.d.
[370] Transparency International Deutschland e.V., 2021.
[371] cf. Transparency International Deutschland e.V. (Publikationen), n.d.
[372] In addition, threats and vulnerabilities that are primarily associated with ML may also pose risks to TF and vice versa, but as they are considered less significant in this regard, they are not discussed in detail in this context.

4.3.1 Real Estate

The German real estate market is of global importance, attracting domestic and international investors due to stable values and high transaction volumes.[373] However, this prominence exposes the sector to high ML risks.[374] With rising rents and purchase prices in major cities and a shortage of affordable housing, it is crucial to prevent ML in this sector.[375] In 2017, an estimated EUR 30 billion was laundered through real estate.[376] The availability of numerous legal options for structuring real estate transactions can conceal financing sources and ownership structures, exacerbating these risks. In this context, there is also a significant ML risk associated with foreign ownership and investment in real estate through complex legal arrangements and entities.[377]

For example, nominee directors of offshore funded companies can be used to acquire properties in need of renovation in urban areas. In order to benefit from tax relief, part of the purchase amount can be paid in cash with dirty money, but to maintain plausibility, a significant portion is paid with legitimate funds. Renovation work provides an additional opportunity for ML, especially if cash payments are accepted for these services. After renovation, properties can be rented out in real or fictitious terms. The resources required are relatively easy to obtain and the risks are limited. Larger transactions involve economic risks and may attract the attention of notaries, tax authorities and the media. Smaller, more plausible transactions, on the other hand, rarely attract investigation.[378]

Furthermore, tracing illicit assets becomes difficult when there is a difference between beneficial and formal ownership, when assets are held on behalf of another party, such as in trusts, and in the case of deeply intertwined corporate networks and structures. These issues highlight the sector's vulnerability to ML through share deals, where investors, often bypassing notaries, can acquire shares in a real estate vehicle that in turn holds real estate, and interlocking shareholdings, particularly in relation to foreign shell companies. Therefore, credit institutions, as well as lawyers, tax advisors, auditors and notaries involved

[373] cf. Teichmann (Real estate money laundering), 2018, p. 372; Financial Action Task Force, 2022, p. 23; Bundesministerium der Finanzen, 2019, p. 103; European Parliament (Money laundering through real estate), 2019, p. 2.
[374] cf. Transparency International Deutschland e.V., 2018, p. 10; Organization for Economic Cooperation and Development, 2007, p. 2.
[375] cf. Financial Intelligence Unit, 2022, p. 39.
[376] cf. Financial Action Task Force, 2022, p. 23; Transparency International, 2019.
[377] cf. Bussmann, 2018, pp. 115-117; Financial Action Task Force, 2022, p. 23; Financial Intelligence Unit, 2022, p. 30; Bundesministerium der Finanzen, 2019, p. 103; European Parliament (Money laundering through real estate), 2019, p. 3; Transparency International Deutschland e.V., 2018, pp. 12-14, 17-20, 23-24.
[378] cf. Teichmann, 2020, pp. 242, 244; Teichmann (Real estate money laundering), 2018, pp. 372-374; Teichmann, 2017, p. 135; Opitek, 2021, p. 5; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 58-59.

in this context, should exercise vigilance and monitor the risks of ML and TF. Additionally, intermediaries play a critical role in these higher-risk real estate transactions where clarity of ownership may be compromised. Real estate agents also need to be vigilant against such risks, especially with the 2017 reform of the asset recovery law[379], which allows assets to be seized based on a judge's belief that they are of illicit origin, even if individuals cannot be prosecuted or convicted of the crime. As a result, illicit funds may increasingly be used to rent rather than buy luxury real estate.[380]

Foreclosures are another method of real estate-related ML that criminal organizations, particularly clans, are increasingly using to acquire properties with incriminating funds, which to date have often been cash.[381]

Key Countermeasures Implemented

The Sanctions Enforcement Act II[382], which was passed by the lower house of the German parliament (Bundestag) and the upper house of the German parliament (Bundesrat) in December 2022, aims to enable more effective sanctions enforcement and to introduce improved measures against ML. Key elements of the law include a prohibition on payments in cash, cryptocurrencies or commodities for the purchase of real estate (§ 16a GwG). Transparency in the real estate sector will be improved through the use of relevant data from land registers, which will be included in the transparency register and assigned to the relevant associations. Furthermore, the introduction of a register of sanctioned persons and their assets will improve the traceability of ownership and beneficial ownership. In addition, the law requires reporting by foreign entities that own real estate in Germany. To coordinate and implement the measures, a central office has been established, which may appoint special representatives to monitor suspicious entities.[383]

In addition to the land register of real estate owners in Germany, where a unified land register database is being developed, the transparency of the beneficial owner has been improved by

[379] Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung, 2017; The Federal Court of Justice considered the reform to be a violation of the prohibition of retroactivity, but the Federal Constitutional Court (Bundesverfassungsgericht) decided differently and considered Art. 316h Sentence 1 of the Introductory Act to the Criminal Code (Einführungsgesetz zum Strafgesetzbuch, EGStGB) as compatible with the GG (cf. Bundesverfassungsgericht, 2021; Beck-aktuell, 2021).
[380] cf. Meißner, 2017; Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung, 2017, Art. 1 No. 13 § 76a (4); Financial Action Task Force, 2022, p. 32; Bundesministerium der Finanzen, 2019, pp. 43-44, 103-104; Transparency International Deutschland e.V., 2021, p. 25; Financial Action Task Force (Annual Report), 2023, p. 33; Transparency International Deutschland e.V., 2018, pp. 29-33; Bundesministerium der Finanzen (Sektorspezifische Risikoanalyse), 2020, p. 45.
[381] cf. Bundesministerium der Finanzen, 2019, p. 104.
[382] Zweites Gesetz zur effektiveren Durchsetzung von Sanktionen (Sanktionsdurchsetzungsgesetz II), 2022.
[383] cf. Bundesministerium der Finanzen (Sanktionsdurchsetzungsgesetz II), 2022; Bundesministerium der Finanzen (Zweites Gesetz zur effektiveren Durchsetzung von Sanktionen), 2022; Bundesregierung, 2022; GwG, 2023, § 16a.

the introduction of the TraFinG in 2021. Beneficial owners of foreign companies must now be reported to the transparency register if they have an interest in a company that owns real estate in Germany. In addition, as mentioned above, the transparency register has been expanded and the conditions for evading real estate transfer tax have been tightened.[384]

The *Ordinance on Matters in the Real Estate Sector Subject to Reporting under the Anti-Money Laundering Act* (Geldwäschegesetzmeldepflichtverordnung-Immobilien, GwGMeldV-Immobilien)[385], which came into force in 2020, requires certain professional groups to report suspicious real estate transactions that may be related to ML. As a result, the number of reports has increased significantly, which is of particular value when analyzed together with reports from other reporting bodies. The majority of reports concern recurring situations. These include premature purchase price payments of more than EUR 10,000 (§ 6 (1) No. 3 GwGMeldV-Immobilien), the resale of properties within three years at significantly different prices without any apparent reason (§ 6 (2) No. 1 GwGMeldV-Immobilien), payments by or to third parties (§ 6 (1) No. 4 GwGMeldV-Immobilien), cash payments (§ 6 (1) No. 1a GwGMeldV-Immobilien) and connections to high-risk countries (§ 3 (1) GwGMeldV-Immobilien). While not all reports were actually related to ML, the triggers for the reports suggested a need for in-depth analysis.[386]

In addition, with regard to the higher risk of ML through renting rather than purchasing, as of 2020 real estate agents are subject to the GwG not only in relation to the purchase and sale of real estate, but also in transactions involving a monthly rent of more than EUR 10,000 (§§ 1 (11), 4 (4) No. 2, 10 (6) No. 2 GwG). Similarly, the provisions of the GwG must also be complied with in the case of public auctions where the value limit of EUR 10,000 is reached. This applies in particular to court-ordered forced auctions of real estate (§ 2 (3)-(4) GwG).[387]

The 2017 reform of the asset recovery law significantly amended the German StGB and the Code of Criminal Procedure (Strafprozessordnung, StPO), with a particular focus on strengthening extended as well as independent confiscation. As a result, asset freezing is generally required during investigations. As noted above, this extended confiscation allows

[384] cf. Financial Intelligence Unit, 2022, p. 39, Bundesministerium der Finanzen, 2019, p. 103; Bayerisches Staatsministerium der Justiz, 2023; Financial Action Task Force, 2022, p. 47; TraFinG, 2021, Art. 1 No. 17 a) aa).
[385] Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich (Geldwäschegesetzmeldepflichtverordnung-Immobilien – GwGMeldV-Immobilien), 2020.
[386] cf. Financial Intelligence Unit, 2022, p. 40; Financial Action Task Force, 2022, p. 47; GwGMeldV-Immobilien, 2020, §§ 3 (1), 6 (1)-(2).
[387] cf. Schleswig-Holstein Finanzministerium, 2020; Bundesministerium der Finanzen, 2019, p. 104; Financial Action Task Force, 2022, p. 47; GwG, 2023, §§ 1 (11), 2 (3)-(4), 4 (4) No. 2, 10 (6) No. 2.

assets to be seized without tracing them back to a specific crime. Asset recovery is generally applicable to any crime that generates illicit profits. In cases of suspicion, such as ML, a court may authorize the seizure of assets even without specific criminal evidence. This decision depends on circumstantial evidence, such as a person's financial status and discrepancy in the value of assets. In addition, assets may be temporarily frozen to mitigate public threats.[388]

Additionally, the FIU prioritizes SARs related to transactions in real estate and analyses them for new typologies, which enables the provision of important information, e.g. within the framework of the AFCA working group Money Laundering in the Real Estate Sector, in order to identify future reportable acts more systematically. In this regard, most SARs come from credit institutions, public authorities and other obligated parties, and fewer from real estate agents, notaries and lawyers. It is therefore necessary to further raise awareness among reporting entities, especially in the non-financial sector, to improve AML and CFT measures in the real estate sector.[389]

In 2020, a special AML task force was established within the notary supervision unit of the Berlin Regional Court to monitor notaries in real estate transactions to prevent the laundering of illegally acquired assets. The task force has conducted training for approximately 400 notaries, highlighting their obligations under AML laws. As notaries are required by law to participate in the verification of major real estate and land transactions, the task force aims to increase the expertise of notaries in recognizing and handling suspected cases of ML in high-value real estate transactions.[390]

4.3.2 Trade-Based Money Laundering

As a major exporter and importer of goods, Germany is particularly vulnerable to trade-based money laundering (TBML).[391] Therefore, the German NRA emphasizes the importance of TBML due to the country's trade volume.[392]

Trade-based money laundering is defined as the process of concealing the proceeds of criminal activity by using trade transactions to move value and legitimize its source.[393] In

[388] cf. Meißner, 2017; Bundesministerium der Finanzen, 2019, pp. 43-44; Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung, 2017, Art. 1, 3.
[389] cf. Financial Intelligence Unit, 2022, pp. 17, 39; Financial Action Task Force, 2022, p. 47.
[390] cf. Senatsverwaltung für Justiz und Verbraucherschutz, 2022; Financial Action Task Force, 2022, p. 47.
[391] cf. Financial Intelligence Unit, 2022, p. 30; Financial Action Task Force, 2022, pp. 22, 81.
[392] cf. Bundesministerium der Finanzen, 2019, p. 68; Financial Action Task Force/Egmont Group, 2020, p. 17.
[393] cf. Sullivan & Smith, 2012, pp. 4-5; Zdanowicz, 2009, pp. 855-856; Financial Action Task Force/Egmont Group, 2020, pp. 11-12; Financial Action Task Force/Organization for Economic Cooperation and Development, 2006, p. 3.

contrast, trade-related predicate offenses focus on the movement of goods rather than the movement of money facilitated by trade transactions. Additionally, TBML schemes often involve PMLs who use their expertise to diversify the risk exposure of organized crime groups.[394]

Trade and financing processes are designed to address the risks and uncertainties of international transactions. There are five primary payment methods for international transactions, which are preferred differently by importers and exporters: consignment, open account, documentary collections, letters of credit and cash in advance. Open account and documentary collections are the most common, with approximately 80 percent of international trade conducted by financial institutions using open account trade.

Open account trade involves the shipment and delivery of goods prior to payment and is a fundamental part of global trade. As financial institutions play a smaller role in open account trade, assessing the legitimacy of customers' activities can be challenging. TBML schemes often exploit this disconnect between the transfer of goods and the transfer of funds or payment.

In documentary collection, the payment is requested by the exporter, who submits the required documents to its financial institution, which forwards them to the importer's financial institution for transfer. The funds received from the importer's financial institution are then credited to the exporter by its financial institution. Despite the increased involvement of financial institutions, risks of TBML exploitation remain due to potential inconsistencies in document verification and lack of standardization.[395]

TBML can occur anywhere because every country is involved in the trade and criminals exploit gaps and loopholes in different jurisdictions. Similarly, gaps in KYC and customer due diligence processes or inconsistent application are also exploited.

There is a wide range of industries that are vulnerable to TBML, but common criteria for TBML exploitation include high margin goods, extended trade cycles such as shipping through multiple jurisdictions, and goods that are difficult for authorities to inspect.

The supply chains of lower-value goods are more likely to be in the hands of criminals because the setup costs can be significantly lower. As a result, money launderers could, for example, make legitimate deliveries while creating valid documentation to enable subsequent bogus deliveries by misusing that earlier documentation. However, the

[394] cf. Financial Action Task Force, 2018, p. 31; Financial Action Task Force/Egmont Group, 2020, pp. 11-12.
[395] cf. Financial Action Task Force/Egmont Group, 2020, pp. 12-14.

exploitation of higher value products is more likely to occur through infiltration and abuse of established supply chains.

The types of businesses at risk for TBML are diverse, ranging from small as well as mid-sized companies to large multinational corporations. Key indicators include rapid growth of startups in existing markets, unnecessarily complex and complicated supply chains, large and recurring cash payments, and companies operating in multiple unrelated sectors.[396]

Criminals may combine different methods in a single scheme to complicate the transaction chain. Over- and under-invoicing, multiple invoicing, over- and under-shipment, and misdescription of goods and services are common TBML techniques[397] related to trade description fraud that have been identified.[398]

Today's TBML risks involve a combination of traditional techniques and newer methods that facilitate the integration of illicit cash into the financial system, some of which do not require the falsification of trade or product documents. Examples include the integration of illicit cash through the exploitation of legitimate supply chains or surrogate shopping and third-party intermediaries that facilitate bill payment.

In general, feedback from the public sector suggests a link between TBML and several domestic and foreign predicate offenses, such as drug and arms trafficking, tobacco smuggling, and tax evasion. These schemes often involve multiple countries and the development of new financial intermediaries and supply chains that can be exploited for this purpose. In addition, jurisdictions with specialized company formation sectors and accounting service providers should consider their potential exposure to TBML.[399]

Tackling TBML remains a challenge for countries, resulting in few successful investigations despite the attention and resources devoted to the issue. Key challenges include a lack of awareness and understanding, due in part to the evolving and complex nature of ML techniques, a lack of national cooperation and coordination among authorities, and international cooperation, particularly information sharing. In addition, investigation and prosecution can be difficult because of the need to prove that the laundered funds are of illicit origin and, in particular, that the launderer was unaware of this fact.

[396] cf. Miller, Rosen & Jackson, 2016, pp. 4-5; Financial Action Task Force/Egmont Group, 2020, pp. 17, 20, 24-25; United States Government Accountability Office, 2020, p. 4; Financial Action Task Force, 2018, p. 30.
[397] These techniques are also used for terrorist financing (cf. Bundesministerium der Finanzen, 2019, p. 68).
[398] cf. Saenz & Lewer, 2022, p. 5992; Hanley-Giersch, 2019; United States Government Accountability Office, 2020, p. 5; Egmont Group/World Customs Organization, 2020, pp. 11-12; Bundesministerium der Finanzen, 2019, p. 68; Naheem, 2016, pp. 98-99; Miller, Rosen & Jackson, 2016, p. 2; Financial Action Task Force/ Organization for Economic Cooperation and Development, 2006, pp. 4-6.
[399] cf. Financial Action Task Force/Egmont Group, 2020, pp. 16-17, 28-32.

Financial institutions and designated non-financial businesses and professions (DNFBPs) are key players in the fight against TBML, but face challenges in detecting it due to its adaptability and exploitation of different sectors. However, most trading and supply chain businesses do not have comparable reporting requirements under the FATF Recommendations, nor are they generally subject to domestic legal frameworks of many jurisdictions, leaving the burden of identifying and reporting potential TBML activity to financial institutions and DNFBPs. In addition, financial institutions regularly face difficulties in verifying customer information, obtaining details of the ultimate beneficial owners of a customer's counterparties, and estimating reasonable prices for traded goods. Furthermore, documentation provided to financial institutions may be in multiple languages and formats, requiring additional resources for manual review.[400]

Key Countermeasures Implemented

The German GwG includes merchants among the obligated parties (§ 2 (1) GwG), regardless of for whom they are acting, which means that a wide range of persons are subject to its jurisdiction and obligations.[401] In addition, violations of the Commercial Code (Handelsgesetzbuch, HGB) can result in up to two years in prison or a fine under § 283b StGB.[402]

As noted above, the risk-based approach is important for countries to assess their exposure to ML risk. According to the FATF Recommendations, countries must identify, assess and understand ML risks, implement appropriate measures and promote effective cooperation within their AML systems. To improve the understanding of TBML, jurisdictions can use NRAs, which often include inputs such as intelligence and SARs, investigative findings, threat assessments, social and economic indicators, and the level of vulnerability and threat, as a valuable source of information on ML risks. In particular, they contain information from the public sector, but may also include contributions from the private sector, which often conducts its own risk assessment. The content of NRAs should therefore be accessible and understandable to a wider range of stakeholders. In addition, numerous national and regional initiatives, including by private sector organizations, FIUs and international bodies, have focused on increasing awareness and understanding of TBML.[403]

[400] cf. Miller, Rosen & Jackson, 2016, p. 5.; Financial Action Task Force/Egmont Group, 2020, pp. 37-42.
[401] cf. Hanley-Giersch, 2019; GwG, 2023, § 2 (1); Bundesministerium der Finanzen, 2019, p. 105.
[402] cf. Financial Action Task Force, 2022, p. 304; StGB, 2023, § 283b.
[403] cf. Financial Action Task Force/Egmont Group, 2020, pp. 16-19, 37, 43-46; Bundesministerium der Finanzen, 2019, pp. 9-15, 107.

Furthermore, FIUs play a critical role in the detection of TBML by combining data from multiple sources and sharing financial intelligence to develop a holistic understanding of criminal schemes. In this context, the SARs submitted form the basis of the analysis. By communicating directly with their counterparts in more than 160 countries, FIUs can also obtain law enforcement, administrative, and financial details on individuals and entities, as well as transactions, which is necessary to detect TBML, given the transnational nature of international trade. Increasingly, FIUs are using advanced tools and technologies to manage large data sets and uncover complex TBML cases. Strategic analysis is a core function of FIUs that helps improve the understanding of TBML risks among FIUs themselves, financial institutions, authorities, and the public.[404]

Customs authorities are also important in the fight against TBML because of their in-depth knowledge of international trade, their unique access to trade data, and their mandate to combat trade crime, including TBML. In this regard, they are responsible for the identification and analysis of shipments and goods that may be used for the purposes of TBML. Close cooperation between customs and FIUs is necessary to strengthen these efforts and the corresponding capacities. In this context, the World Customs Organization and the Egmont Group have jointly developed the *Customs-FIU Cooperation Handbook*[405], which serves as a comprehensive guide. It aims to strengthen efforts to combat ML and TF, particularly in areas such as cash smuggling and TBML.[406]

From a private sector perspective, certain companies are responsible for implementing AML measures such as customer due diligence, record keeping and suspicious activity reporting. Therefore, an important part of understanding TBML risk has been working with the private sector and the reporting behavior of covered entities. This experience in transferring information and knowledge from the private sector has enabled financial institutions to gain sufficient knowledge about trade operations and counterparties and, in turn, to be better able to identify TBML indicators and report suspicious transactions to the FIU.[407]

4.3.3 Organized Crime

Another criminal risk in Germany is organized crime, especially in the form of clans. Organized criminal structures generate large sums of profit from criminal activities, which

[404] cf. Jiao, 2023, pp. 306-308; Financial Intelligence Unit, 2022, pp. 13-28, 30; Naheem, 2016, p. 103; Financial Action Task Force/Egmont Group, 2020, pp. 49-52.
[405] Egmont Group/World Customs Organization, 2020.
[406] cf. Zoll, 2020; Financial Action Task Force/Egmont Group, 2020, pp. 54-56.
[407] cf. Hanley-Giersch, 2019; Bundesministerium der Finanzen, 2019, p. 68; Financial Action Task Force/Egmont Group, 2020, pp. 41-42, 58-59; Financial Action Task Force, 2022, p. 262.

have to be laundered in order to be able to bring them into the legal economy. In this context, the focus is currently on foreign clans in particular.[408]

Organized crime involves the systematic commission of significant crimes motivated by profit or power, committed by more than two individuals over an extended or indefinite period of time, using violence, intimidation, commercial or business-like structures, or influence in politics, public administration, the media, the judiciary, or the economy.[409]

The number of reported cases related to organized crime increased significantly in 2021 compared to the previous year, mainly due to the opening of investigations into the use of encrypted telecommunications by organized crime groups. The decryption of these communications highlights the extent to which they are used, particularly by criminals operating internationally, to plan and execute criminal activities, and necessitates a reassessment of the strategic direction of organized crime prevention efforts to identify existing areas for action.

In addition, organized crime groups are increasingly using violence and intimidation to assert power, exert influence, or collect alleged debts, as evidenced by cases of extortion, robbery, assault, and murder or attempted murder. As a result, there is an increased risk of armed confrontations, potentially in public spaces. Moreover, criminals are increasingly flexible, dividing their work and collaborating with other criminal groups for profit and for a specific purpose.

The significant financial damage of EUR 2.2 billion and the criminally generated income of EUR 1.4 billion in 2021 pose a threat to several sectors of society. This is illustrated by the reinvestment of illicit funds, corruption and other forms of influence.[410]

The quantity of organized crime groups engaged in ML activities has increased by 50 percent from the previous year. In addition, ML operations have been identified within other organized crime groups that focus primarily on various major criminal activities and attempt to integrate their illicitly obtained funds into the legitimate economy.[411] In this context, the majority of groups were dominated by German nationals, followed by Turkish- and Italian-dominated groups.[412]

[408] cf. Beka, 2019, p. 229; Bussmann, 2018, p. 1; Financial Intelligence Unit, 2022, p. 31; Financial Action Task Force, 2022, p. 69.
[409] cf. Bussmann, 2018, p. 1; Bundeskriminalamt, 2022, p. 10; Bundesministerium der Finanzen, 2019, p. 27.
[410] cf. Kleemans & Van Koppen, 2020, pp. 388, 401; Bannenberg, 2022, pp. 70-71; Bundeskriminalamt, 2022, pp. 50-52; Criminal Intelligence Service Canada, 2022; National Crime Agency, 2021, p. 31; United Nations Office on Drugs and Crime (Transnational organized crime), n.d.
[411] cf. Bundeskriminalamt, 2022, p. 51.
[412] cf. Bussmann, 2018, p. 5; Bundeskriminalamt, 2022, p. 43.

4 Current Threats and Vulnerabilities in Germany and Specific Countermeasures

The main criminal activities of organized crime in Germany are related to drug trafficking and smuggling, economic crime, and property crime, while drug trafficking, human trafficking, and fraud are the predicate offenses that pose the greatest ML threat.[413] Organized crime groups of particular concern include outlaw motorcycle gangs such as the Hells Angels MC and outlaw motorcycle gangs-type groups, groups associated with Italian organized crime such as the 'Ndrangheta, and groups associated with Russian-Eurasian organized crime.[414]

A clan specifically, as a category of organized crime groups, is an informal social group based on a shared understanding of the ancestry of its members. It has a hierarchical structure and a strong sense of belonging, with shared norms and values. Clan crime describes the criminal behavior of members of a clan, where clan membership serves as a binding and facilitating component for the commission of the crime, often at the expense of German law and values. The individual or collective offenses must be significant to the phenomenon.[415]

Clan crime in Germany, as a subcategory of organized crime, developed in the 1980s, but has only been the subject of increased security policy measures in recent years. One of the reasons for the criminal development of clan members was their lack of social integration after migrating to Germany. Since most clan members have been naturalized, measures under immigration law are rarely possible in the fight against clan crime. In addition, state measures have little effect because of the clan members' isolation and their own understanding of the law.[416]

The most common nationality among clan crime groups in the organized crime sector in Germany in 2021 was Turkish, with 29.8 percent. A commonly represented ethnic group is the Arabic-speaking Mhallamiye from Turkey and Lebanon, which includes clans such as the Miri and Remmo clans.[417] In the area of clan crime, too, most cases involve drug trafficking, property crimes and economic crimes.[418]

The significant number of organized crime cases with international links underlines the global and complex nature of organized criminal activities, which requires close cooperation with law enforcement agencies within the EU and around the world. In the area of clan-

[413] cf. Kleemans & Van Koppen, 2020, pp. 388, 392; Financial Action Task Force, 2022, pp. 22, 45, 78; Bundesministerium der Finanzen, 2019, pp. 25-28; Bundeskriminalamt, 2022, p. 6.
[414] cf. Heitmüller & Von Lampe, 2020, pp. 484-488; Sergi, 2019, pp. 115, 117, 127; Bundeskriminalamt, 2022, pp. 15-21.
[415] cf. Bannenberg, 2022, pp. 70-72; Bundeskriminalamt, 2022, pp. 23-24; European Parliament, 2021.
[416] cf. Rohde, Dienstbühl & Labryga, 2019.
[417] cf. Statista Research Department, 2023; Bannenberg, 2022, pp. 69-70, 72.
[418] cf. Bundeskriminalamt, 2022, p. 27.

based crime, transnational criminal activities and strong networking can be observed both within the EU and in the countries of origin of the clan members. These links serve to facilitate criminal activity and provide potential safe havens when prosecuted.[419]

Key Countermeasures Implemented

Criminal asset forfeiture, as described above, serves as an effective tool against organized crime by significantly undermining the financial gains that motivate illegal activity. In this regard, asset recovery offices have been established in police departments at the federal, state, and local levels to assist in these efforts.[420]

The primary authorities responsible for investigating and prosecuting ML are the State Criminal Police Offices (Landeskriminalämter, LKAs), the local police offices, and the relevant State Prosecutor's Office (Staatsanwaltschaft), but the BKA is particularly responsible for ML cases involving organized crime or international aspects. In certain cases, customs and tax authorities are also involved, and investigations are supported by the German Federal Intelligence Service (Bundesnachrichtendienst). However, most investigations focus on financial or organized crime, not specifically ML, and the level of resources and specialization varies from state to state. Some agencies, such as BaFin and the FIU, have reorganized their staff and internal operations to respond to specific risk areas. In addition, cooperation mechanisms at the operational law enforcement and supervisory levels promote the exchange of information between agencies, but still sometimes do not include all relevant parties and focus on organized crime rather than ML.[421]

4.3.4 Serious Tax Crimes

Public charges form the basis of any political system, and in Germany, financial needs are met primarily through tax revenues. Therefore, tax crimes, such as tax evasion, drain financial resources from the community.

Funds from tax crimes returned to the legitimate financial and economic cycle may constitute ML. The updated version of § 261 of the StGB as of 2021 and the all-crimes approach have implications for whether tax evasion is classified as an appropriate predicate offense. While the attribute of a professional or gang-related commission is no longer a required predicate,

[419] cf. United Nations Office on Drugs and Crime (Transnational organized crime threat assessments), n.d.; European Commission, 2017, p. 2; Bundeskriminalamt, 2022, p. 51; Bundesministerium der Finanzen, 2019, p. 27.
[420] cf. Trinchera, 2020, pp. 51-55; Bundesministerium der Finanzen, 2019, p. 43; Financial Action Task Force, 2022, pp. 28-29; Transparency International Deutschland e.V., 2021, pp. 2-3.
[421] cf. Financial Action Task Force, 2022, pp. 28, 50, 75, 77, 80, 232, 234-235.

the extension to certain tax offenses has been removed. As a result, expenses avoided through tax evasion are no longer considered a valid subject for ML offenses.

In 2021, approximately 3,600 SARs and notifications were classified as serious tax evasion, with an upward trend since the introduction of the risk-based approach, which continued throughout the year. Credit institutions accounted for 94.8 percent of SARs, while fiscal authorities accounted for 1.6 percent. Approximately 20 percent of the SARs involved unusual large cash transactions, 5 percent involved atypical cash payments in commercial transactions, and in more than 25 percent of the cases, the source of the funds was not disclosed.

The most common type of tax cited in SARs was value-added tax (VAT). In this context, information referring to sales tax, VAT or input tax regularly contained references to possible carousel fraud.[422]

Carousel fraud is a widespread form of VAT evasion within the EU involving several companies from different member states. Typically, the companies resell small, high-priced consumer goods in a circuit that takes the goods through at least three actors in one EU country back to the supplier in another EU country. The method is designed to be fast to maximize the circulation of goods and carousel repetitions before the tax authorities detect it. Depending on the setup, VAT may be partially or fully unpaid and refunded without justification.

First, the aforementioned supplier in the foreign EU country sells the goods to the so-called missing trader, also located in the EU, without charging VAT due to the intra-Community delivery. The missing trader is obliged to pay the VAT, but can claim an input tax deduction. The abuse starts with the resale of the goods to the second buyer, the so-called *buffer*. The missing trader disappears from the market as soon as he sells the goods with the VAT paid by the buffer, hence the term *missing*. The VAT due is not paid to the tax office but evaded.

The transaction in which the buffer sells the goods to the so-called distributor or broker is usually legal, with the appropriate VAT paid to the tax authorities by the distributor or broker, and serves as a means of disguising the carousel fraud. In the final step, the distributor or broker resells the goods to the supplier, which is located in another EU member state. Since the distributor or broker does not charge the remitted VAT to the supplier on the

[422] cf. Bussmann, 2018, p. 1; Financial Intelligence Unit, 2022, pp. 43-44; Bundesministerium der Finanzen, 2019, pp. 21, 29; Transparency International Deutschland e.V., 2021, p. 7; European Parliament (Tax fraud), 2019, pp. 2-3; StGB, 2023, § 261.

intra-Community delivery, the distributor or broker receives an input tax refund, thus perpetuating the carousel.

Complex company networks and bogus invoices are used to disguise carousel fraud. Furthermore, several buffers can be involved, making it more difficult for authorities to investigate. Companies may also be unwittingly included in the carousel to divert suspicion from tax investigators.

Indicators of VAT carousel schemes include cross-border trade, large VAT refunds, significant sales early in the life of a company, regular changes of location or management, and high and uniform sales volumes. Moreover, inadequate storage facilities in warehouse-intensive businesses and the trading of rights or goods other than small and expensive ones, such as cars or emission rights, may also indicate such tax evasion practices. [423]

Key Countermeasures Implemented

In addition to § 31b of the German Fiscal Code (Abgabenordnung, AO)[424], which contains disclosure requirements for fiscal authorities in the fight against ML and TF, tax advisors, auditors, lawyers and notaries are also obliged parties pursuant to § 2 (1) Nos. 10 and 12 GwG, who are subject to the reporting obligation pursuant to § 43 (1) GwG (for exceptions, see § 43 (2) GwG). For these four professions, membership in the respective professional governing bodies is mandatory. These bodies represent the interests of their members, promote professional development, enforce compliance with professional requirements, and, in the case of tax advisors and lawyers, also provide AML and CFT oversight. In addition, the professional governing bodies of tax advisors, lawyers and auditors, in cooperation with the regional governing bodies, have developed and made available to the obligated parties interpretation and application guidelines to ensure a uniform interpretation of the law across all professional groups and throughout Germany.[425]

Furthermore, the amendment to the GwG expanded the group of obligated parties to include, among others, associations providing income tax assistance. As a result of the FIU's awareness-raising activities with associations and chambers, 162 of the approximately 800

[423] cf. Holá, Arltová & Zídková, 2022, pp. 299-300; Dühnfort, Zitzmann, Hundebeck, Hlavica & Kühne, 2017, pp. 80-89; Financial Intelligence Unit, 2022, pp. 44-45; Transparency International Deutschland e.V., 2021, p. 7; European Parliament (Tax fraud), 2019, p. 4.
[424] cf. Abgabenordnung (AO), 2022, § 31b.
[425] cf. Bussmann, 2018, p. 62; Hlavica, Thomann & Martenstein, 2017, pp. 46, 55; Kaufmann, 2017, pp. 177-178; Bundesministerium der Finanzen, 2019, pp. 19, 37, 110-111; Financial Intelligence Unit, 2022, pp. 14, 55; GwG, 2023, §§ 2 (1) Nos. 10-11, 43 (1)-(2).

associations providing income tax assistance (§ 2 (1) No. 12 GwG) in Germany have registered with the FIU.[426]

Money laundering investigations are conducted by federal and state prosecutors and police and, where appropriate, by customs and tax authorities, as in the case of tax predicate offenses.[427]

Effectively preventing and combating ML and TF requires cooperation with all parties involved, which is why the FIU continues to expand its exchange with the reporting parties pursuant to § 2 (1) GwG. The national partner authorities of the FIU include the tax investigation authorities and the Federal Central Tax Office (Bundeszentralamt für Steuer).

Moreover, the prioritization of serious tax crimes as a key risk area ensures that reports and notifications in Germany that may involve tax crimes are handled quickly.

In addition to the AFCA working groups in the context of gambling and ML in the real estate sector, there is also a working group on tax crimes.[428]

4.3.5 Gambling Sector

The gambling sector offers opportunities to disguise the origin of illicit funds used and their subsequent use, in part due to the existence of a diverse online market. In Germany, the use of cash below the identification threshold of EUR 2,000 and the high velocity of circulation increase the vulnerability of the gambling sector to ML.[429] In addition, the growing popularity of online gambling has created new opportunities for ML in Germany, along with the risks associated with Internet-based transactions. In this context, variety of payment options are offered, including cryptocurrency payments, which often do not reveal the origin of the funds or the payer.[430]

In particular, ML can be carried out by the player in different ways, such as the anonymous deposit of dirty money and the subsequent payout as gambling winnings, which are usually tax-free in Germany. In this context, people often do not actively participate in the game in order to minimize the loss, and multiple accounts are used to conceal ML. Another trend is so-called chip walking, in which a perpetrator takes large sums of casino chips from one city

[426] cf. Financial Intelligence Unit, 2022, p. 18; GwG, 2023, § 2 (1) No. 12.
[427] cf. Financial Action Task Force, 2022, p. 75; Bundesministerium der Finanzen, 2019, p. 39.
[428] cf. Financial Intelligence Unit, 2022, pp. 43, 58, 74; GwG, 2023, § 2 (1).
[429] cf. Teichmann, 2020, p. 239; Financial Intelligence Unit, 2022, p. 30; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 56-57; Bundesministerium der Finanzen, 2019, p. 107; GwG, 2023, § 10 (5); Therefore, the risk of ML in the gambling sector is considered high by the German NRA, while the risk of TF is considered low (cf. Bundesministerium der Finanzen, 2019, p. 108).
[430] cf. Bussmann, 2018, p. 131; European Commission, 2022, p. 11; Bundesministerium der Finanzen, 2019, p. 107-108.

to another city's casino to play with and then gives the chips to an accomplice instead of cashing out. Furthermore, gambling providers can be exploited as payment platforms through the transfer of dirty money between player accounts or the deposit of dirty money into a criminal's account by a third party. Buying up other players' winnings claims with illegal money in order to disguise gambling winnings is also possible, although rather rare in practice. Manipulation of game procedures, corruption, or collusion with the operator, its employees, or fellow players are other ways to increase the frequency and payout rate of supposedly legitimate winnings. Furthermore, participating in gambling with some control, e.g. by simultaneously betting on winning and losing sports events, reduces gambling risks.[431]

The role of the operator is also important in analyzing the ML potential of gambling. Since gambling is not a physical product, operators are more likely to falsify their revenues and thereby engage in ML by overstating them. Such an approach can be carried out through fictitious gambling operations or the use of so-called *runners* who deliberately lose money in gambling operations on behalf of criminal actors. This method is particularly suitable for laundering large sums of money. However, the greatest risk of ML in the gambling sector is ML through the scaling of an operator’s revenues, which is why verification of the beneficial owners of operators is required at the time of licensing. In this context, legal and tax havens are a significant problem that cannot be solved unilaterally.[432]

Key Countermeasures Implemented

According to the German GwG, gambling operators and intermediaries are obligated parties (with the exception of § 2 (1) No. 15 a)-c) GwG). The responsibility for monitoring them for potential ML lies with the respective state authorities. For the regulation of interstate and online gambling services, the Joint Gambling Supervisory Authority of the Federal States (Gemeinsame Glücksspielbehörde der Länder) is the main body. Pursuant to § 57 GwG, supervisory authorities are required to publish the measures and fines they have imposed for violations of the GwG or related legal provisions, after the person subject to the sanction has been duly informed.[433]

[431] cf. Fiedler, Krumma, Zanconato, McCarthy & Reh, 2017, pp. 154, 158, 162; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 56-57; Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), 2021; Bundesministerium der Finanzen, 2019, pp. 108-109.
[432] cf. Fiedler, Krumma, Zanconato, McCarthy & Reh, 2017, pp. 162-163; Transparency International Deutschland e.V., 2021, p. 9; Bundesministerium der Finanzen, 2019, p. 109.
[433] cf. Bayerisches Staatsministerium des Innern, für Sport und Integration, 2023; Levi, 2010, pp. 540-541, 543; GwG, 2023, §§ 2 (1) No. 15, 57.

The FIU annual report[434] and the interpretation and application guidance on the GwG issued by the state supreme gambling supervisory authorities[435], highlight the key risks within the gambling sector and assist in the effective implementation of the risk mitigation measures required by law. In response to the inherent vulnerability of German casinos to exploitation for currency exchange services, strict compliance measures have been implemented for casino owners, such as the strategic selection of payout methods for winnings. Some casinos also refuse entry to certain foreign nationals to reduce the risk of international criminal gambling.[436]

Moreover, the interpretation and application guidance provides enforcement guidance regarding to supervisory authorities regarding online sports betting. Online sports betting may be prohibited if substantial violations of the Interstate Treaty on Gambling[437], a pact between the 16 German states, are found. Online casinos, secondary lotteries and online poker are generally illegal in Germany without prior state licensing. As a result, such activities by operators and intermediaries are prohibited by the supervisory authorities. However, due to the lack of international agreements, enforcement resources are often ineffective against foreign operators.[438]

Additionally, the AFCA has established a gambling working group, which, among other things, prepares reports on the market situation in the gaming sector and its classification under AML legislation, and proposes future AML measures.[439]

Due to the higher risks associated with online gambling, these providers are subject to more stringent customer due diligence requirements.[440]

4.3.6 Commercial Fraud

Commercial fraud consists of several elements, including the use of misleading or incomplete information or deception, significant economic impact, manipulation of legitimate commercial systems, possibly with international implications, inducing a target to relinquish a valuable asset or right, and resulting in a loss of value.[441]

[434] cf. Financial Intelligence Unit, 2022, p. 30.
[435] cf. Oberste Aufsichtsbehörden der Länder im Glücksspielsektor, 2020.
[436] cf. Bundesministerium der Finanzen, 2019, pp. 108, 147.
[437] Staatsvertrag zur Neuregulierung des Glücksspielwesens in Deutschland (Glücksspielstaatsvertrag 2021 – GlüStV 2021), 2020.
[438] cf. Bundesministerium der Finanzen, 2019, pp. 32, 109.
[439] cf. Financial Intelligence Unit, 2022, p. 74.
[440] cf. Financial Action Task Force, 2022, p. 48.
[441] cf. United Nations Commission on International Trade Law, 2013, p. 5.

In the context of ML predicate offenses, commercial fraud activities are often associated with Internet fraudsters exploiting account opening processes. Thus, they can, for example, operate fake stores.[442]

In the context of fake stores, non-delivery fraud is common, where perpetrators offer popular products, accept payment, but fail to deliver the items. Although the scheme is simple, it has the potential for large illicit profits and can be adapted to a variety of goods, with profits increasing with the volume sold. The criminals lure victims through advertisements and fake websites that mimic legitimate businesses, negotiate large orders, and request advance payments into the accounts of fake companies. Acting as sellers, they establish relationships with buyers, maintain contact during the supposed delivery process, and find excuses for additional payments. When suspicion arises, they abruptly cease all communication.[443]

In addition, there is a regular occurrence of false invoice scams, which involve deceptive requests for payment of fraudulent invoices, often for services not ordered, such as advertising, directory listings, domain name renewals, or office supplies. These fraudulent schemes take advantage of potential administrative confusion or lack of awareness about the authenticity of such service requests.[444]

Furthermore, credit card fraud is a global problem that affects not only individuals, but also merchants and credit card companies. Credit card fraud can take several forms, such as the loss of the card or deceitful applications by criminals. The consequences of being defrauded, such as financial loss, can be severe, often requiring years of credit repair and a significant investment of time.[445]

Another way to abuse the account opening process is to facilitate money transfers in connection with romance scams.[446] Romance scams involve criminals who create fake online personas to establish an emotional connection and gain the trust of unsuspecting victims. Predominant on dating and social media platforms, scammers aim to quickly build a relationship to gain credibility and ultimately ask for money.[447]

[442] cf. Financial Intelligence Unit, 2022, p. 31.
[443] cf. International Criminal Police Organization (Non-delivery scams), 2020.
[444] cf. Government of Western Australia, n.d.
[445] cf. Bin Sulaiman, Schetinin & Sant, 2022, p. 55; John & Naaz, 2019, p. 1060.
[446] cf. Bin Sulaiman, Schetinin & Sant, 2022, p. 55; Financial Intelligence Unit, 2022, p. 31.
[447] cf. Federal Bureau of Investigation, n.d.

Identity theft is also often part of commercial fraud, although not necessarily a criterion for it. It does, however, help to commit the crime again and again under a different name in order to generate regular income.[448]

In this context, synthetic identity fraud is of particular concern.[449] It refers to the manipulative strategy of creating a fictitious identity using various types of personally identifiable information for illicit financial or personal gain. Combined primary personally identifiable information elements such as name, date of birth, and government-issued identifiers can usually be uniquely associated with an individual. In addition, supplemental personally identifiable information elements such as addresses, electronic mail (email) addresses, or phone numbers, while not unique identifiers, reinforce the perceived legitimacy of the false identity.[450] In order to illegally obtain personally identifiable information, criminals use a variety of tactics. These include the distribution of malware through deceptive social media advertisements, phishing emails, or data breaches, with compromised data often available for sale on the Internet or Darknet.[451] Therefore, synthetic identity fraud is a complex scam that does not use the identity of a real person, but combines real and fabricated data to create a new identity.[452] Subsequently, this synthetic persona then applies for bank or credit card accounts, commits fraudulent purchases, and gains anonymous access to the financial system when the person would not normally have access.[453]

Key Countermeasures Implemented

Under § 263 StGB, anyone who intentionally deceives another person with the intent to gain unlawful enrichment is punishable by a maximum of five years in prison or a fine. Notably, even attempted fraud is punishable under this statute. In particularly serious cases of fraud, the perpetrator may be imprisoned for up to ten years.[454] In this context, §§ 202a and 202b StGB also cover espionage and data interception, and § 269 StGB covers the falsification of evidentiary data.[455] Furthermore, the Second Payment Services Directive[456], which was

[448] cf. Financial Intelligence Unit, 2022, p. 31.
[449] cf. United States Department of the Treasury (ML Risk Assessment), 2022, p. 11.
[450] cf. Federal Reserve, n.d.
[451] cf. United States Department of the Treasury (ML Risk Assessment), 2022, pp. 11-12.
[452] cf. Federal Bureau of Investigation, 2020.
[453] cf. United States Department of the Treasury (ML Risk Assessment), 2022, p. 12.
[454] cf. Financial Action Task Force, 2022, pp. 78, 85; StGB, 2023, § 263; Kriminalpolizei, n.d.
[455] cf. StGB, 2023, §§ 202a, 202b, 269.
[456] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Document 32015L2366), 2015.

implemented into national law in Germany in 2018, aims to improve consumer protection and the security of payment transactions.[457]

The BKA provides warnings and prevention tips for current scams, as well as information on what to do as a victim, and investigates.[458] In this context, it also cooperates with BaFin.[459]

Moreover, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) is Germany's main cybersecurity agency and is responsible for combating cyberthreats. It offers regular events, security instructions such as cybersecurity alerts, information for consumers on the current cybersecurity situation, e.g. on identity theft and its consequences, security recommendations for everyday digital life, including secure passwords, and offers services and cooperates with various authorities, such as the police. It is also responsible for public administration, such as federal minimum standards and critical infrastructure, and provides companies and organizations with recommendations and information on cybersecurity, standards and certifications.[460]

Beyond the regulatory requirements, companies have implemented sophisticated fraud prevention and detection systems, such as the use of artificial intelligence (AI), and rigorous customer due diligence processes.[461]

In addition to the reporting requirements under the GwG, reporting credit institutions and payment service providers are required to submit statistical data on fraud cases to the German Central Bank (Bundesbank) on a semi-annual basis as part of the revised European System of Central Banks payment statistics.[462]

4.3.7 Legal Arrangements and Legal Persons

Given Germany's status as an interconnected economy and major financial center, there are ML risks associated with certain types of international companies. Although the German economy is globally integrated, the majority of the companies are small businesses with less than ten employees subject to social security.

According to the European Commission's supranational risk assessment, criminals regularly use shell companies, complex corporate structures or trusts to disguise their identities, making it difficult to identify beneficial owners. It has been noted by law enforcement

[457] cf. Deutsche Bundesbank (PSD2), n.d.
[458] cf. Bundeskriminalamt (Warnhinweise), n.d.; Bundeskriminalamt (Richtiges Verhalten), n.d.
[459] cf. Bundeskriminalamt, 2018.
[460] cf. Schallbruch, 2021, pp. 229-230; Federal Office for Information Security (Mandate), n.d.; Federal Office for Information Security (Home), n.d.
[461] cf. Schunck, Sellung & Rossnagel, 2021, pp. 18-19; Bock, 2020, pp. 43-45.
[462] cf. Bundesanstalt für Finanzaufsicht (Meldung), 2022; Deutsche Bundesbank (Payments statistics), n.d.

authorities that such opaque structures are used in particular in major cases of ML and TF. While German legal entities are generally not susceptible to ML due to strict registration requirements, the primary vulnerability lies with foreign companies as shareholders, essentially posing an indirect risk to Germany.[463]

The NRA analyzed the ML risk of common types of businesses in Germany. Organized crime groups often choose business types based on factors such as area of operation, economic strength, and intended ML tactics to minimize detection and maximize profits from illegal activities. In this context, they often prefer to use foreign entities due to the lower veracity requirements of the registry, resulting in significant risks.

As far as German companies are concerned, the majority of white-collar crime cases involve private limited liability companies (Gesellschaft mit beschränkter Haftung, GmbH) due to their popularity and common use. In particular, small and medium-sized businesses, which are not specifically created for ML purposes but rather use pre-existing corporate structures, are associated with ML. Essentially, the GmbH is a preferred structure for small and medium-sized businesses due to its limited liability framework.

A subtype of the GmbH, the Unternehmergesellschaft (haftungsbeschränkt), also appears regularly in ML contexts. It is a type of limited liability company that can be formed without significant capital, similar to the limited company in the United Kingdom, which is also conducive to ML. In general, entities with an anonymous or anonymized entity as the ultimate beneficiary, pose both ML and TF risks and complicate criminal investigations.

Another common type of company in various industries is the public limited company (Aktiengesellschaft, AG). Typically, these are large companies that are susceptible to ML because of their actual business activities rather than the corporate structure itself. In addition, it is unusual for an AG to be formed for the express purpose of the conduct and concealment of ML activities.[464]

The German partnership under civil law (Gesellschaft bürgerlichen Rechts, GbR), of which there is a relatively large number in Germany, presents ML vulnerabilities due to its flexible and diverse forms of organization, which make it difficult to regulate. In general, ML schemes are more likely to be facilitated by entities that are easy and quick to set up. However, in the case of a GbR, the vulnerability is mitigated because it is directly linked to the identity of its partners and offers little anonymity. Still, there is no comprehensive source

[463] cf. European Commission, 2022, pp. 8-9; Bundesministerium der Finanzen, 2019, p. 34; Financial Action Task Force (Annual Report), 2023, p. 12.
[464] cf. Bundesministerium der Finanzen, 2019, pp. 34-35.

of beneficial ownership or basic information available to competent authorities, and reforms to German partnership law[465] will not be fully effective until 2024.[466]

Moreover, NPOs, which in Germany are often registered associations (e.V.), are often involved in the financing of terrorism as described above. In particular, they are often associated with crimes such as rocker crime or politically motivated foreigner crime.[467]

Criminals often use foreign entities to disguise and launder their illicit proceeds through global investments, including in real estate in Germany. A notable example of this pattern is the Panama Papers, which contained confidential data such as emails, client interactions, account transactions, client portfolios, and incorporation documents leaked from Mossack Fonseca, a Panamanian offshore service provider. It shows that Mossack Fonseca helped some 14,000 clients set up nearly 270,000 shell companies in 21 offshore jurisdictions. This case underscores the vast scope of organized crime investigations in this area. The use of foreign corporate forms can indeed complicate ownership structures and effectively hide illicit assets. The incorporation of such entities into German law poses a corresponding risk, particularly in the case of offshore companies.[468]

Key Countermeasures Implemented

Germany's system for combating ML and TF in relation to legal persons and arrangements is evolving. Current efforts are aimed at consolidating and centralizing beneficial ownership data through the transparency register. With its implementation and the aforementioned legislative changes in 2021, obligated entities must file discrepancy reports when verifying data on the transparency register and all relevant entities must file directly with the transparency register, which significantly improves access to accurate, up-to-date and adequate data. Additionally, beneficial ownership information is accessible through law enforcement agency powers and the Electronic Account Retrieval System, which, despite its limitations, is commonly used by authorities.

In addition, public access to information on the establishment of legal persons and arrangements is considerable. This access, together with a recent sectoral risk analysis,

[465] Gesetz zur Modernisierung des Personengesellschaftsrechts (Personengesellschaftsrechtsmodernisierungsgesetz - MoPeG), 2021.
[466] cf. Bussmann, 2018, pp. 149-150; Financial Action Task Force, 2022, p. 198; Bundesministerium der Finanzen, 2019, p. 35; European Commission, 2022, p. 10; MoPeG, 2021, Art. 137.
[467] cf. Financial Intelligence Unit, 2022, p. 31; Financial Action Task Force, 2022, p. 101; Bundesministerium der Finanzen, 2019, p. 35.
[468] cf. Garcia Alvarado & Antoine, 2019, pp. 4-5; O'Donovan, Wagner & Zeume, 2019, pp. 4118-4119, 4123; Bundesministerium der Finanzen, 2019, pp. 35-36.

facilitates the understanding of the risks associated with different legal arrangements and persons.

To combat ML and TF, Germany has introduced several mitigating measures, such as the use of an automated account data retrieval system and various registers, provisions on nominee directors and shareholders, and increased restrictions on bearer shares.

Accurate and up-to-date basic information can be obtained by competent authorities and obligated parties through the Common Register Portal of the German federal states (Gemeinsames Registerportal der Länder)[469], which, however, does not contain information on beneficial ownership. Only the commercial registers provide information on the partners of commercial partnerships.

Furthermore, the transparency register has imposed sanctions for failure to report, and BaFin has taken supervisory action on a small scale.[470]

4.3.8 International Interconnectedness

Deeply embedded in the global financial system, the German economy occupies a prominent position in the European Single Market and in global exports. Both its financial and non-financial sectors are closely linked to the international economy and pose a high risk of international ML and TF, including foreign predicate offenses.[471]

Therefore, the NRA analyzed cross-border ML threats and their impact between Germany and more than 30 other countries or territories. The selection of these countries was based on factors such as geographic proximity to Germany, German population in the country and vice versa, economic ties to Germany, and their association with ML and TF activities. Germany's ML vulnerability was identified as high[472] relative to 11 states or regions, including Turkey, Eastern Europe, particularly Russia, China, Malta, Cyprus, British Virgin Islands, Bermuda, Cayman Islands, Guernsey, Isle of Man, and Jersey. However, the specific ML threats to Germany from these regions vary considerably.[473]

Germany and Turkey have significant economic and financial ties, strengthened by a large Turkish community in Germany. This often draws the attention of ML specialists to

[469] Common Register Portal of the German Federal States, n.d.
[470] cf. Bussmann, 2018, pp. 150-153; Financial Action Task Force, 2022, pp. 197-198, 203-204; Bundesministerium der Finanzen, 2019, pp. 34, 36-38; Financial Action Task Force (Annual Report), 2023, pp. 13, 31.
[471] cf. Matthes, 2022, p. 24; Financial Action Task Force, 2022, pp. 7, 22, 38; Bundesministerium der Finanzen, 2019, pp. 3, 31.
[472] Scale used: low, medium-low, medium, medium-high, high (cf. Bundesministerium der Finanzen, 2019, p. 3).
[473] cf. Bundesministerium der Finanzen, 2019, pp. 31-32.

Germany as a strategic link between East and West. Istanbul, in particular, is a hub for drug trafficking and illegal migration to Europe, and there are also links to TF through the hawala banking system. In addition, the route from Germany to Turkey is essential for MVTS, with large amounts of cash regularly found on flights to Turkey.

Russian or Russian-speaking organized crime groups are also a significant ML threat to Germany and Europe, with Western Europe being a prime target. The links between Russian organized crime and regional intelligence structures exacerbate this risk. According to German security agencies, Russian illicit funds were laundered through the financial center of Frankfurt am Main and also routed through places such as London, Malta, Cyprus, Switzerland, and offshore islands before being invested in Germany.

Cash violations on flights from Germany to China are also common, as is the distribution of large quantities of Chinese counterfeit goods in Europe through organized crime channels. Illicit profits were often laundered in Germany, typically through luxury purchases or real estate investments, and then transported back to China using cash couriers.[474]

The ML risk for Germany with respect to Malta, Cyprus, the British Virgin Islands, Bermuda, the Cayman Islands, Guernsey, the Isle of Man, and Jersey arises from the structure of their financial centers, which can facilitate concealment. In these jurisdictions, illicit funds, including those from Germany, can be seamlessly invested in entities such as shell companies. Malta, in particular, is also a hub for online gambling, which generates illicit profits in Germany and is illegal in Germany. In addition, some of these countries offer the Golden Visa program, which allows individuals to obtain citizenship in exchange for certain investments. The prospect of investing illicit profits while securing citizenship in that country poses significant threats, such as ML, security threats, tax evasion, or corruption. These risks are compounded by the cross-border privileges associated with EU citizenship. Therefore, customer due diligence is mandatory for entities bound by EU regulations, and member states are responsible for ensuring that the provision of citizenship to investors is not used as a loophole to circumvent EU AML laws.

Moreover, according to the NRA, Germany is exposed to a medium-high risk of ML from six countries, including Lebanon, Italy, Panama, Switzerland, Latvia and the United Kingdom. As described above, Lebanon is particularly involved in the laundering of illicit

[474] cf. McFadden, 2019, p. 88; Bundeskriminalamt, 2022, pp. 15-16, 21-22, 43, 50-51; Bundesministerium der Finanzen, 2019, p. 32; Statista Research Department, 2023; Financial Action Task Force, 2022, pp. 22, 78.

funds from clan crime. These funds, generated in Germany, are often transferred to Lebanon and laundered there.

Additionally, there are strong economic and personal ties between Germany and Italy, strengthened by the large Italian community in Germany. Italian organized crime groups have been observed attempting to launder locally and internationally generated illicit funds in Germany, often through the purchase of real estate. These groups have also engaged in protection racketeering in Germany, with the illicit proceeds laundered in both countries.

In summary, 17 countries or regions pose a high or medium-high ML threat to Germany. All other countries included in the assessment pose a medium, medium-low, or low ML threat to Germany and are therefore not discussed further in this framework.[475]

Key Countermeasures Implemented

Financial institutions engaged in cross-border correspondent banking outside the European Economic Area are required to obtain thorough information about the nature of the business and reputation of the respondent, the quality of supervision (§ 15 (7) No. 1 GwG), the respondent's AML and CFT controls and the approval of senior management before entering into the relationship (§ 15 (7) No. 2 GwG). Furthermore, each institution's due diligence responsibilities must be identified and documented (§ 15 (7) No. 3 GwG). For correspondent banking relationships within the European Economic Area, however, an individualized, risk-based approach is applied (§ 15 (3) No. 4 GwG).

Both credit and financial services institutions are prohibited from establishing or maintaining business relationships with shell banks (§ 25m KWG). Additionally, it is incumbent upon all financial institutions to implement strategies to avoid establishing or maintaining business relationships with entities whose accounts are used by a shell bank (§ 15 (7) No. 4 GwG).[476]

Moreover, pursuant to Art. 4 of EU Regulation 2015/847, German financial institutions are responsible for ensuring that cross-border wire transfers in excess of EUR 1,000 contain several mandatory details of both the originator and the beneficiary. For wire transfers of less than EUR 1,000, the information and verification requirements are less stringent if there is no reasonable suspicion of ML or TF and no cash or anonymous electronic money is involved (Art. 6 (2) EU Regulation 2015/847). Other simplifications apply to batch files (Art. 6 (1) EU Regulation 2015/847) and domestic or intra-EU wire transfers (Art. 5, 14 EU

[475] cf. Bussmann, 2018, p. 5; Bundesministerium der Finanzen, 2019, pp. 32-33; Statista Research Department, 2023; Bundeskriminalamt, 2022, pp. 15-16, 19-20, 43, 50-51.
[476] cf. GwG, 2023, § 15 (3) No. 4, (7) Nos. 1-4; KWG, 2023, § 25m; Financial Action Task Force, 2022, p. 264.

Regulation 2015/847). The beneficiary's financial institution must verify the beneficiary's identity and confirm that the beneficiary's and originator's details are complete (Art. 7 EU Regulation 2015/847). Intermediary financial institutions must identify transfers that lack required information, and both intermediary and beneficiary financial institutions must have established risk-based procedures and policies for determining when to execute, suspend, or reject such transfers and the subsequent steps to be taken (Art. 8, 11, 12 EU Regulation 2015/847). In addition, retention requirements are set forth in Art. 10 and 16 (1) of the EU Regulation 2015/847. The listed obligations also apply to MVTS providers, including agents (Art. 2 (1), 3 (5) EU Regulation 2015/847).[477]

Furthermore, Germany investigates and prosecutes ML cases involving both domestic and foreign offenses, tracks proceeds moved offshore, and actively freezes and confiscates the proceeds of crime, including foreign predicate offenses.[478]

German financial institutions must ensure that majority-owned subsidiaries and foreign branches comply with German AML and CFT regulations, especially where host country regulations are less stringent. In the event of conflicts with host country regulations, these entities must take appropriate measures to manage ML and TF risks and report to their home supervisor. Foreign branches are also actively supervised by BaFin. Moreover, financial institutions must apply enhanced countermeasures and due diligence to transactions and business relationships with high-risk third countries (§ 15 (3), (5a), (8), (10) No. 1 GwG and Art. 9 (2) of EU Directive 2015/849 as amended by Art. 1 (5) of EU Directive 2018/843).[479]

Countermeasures for cross-border cash transactions in this context are described in chapter *4.4.1 Use of Cash* below.

4.3.9 Lack of Problem Understanding

Understanding the scope and nature of ML is key to effectively combating ML activities. However, Germany faces challenges in achieving this. The first German NRA of 2019 relied primarily on the experience of AML officials and investigators, rather than empirically based information on ML, especially in cashless payments, and partly lacked contextual links. Moreover, the views of investigators provide only a limited perspective on the broader problem.

[477] cf. Financial Action Task Force, 2022, pp. 269-270; Document 32015R0847, 2015, Art. 2 (1), 3 (5), 4-5, 6 (1)-(2), 7-8, 10-12, 14, 16 (1).
[478] cf. Bundesministerium der Justiz und für Verbraucherschutz, 2015, pp. 7-8, 12, 15, 18, 21, 25; Financial Action Task Force, 2022, pp. 83, 90, 92, 98.
[479] cf. GwG, 2023, § 15 (3), (5a), (8), (10) No. 1; Document 32018L0843, 2018, Art. 1 (5); Financial Action Task Force, 2022, pp. 177, 273; Bundesanstalt für Finanzaufsicht (Europäischer Pass), 2022.

In 2018, the German Federal Ministry of Finance attempted to improve the documentation of identified and addressed ML incidents. However, German statistical practices, which focus on the most serious offense, often the precursor crime rather than potential ML, thwarted these efforts. Consequently, these cases were not identifiable for further analysis. Additionally, access to relevant organized crime and tax cases involving suspected ML has been limited, resulting in a focus on cases against individuals who provide fraudsters with access to their addresses or bank accounts for the delivery of illegally obtained goods or financial transactions. Prosecutors and investigators confirmed that, due to a lack of awareness, they often focus only on known individuals, leaving larger, complex structures untouched. Therefore, the prevalence of such cases does not indicate the extent and or effectiveness of Germany's AML efforts.[480]

Reliable analyses of unreported ML are scarce. In 2016, another German study commissioned by the Federal Ministry of Finance surveyed 942 obliged entities on the volume of suspicious transactions in the previous year. This led to an extrapolation of potential ML of EUR 20 to 30 billion in the non-financial sector and, according to a different study, a possible total volume of over EUR 100 billion. Despite their uncertain basis, these estimates have gained a prominent place in political discourse and serve as a reference point for NRA.[481]

In particular, the FATF identified gaps in the understanding of complex ML scenarios, the use of legal entities, and the role of professional intermediaries, largely due to information gaps, limited sectoral involvement in the NRA, and past limitations of the ML offense.[482]

Key Countermeasures Implemented

As noted above, Germany has undertaken several initiatives to improve its understanding of the risks of ML and TF. These include its first NRA, a number of risk assessment products, such as analyses and reports by the FIU, BKA and BaFin, state-level agency activities, and the formation of the AFCA. These efforts have improved the understanding of risks, particularly those associated with real estate, cash, the banking sector, cross-border vulnerabilities, virtual assets, NPOs, and the Coronavirus Disease 2019 (COVID-19) pandemic.[483]

[480] cf. Transparency International Deutschland e.V., 2021, p. 13.
[481] cf. Unger, Addink, Walker, Ferwerda, Van Den Broek & Deleanu, 2013, p. 43; Transparency International Deutschland e.V., 2021, p. 14; Bundesministerium der Finanzen, 2019, p. 25.
[482] cf. Financial Action Task Force, 2022, pp. 3, 8, 39, 42, 44-45, 53.
[483] cf. Ibid., pp. 3-4, 8, 10, 39, 42, 44, 53, 102, 125.

Guidance has frequently been issued by BaFin in a variety of forms, including circulars, notices, interpretative decisions, annual reports, and monthly bulletins. These communications are intended to inform and educate institutions about risks and regulatory obligations. In addition, BaFin's outreach efforts include an annual symposium for financial institutions, bilateral and multilateral engagements, participation in external events, and ongoing dialogue with high-risk institutions. Furthermore, it uses the AFCA for risk communication and typology input.

For most sectors, guidance has been provided by the supervisors of DNFBPs with training provided primarily by the supervisors of the professional bodies.

Additionally, state and district government supervisors have worked together to provide guidance on the interpretation and application of the German GwG to casinos and other DNFBPs. These supervisors also work with industry chambers to disseminate information, particularly to newly registered firms.

Professional body supervisors have developed sector-specific AML and CFT guidance for tax advisors, lawyers, accountants and notaries to ensure consistent interpretation across and within sectors. Moreover, AML and CFT training is provided by all legal and accountancy supervisors, with the exception of notary supervisors. Additional awareness tools and guidance have been developed by several supervisors, and notaries are trained by regional and federal chambers.[484]

4.3.10 Lack of Investigative Capacities

While increased transparency and reporting can contribute to the effectiveness of ML investigations, they cannot be a complete substitute for the essential resources and capacity within law enforcement agencies. In addition, it is not enough to impose stricter regulations and preventive measures on the private sector, as professional enablers regularly find ways to circumvent these measures.[485]

Recent high-profile cases, such as the Wirecard case[486], underscore the inadequacy of the existing structural conditions and legal framework for an effective AML regime. In Germany, investigations can only be initiated when there is a concrete suspicion of the underlying crime, which poses a significant challenge in the fight against ML, where the

[484] cf. Financial Action Task Force, 2022, pp. 194-196.
[485] cf. Transparency International Deutschland e.V., 2021, p. 24; Financial Action Task Force, 2018, pp. 10-11, 15, 30, 33-47.
[486] see for example: Jo, Hsu, Llanos-Popolizio & Vergara-Vega, 2021; Schäfer, 2020; Sellhorn, 2020.

primary objective is to conceal the link between illicit activities and transactions. As a result, law enforcement is often unable to initiate an investigation.[487]

Furthermore, inadequate human resources within law enforcement agencies, coupled with a limited system for calculating personnel requirements called *Pebb§y*, often mean that time-consuming investigations into money flows or complex criminal structures are sacrificed in favor of simpler prosecution of the predicate offense.[488]

In addition, the resources available for financial investigations, which vary from state to state, tend to focus on financial or organized crime rather than specifically on ML or TF. Despite changes in AML legislation and a restructuring of the FIU, Germany has not increased the resources devoted to these areas. In this context, the lack of resources, particularly in high-risk states and within the BKA's AML team, poses a challenge to the effective implementation of recent policy and legislative changes aimed at intensifying AML investigations and prosecutions.[489]

Key Countermeasures Implemented

Germany demonstrated its commitment to improving investigative capacity in ML scenarios by amending the GwG in 2021, thereby enhancing law enforcement's ability to trace financial transactions.

In terms of human resources, BaFin made organizational adjustments to its AML department in 2017, integrating more personnel to effectively manage identified risks in the banking sector. In 2020, additional staff were integrated to address risks in the non-banking sector. Staffing is allocated on a risk-based basis, with more staff assigned to the supervision of institutions with a higher risk profile, e.g. additional staff to address emerging threats from VASPs. In general, BaFin has increased its resources to conduct its own supervisory activities in order to complement the audits and to verify the results. In this context, the banks supervised by BaFin have also adjusted their staffing levels based on the results of the inspections.

Moreover, the FIU has significantly strengthened its staff in recent years to carry out its tasks effectively, although further law enforcement and financial expertise could enhance its capacity.

[487] cf. Vogel (Reform des Geldwäscheparagraphen), 2020; Transparency International Deutschland e.V., 2021, pp. 2-3, 24; Deutscher Bundestag, 2020.
[488] cf. Transparency International Deutschland e.V., 2021, p. 25.
[489] cf. Financial Action Task Force, 2022, p. 76.

As a result of the 2017 reform of the asset recovery law, prosecution offices received more resources and staffing was increased in several LKAs. In order to focus resources on the tracing of the proceeds of crime, specialized units have been established in all prosecution offices and LKAs.[490]

4.4 Money Laundering and Terrorist Financing Threats and Vulnerabilities and Specific Countermeasures

4.4.1 Use of Cash

Legal and illegal cash[491] transactions are widespread. Criminals regularly use cash because of its anonymity, liquidity, portability and lack of audit trail.[492] In addition, the establishment of relatively high standards of AML and CFT controls in the financial sector has led money launderers to increasingly use the cash sector.[493]

The cross-border transportation of cash by couriers, which increasingly takes advantage of organized crime networks, particularly in Eastern Europe, enables terrorists to launder money while avoiding the traditional oversight of the financial system. In this context, couriers can be paid professional couriers, casual couriers who, for example, transport money while traveling for business, and jihadi volunteers who pay to join terror camps. In addition, there are unsuspecting individuals who unwittingly support a terrorist organization. For example, by working in another country and visiting their homes in the target country, they often carry funds from private donors or foundations that are channeled to terrorists upon arrival.[494]

Furthermore, the majority of transactions in Germany are in cash, as Germans have a strong historical and social attachment to cash. This cash-intensive economy, combined with access to the Euro, increases Germany's vulnerability to the laundering of illicit foreign proceeds.

As illicit cash can also be converted into tangible assets of high value, sectors dealing in valuables such as cars, antiques, art or other luxury goods, which tend to use cash transactions, are more susceptible to ML risks, along with increasingly diversified investments.

[490] cf. Financial Action Task Force, 2022, pp. 50, 66, 74, 88, 174-175, 178, 226, 228.
[491] Cash, as defined by Regulation (EU) 2018/1672, includes currency, bearer-negotiable instruments, commodities used as highly liquid stores of value and prepaid cards (cf. Document 32018R1672, 2018, Art. 2 (1) lit. a; Financial Intelligence Unit, 2022, p. 55).
[492] cf. Bussmann, 2018, p. 49; United States Department of the Treasury (TF Risk Assessment), 2022, p. 20; Bundesministerium der Finanzen, 2019, p. 115; European Commission, 2022, pp. 6-7.
[493] cf. Teichmann, 2017, p. 135.
[494] cf. Bundesministerium der Finanzen, 2019, p. 47; Financial Action Task Force, 2022, p. 21.

In addition, the high level of cash has implications for ML and TF through the banking and MVTS sectors, where cash is typically used for payments, often outside of a professional relationship, such as through unauthorized MVTS providers like hawaladars (see chapter *4.5.2 Abuse of Money or Value Transfer Services*).

As a result, these transactions have been identified as key risk areas. In this context, the monitoring of cross-border cash movements, which are one of the highest-risk TF channels and equated means of payment[495] is particularly important in the fight against ML and TF.[496]

Key Countermeasures Implemented

The GwG applies to all financial and non-financial institutions covered by the FATF standards, as well as some entities that are not covered by the FATF standards but are subject to EU risks and requirements, including all commodity dealers if they conduct cash transactions in excess of EUR 10,000, as required by the EU's Fourth AML Directive. In addition, in some cases, enhanced measures have been put in place to mitigate specific risk areas, such as AML and CFT obligations for public auctions due to the frequent use of cash in this area.

Furthermore, the threshold for the application of AML and CFT measures for the sale of precious stones and metals has been lowered from EUR 10,000 to EUR 2,000 for cash transactions, and the amount for enhanced due diligence for cash transactions in sectors with high cash volumes has also been lowered.

Moreover, BaFin has issued guidance to financial institutions recommending enhanced measures for cash payments, and some reporting entities are implementing their own measures, such as not accepting cash or conducting cash transactions.

In Germany, cash or bearer negotiable instruments in excess of EUR 10,000 entering or leaving the EU must be declared. Similarly, movements of such amounts within the EU must be disclosed to customs. Data on cash declarations and disclosures are stored by customs in a database that is accessible to the BKA, members of Joint Financial Investigation Groups and the FIU, as well as to police, prosecutors, and other investigative agencies upon request.

[495] Equated means of payment under the Customs Administration Act (Zollverwaltungsgesetz (ZollVG), 2021, §1 (4)) are precious stones and metals, as well as securities within the meaning of the Custody Act (Gesetz über die Verwahrung und Anschaffung von Wertpapieren (Depotgesetz - DepotG), 2021, §1) and of the Civil Code (Bürgerliches Gesetzbuch (BGB), 2023, § 808), unless they are already considered to be cash (cf. Financial Intelligence Unit, 2022, p. 55).

[496] cf. Financial Action Task Force, 2022, pp. 7, 21-23, 25-26, 31; Senatsverwaltung für Wirtschaft, Energie und Betriebe, 2021, p. 23; Financial Intelligence Unit, 2022, p. 55; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 23; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 34-35; Transparency International Deutschland e.V., 2021, p. 16; Bundesministerium der Finanzen, 2019, pp. 3, 25-27, 58, 68.

As the supervisor of cross-border cash movements, customs uses of this information for ML and TF investigations and may share it with foreign counterparts. The FIU cross-checks submitted SARs against the database on a hit or miss basis and may perform further manual matching.[497]

In this context, the FIU collects information on the monitoring of customs duties for both accompanied and unaccompanied cash. Accompanied cash refers to cash carried by individuals, while unaccompanied cash refers to cash sent to or from the EU via courier services, postal parcels, container freight or unaccompanied luggage. As part of the Customs Investigation Service's clearing procedure, the FIU collects data on the registration and control of cash, both in intra-Community transport and in third country transport, which plays an important role in the operational analysis of cases (see § 30 (1) No. 3 GwG).

Cash discoveries play a critical role in AML and CFT efforts. A review of around 450 cases from 2021 shows a nearly 63 percent increase in such findings compared to the previous year. This increase is mainly attributed to pandemic-related travel restrictions in 2020, which led to a temporary decrease in notifications. Although travel restrictions continued, there was a significant increase towards the end of 2020 and beginning of 2021, likely due to increased use of alternative modes of transport as air travel was disrupted. The majority, 49.8 percent, of cash or equated means of payment detected were found in air traffic, followed by 27.3 percent in car controls and 17.1 percent in postal traffic. Of these detections, cash accounted for 87.4 percent and transferrable bearer securities for almost 8.8 percent.[498]

Where ML or TF is suspected, customs may seize and, on conviction, confiscate cash or equated means of payment. A fine of up to EUR 1 million is imposed for willful or negligent failure to make a declaration or disclosure and for making a false declaration or disclosure.

Germany has taken several steps to better understand the risks of cash-based ML and TF. For example, specialized customs units collect and analyze data on cross-border, undisclosed or undeclared, and ML- and TF-related cash movements. Results, such as new methods or trends, are regularly reported to the Federal Ministry of Finance.[499]

[497] cf. Financial Action Task Force, 2022, pp. 28, 33, 39, 48, 60, 68, 75-76, 95, 146, 225, 299-300; Transparency International Deutschland e.V., 2021, pp. 16-17; GwG, 2023, §§ 1-2, 4 (5); Document 32018R1672, 2018, Art. 3-4.
[498] cf. Financial Intelligence Unit, 2022, pp. 55-56; United States Department of the Treasury (ML Risk Assessment), 2022, p. 31; GwG, 2023, § 30 (1) No. 3.
[499] cf. Financial Action Task Force, 2022, pp. 53, 96, 131, 300-301; Transparency International Deutschland e.V., 2021, p. 16.

4.4.2 Virtual Assets

Persistent innovation in payment technologies, such as mobile applications (apps), has notably enhanced transaction efficiency. The incorporation of virtual assets, such as cryptocurrencies, further exemplifies this evolution. However, the widespread use of cryptographic and digital methods makes transaction tracking in these systems exceedingly complex, if not impossible. This obscurity potentially invites illicit activities like ML and TF.[500]

The adoption of new payment methods, which is reflected in an increase in related SARs, is steadily growing, with the majority of SARs related to virtual assets. Although the proportion of SARs from financial services institutions increased in 2021, the majority of SARs still come from credit institutions. A relatively high number of these reports are categorized as urgent or time-sensitive. It is important to note, however, that these virtual asset SARs are not exclusively related to new payment methods, but can also be associated with risk areas such as gambling or serious tax offenses. In this context, SARs also indicate a higher ML risk for offshore financial technology (fintech) companies providing money transfer and virtual asset trading services.[501]

The virtual asset market exhibited marked growth in 2021, highlighted by increased total market capitalization despite significant price volatility. Recent technological advances, like the emergence of decentralized financial services and the distribution of goods and services through unique, non-fungible tokens (NFTs), have attracted increasing public interest.

Decentralized Finance (DeFi) involves peer-to-peer financial services enabled by distributed ledger technology, such as blockchain, and smart contracts that are executed automatically. Accessible via decentralized apps, these services span a range of traditional financial functions. Examples include the exchange of virtual assets on decentralized exchanges, also called DEX, or the lending of virtual assets via DeFi apps like aave or compound.

NFTs are non-exchangeable tokens that can be tied to digital art or other digital as well as physical objects, thereby verifying their originality and uniqueness. While NFTs are

[500] cf. Bussmann, 2018, pp. 137-138; Financial Intelligence Unit, 2022, p. 31; Financial Action Task Force, 2022, pp. 7, 23; Bundesministerium der Finanzen, 2019, p. 114; United States Department of the Treasury (TF Risk Assessment), 2022, pp. 21-22; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 35.
[501] cf. Financial Intelligence Unit, 2022, pp. 47-48, 52; Bundesministerium der Finanzen, 2019, p. 100.

currently primarily associated with digital art and digital collectibles, their potential applications are much broader.[502]

Money Laundering

The ongoing development of innovative solutions based on distributed ledger technology, coupled with the significant financial value of virtual assets, continues to make them susceptible to criminal activities.[503]

Because transactions are difficult to trace, virtual assets provide unique opportunities for criminals to conceal their illicit financial activities. For example, the blockchain enables anonymous transactions and users do not have to disclose personal information or sources of funds to conduct transactions.[504] In particular, several new financial services, accessible through decentralized apps, automate transactions between anonymous parties without identifying the participants or verifying the source of funds.

Furthermore, valuation and pricing of NFTs often lack transparency due to underdeveloped valuation criteria or trading standards, creating the potential for exploitative transactions.[505]

In general, virtual assets can be used in several ways to disguise the illicit origin of the funds, such as through mixer or tumbler services that mix virtual assets of different origins.[506]

In addition, the growing acceptance of cryptocurrencies as a means of payment by retailers is an incentive for criminals to use them. Another advantage is the ease of transferring funds across borders, as there is no central authority. Furthermore, virtual assets are used to compensate for illegal activities or are accumulated through illegal activities such as online fraud. The resulting digital ML processes can be characterized as fully digital or seamless crypto ML.

Cryptocurrencies also enable tax evasion when used as a tax haven. By converting their income into cryptocurrency and moving it around the world, criminals are able to evade

[502] cf. Bussmann, 2018, p. 138; Bundesministerium der Finanzen, 2019, p. 114; Financial Intelligence Unit, 2022, pp. 47, 52; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 40-42.
[503] cf. Naheem (AML, digital currencies and blockchain technology), 2019, p. 516; Financial Intelligence Unit, 2022, p. 48.
[504] cf. Albrecht, Duffin, Hawkins & Morales Rocha, 2019, p. 213; Financial Intelligence Unit, 2022, p. 48; Bundesministerium der Finanzen, 2019, pp. 27, 59, 114-115.
[505] cf. Financial Intelligence Unit, 2022, p. 48.
[506] cf. Bundesministerium der Finanzen, 2019, p. 114; United States Department of the Treasury (ML Risk Assessment), 2022, p. 45.

authorities. This increased security gives criminals complete access and authority over the proceeds they generate, facilitating the ML process.[507]

The unregulated misuse of virtual assets for ML can destabilize the global economy. To curb this illicit activity, such crimes must be regulated and prosecuted. Furthermore, virtual assets themselves must be strictly regulated, with AML controls such as customer identification procedures in place to protect innovative currencies from unethical and illegal exploitation.[508]

Terrorist Financing

New payment methods are also used for TF. The stages of raising, moving and using, as explained above, can be applied in the same way to the illegal use of virtual assets.

First, funds are generated or provided, such as through fundraising appeals by terrorist organizations. Aside from transactions involving virtual currency exchanges, there is often evidence of fundraising activities, although comparatively few SARs involving virtual assets are linked to potential TF activities. In 2021, the majority of SARs related to potential TF were related to Islamist activities, specifically mentioning fundraising efforts by Islamist organizations. In addition, some right-wing extremist individuals have increasingly sought financial contributions through virtual assets. Isolated SARs with potential links to right-wing extremism or conspiracy theories have also been reported.

In the process of moving funds, virtual assets can be purchased and then transferred either to intermediaries or to the intended recipients. Tracking the flow of funds becomes increasingly difficult when using virtual assets compared to traditional banking transactions. Moreover, it is not possible to determine whether the reported irregularities, including suspicions of potential TF, have a causal link to the virtual assets purchased or sold.

The virtual assets are then transferred to the intended recipients of the fundraising appeals and possibly sold. Because of the obfuscated transaction flows, it is often difficult to determine the source or purpose of the funds received by the recipients. It is conceivable that the purchased virtual assets could be sent directly to relevant terrorist organizations and used by them either directly to fund terrorism or indirectly to disburse the funds in book or cash form for further use.[509]

[507] cf. Albrecht, Duffin, Hawkins & Morales Rocha, 2019, pp. 213-214; Financial Intelligence Unit, 2022, p. 47; Bundesministerium der Finanzen, 2019, pp. 30, 107-108, 114; United States Department of the Treasury (ML Risk Assessment), 2022, p. 41.
[508] cf. Albrecht, Duffin, Hawkins & Morales Rocha, 2019, p. 215.
[509] cf. Teichmann (Financing terrorism through cryptocurrencies), 2018, pp. 515-517; Irwin & Turner, 2018, pp. 297-299; Financial Intelligence Unit, 2022, p. 53; Bundesministerium der Finanzen, 2019, p. 115; United

Key Countermeasures Implemented

The NRA, additional risk assessments, situation reports, and the AFCA, among others, have contributed to a good understanding of the ML and TF risks associated with virtual assets in Germany, which is shared by most state and federal authorities as well as larger financial institutions and VASPs.[510]

Virtual asset service providers in Germany are licensed as financial service institutions under the KWG.[511] In 2020, Germany introduced adjustments to the regulatory landscape[512] with a special licensing procedure for virtual asset custody businesses (wallet providers). As a result, these virtual asset custody businesses require the approval of the relevant regulatory authorities. This shift also designates these entities as responsible parties under the GwG. As of 2020, a number of companies providing virtual asset custody or related services have initiated their first registration with the FIU.[513]

All financial institutions and VASPs must comply with EU Regulation 2015/847 mutatis mutandis to all transfers of virtual assets, including the responsibility to collect, store and transfer data for transactions between VASPs and those not limited to VASPs (in accordance with §§ 3-4 of the Crypto Asset Transfer Regulation 2023 (Kryptowertetransferverordnung, KryptoWTransferV)[514], including exemptions (§ 5 KryptoWTransferV)[515]).[516]

In June 2023, Regulation (EU) 2023/1113[517], which will extend the scope of EU Regulation 2015/847 to cover virtual asset transfers (Rec. 3) and Regulation (EU) 2023/1114[518] entered into force and will apply from December 30, 2024.[519]

States Department of the Treasury (TF Risk Assessment), 2022, pp. 6, 9, 13, 22-23; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 35-36.

[510] cf. Financial Action Task Force, 2022, pp. 3, 5, 8, 39, 42-43, 53, 139, 266.

[511] cf. KWG, 2023, § 32 (1).

[512] cf. Gesetz zur Umsetzung der Vierten EU-Geldwäschelinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen, 2017; Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, 2019.

[513] cf. Financial Action Task Force, 2022, pp. 166, 170, 266; Financial Intelligence Unit, 2022, p. 48; Bundesanstalt für Finanzaufsicht, 2021, pp. 4, 8.

[514] Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung – KryptoWTransferV), 2023.

[515] cf. Ibid., §§ 3-5.

[516] cf. Financial Action Task Force, 2022, p. 268.

[517] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Document 32023R1113), 2023.

[518] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Document 32023R1114), 2023.

[519] cf. Document 32023R1113, 2023, Rec. 3, Art. 40; Document 32023R1114, 2023, Art. 149.

Furthermore, BaFin reviews the risks associated with each institution on an annual basis, taking into account factors such as clients, complexity of operations, services and products, geography, and delivery channels before considering the quality of controls. Its risk model therefore uses both qualitative and quantitative information, including data related to higher risk scenarios.

As of 2019, BaFin has identified VASPs as a key area for supervision and external audits. Accordingly, since 2020, it has increased its regulatory scrutiny of institutions that provide significant services or products related to virtual assets, in some cases with the help of the FIU. In order to identify higher-risk institutions, BaFin has conducted a series of questionnaire campaigns, which have led to further questionnaires, supervisory meetings, and off-site and on-site inspections. In addition, it has raised its capacities and awareness among AML officers and staff of the risks and red flags associated with virtual assets. Due to banks' critical interactions with unsupervised fintechs, BaFin has created a specialized fintech competence center.

German authorities regularly seize and confiscate virtual assets. In this context, the number of frozen virtual assets has increased significantly since 2018. Asset management is supported by internal police guidelines, and some law enforcement agencies jointly maintain a recovery archive to share, for example, virtual currency freezing guidelines, asset recovery forms, and best practice tools among prosecutors, police, and tax authorities across the country.

In addition, financial institutions have established processes for developing and approving new technologies and products, including thorough risk assessments prior to implementation. Accordingly, financial institutions are increasingly aware of the risks associated with new technologies, especially those related to fintech and virtual assets. Annually audited financial institutions improve controls based on auditor feedback, while VASPs actively develop risk-specific tools, often in collaboration with the government. On the other hand, non-financial businesses are typically risk averse and sectors such as online casinos tend to avoid virtual assets. Legal, tax and accounting professionals have also implemented additional precautions for transactions involving virtual assets.[520]

[520] cf. Financial Action Task Force, 2022, pp. 89, 91, 145-146, 152, 171, 175, 178; Bundesministerium der Finanzen, 2019, p. 100.

In addition, the FIU has published a paper[521] on risk indicators in virtual asset transactions, and BaFin has issued guidance[522] and feedback[523] to financial institutions that also applies to VASPs. However, VASP-specific information is somewhat limited.[524]

4.4.3 Other New Payment Methods

Suspicious activity reports suggest that other new payment methods are less common, but still important to consider in this context.[525] The majority of SARs involving new payment methods, but not virtual assets, come from credit institutions, with a focus on transactions processed through less established, often international, financial and payment service providers. These companies regularly process payments for online gambling operators or offer innovative and cost-effective services, mostly online, such as reduced fees for international payments or free debit and credit cards.

Some reports include alternative methods as a means of transferring assets, such as through the use of various digital debit or credit cards integrated into smartphone apps and physically offered at the customer's request, the purchase of gift cards, or transferable social media credits that are accepted as payment by some online merchants, often collectively referred to as electronic money. These payment instruments are often independent of an existing account relationship with the issuing institution and can be linked to other account relationships with third-party banks or payment alternatives. What is unusual in this context is the high volume of transactions and the seemingly unnecessary use of intermediaries.

Suspicious inbound payments, such as those in electronic wallets originating from peer-to-peer transfers rather than traditional bank transactions, often lack immediate participant identification and do not provide details about the source of the funds, prompting reporting entities to file a SAR. These transactions often involve multiple payment instruments and layers between the payer and payee, including different financial service providers in multiple jurisdictions. [526]

The rapid pace of technological advancement poses significant challenges for regulators and law enforcement. As new virtual assets, platforms, and services emerge, authorities must

[521] Financial Action Task Force (Virtual Assets Red Flag Indicators), 2020.
[522] Among other things, it has issued guidelines on crypto-token issuance and crypto-custody businesses and the related licensing process. Its website also has a dedicated virtual currency section with contact forms for VASPs (cf. Financial Action Task Force, 2022, pp. 267-268).
[523] VASPs receive immediate feedback during the registration and licensing phases, as well as during annual audits and reviews (cf. Financial Action Task Force, 2022, p. 268).
[524] cf. Financial Action Task Force, 2022, pp. 267-268.
[525] cf. Financial Intelligence Unit, 2022, p. 47.
[526] cf. Akartuna, Johnson & Thornton, 2022, pp. 2-3, 11-15; Bundesministerium der Finanzen, 2019, pp. 69, 74, 95-96; Financial Intelligence Unit, 2022, pp. 50-52.

adapt and develop new strategies to effectively mitigate the risks associated with ML and TF.

Key Countermeasures Implemented

In Germany, pursuant to § 10 (1) ZAG, anyone providing payment services as a payment institution requires a written authorization from BaFin. The same applies to electronic money institutions pursuant to § 11 (1) ZAG. Requirements relating to electronic money, including those relating to intermediaries, are set out in §§ 31-33 of the ZAG. The German Central Bank and BaFin oversee these institutions (§ 6 (1) KWG), and violations are punishable by up to five years in prison or a fine of up to EUR 1 million (§§ 63-64 ZAG).

According to § 25i KWG, the due diligence requirements under § 10 GwG also apply to institutions when issuing electronic money, subject to exceptions.[527]

The GwG requires financial institutions to identify, assess, and periodically update their risk assessments with respect to their business activities, including the implementation of new products or technologies, and to implement mechanisms to manage and mitigate any ML or TF risks arising from these new developments. Measures implemented include limits on the value and volume of products sold to customers and restrictions on the value and types of products sold online.[528]

In addition, EU Regulation 2015/847 requires the verification of information on the payer when the funds are received in cash or anonymous electronic money for cross-border credit transfers of less than EUR 1,000 (Art. 6 (2)).[529]

Suspicious transactions must be reported to the FIU. Reports have often highlighted high-value recharges to prepaid cards, and transactions to or from other financial services providers where there is no obvious business reason for such a transaction.[530]

Germany, through the NRA and the subnational risk assessment, has analyzed the ML and TF risks associated with new technologies, products and services. In this context, payment and electronic money institutions were among those consulted during the implementation of the NRA, which promoted a comprehensive understanding of these risks.[531]

[527] cf. Deutsche Bundesbank (Payment institutions), n.d.; Financial Action Task Force, 2022, pp. 145, 171, 175, 265, 303; Bundesministerium der Finanzen, 2019, pp. 89, 95-96; GwG, 2023, § 10; ZAG, 2023, §§ 10 (1), 11 (1), 31-33, 63-64; KWG, 2023, §§ 6 (1), 25i.
[528] cf. Bundesanstalt für Finanzaufsicht (Guidance), 2022, pp. 18, 21; GwG, 2023, §§ 5 (1)-(2), 6 (2), Annex 2; Financial Action Task Force, 2022, pp. 146, 266; Bundesministerium der Finanzen, 2019, pp. 79, 95.
[529] cf. Financial Action Task Force, 2022, pp. 268-269; Document 32015R0847, 2015, Art. 6 (2).
[530] cf. Financial Intelligence Unit, 2022, pp. 50-51; Bundesministerium der Finanzen, 2019, p. 95.
[531] cf. Financial Action Task Force, 2022, pp. 142, 266; Bundesministerium der Finanzen, 2019; Bundesanstalt für Finanzaufsicht, 2021.

4.4.4 Cooperation and Coordination Challenges

The limited focus on policy coordination issues and operational coordination on ML, compounded by the complexity of the system, implies a need for improvement. For example, there are no formal mechanisms, such as inter-agency memoranda of understanding or working groups, to facilitate law enforcement coordination specifically on ML. With regard to the TF, one deficiency is that the FIU is not a regular member of the established operational centers or working groups. The FIU cooperates with law enforcement and administrative oversight bodies on an ad hoc basis, and cooperation with law enforcement needs to be strengthened due to inefficiencies in data analysis, delays in sharing information with law enforcement, and a possible lack of understanding of the role of the FIU by some law enforcement agencies, resulting in low use of FIU information in criminal proceedings.

In addition, with the exception of the FIU and BaFin, there is no specific body mandated to formalize memoranda of understanding when necessary. Also, outside of the FIU or mutual legal assistance provisions, there are no explicit legal safeguards to prevent competent authorities from imposing restrictive, unreasonable or excessive conditions on the provision of assistance.

Moreover, the involvement of state authorities in decision-making remains unclear, although the establishment of the Interagency Steering Committee for Combating ML/TF (Ressortübergreifender Steuerungskreis zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung, RÜST GW/TF) in 2019, which meets twice a year with 14 federal agency representatives and two rotating state representatives from the respective coordinating offices, is intended to facilitate high-level decision-making on AML and CFT policy. The RÜST GW/TF lacks binding authority, and the involvement of state authorities in the process is not formally structured to ensure coordinated participation. In addition, the above-mentioned coordinating offices face challenges due to limited resources, which affect their effectiveness and interregional communication capabilities.

In the area of supervision, some key supervisors are not part of relevant established mechanisms, and supervisors of some DNFBPs sector lack robust coordination mechanisms. Additionally, there is no comprehensive coordination framework on proliferation financing. Given Germany's TF risk profile, there is a lack of active use of the freezing capabilities of the FIU and BaFin, as well as a lack of effective use of targeted financial sanctions (TFS).

In the context of Germany's fragmented federal system, improving cooperation between AML and CFT agencies and the 17 data protection authorities is critical to effective data

integration, advanced analytics, and information sharing, which are key to strengthening AML and CFT efforts.

Furthermore, Germany's decentralized approach to handling international cooperation requests makes it difficult to identify risks, allocate resources, respond in a timely manner, and coordinate across states due to the lack of national records.[532]

Key Countermeasures Implemented

In December 2019, Germany adopted a national AML and CFT strategy, which outlines concrete measures in 11 areas to strengthen the country's AML/CFT system. This strategy reflects a combination of measures that address both international and regional standards and domestic and regional risks. This strategy is updated on a regular basis, with the RÜST GW/TF ensuring that it is up to date.

Germany also has a number of cooperation and coordination mechanisms between competent authorities, such as, with respect to ML, the FIU, the BKA, and the state police authorities, and with respect to TF, ten national security centers, the informal TF working group, the Joint Counter-Terrorism Centre, and the Joint Counter-Extremism and Counter-Terrorism Centre for Combating Extremism and Terrorism. In this context, law enforcement is effectively achieved, for example, through Joint Financial Investigation Groups in each state and the use of task forces. Cooperation between the FIU and law enforcement agencies is enhanced by hospitalization and liaison officers. In addition, supervisory cooperation is promoted through various mechanisms, including a memorandum of understanding between the FIU and BaFin, a federal-state working group for the FIU and supervisors, and state supervisors for specific sectors. In the context of DNFBPs, the Darmstadt Working Group offers a voluntary cooperation platform for all relevant supervisors.

Furthermore, Germany has established comprehensive systems for monitoring and implementing proliferation-related TFS. In this context, an inter-ministerial group coordinates all sanctions issues. Supplementary groups meet semi-annually to discuss export control and sanctions issues, facilitating cooperation on broader proliferation financing issues. The Central Bank, law enforcement agencies, and supervisors also share information to optimize TFS oversight and to identify and investigate potential violations.

With respect to data protection, Germany has established cooperation and coordination mechanisms to align its AML and CFT regime with relevant provisions, including

[532] cf. Financial Action Task Force, 2022, pp. 4, 8-9, 13, 24, 40, 51-53, 55, 67, 72, 115, 129, 182, 234-237, 255-256, 312.

amendments to its AML and CFT framework (§ 51a GwG on the processing of personal data by supervisory authorities).[533]

At the international level, Germany's robust legal framework allows for rapid and high-quality mutual legal assistance, extradition, as well as the recovery of assets. International cooperation is primarily focused on EU member states through regional frameworks such as the European Investigation Order or the European Arrest Warrant. Furthermore, Germany actively cooperates in cases of ML, TF, and predicate offenses, using international networks, liaison officers, and bilateral engagement and both provides and seeks assistance in asset recovery. Moreover, Germany regularly engages in international cooperation for information exchange and supervisory and operational activities, with effective and timely informal cooperation. In this context, the BKA or BaFin, for example, use several channels to cooperate with their foreign counterparts. Furthermore, the FIU maintains robust communication with other international FIUs and consistently and actively participates in global project initiatives and committee work, such as the Egmont Group. Germany also provides partners with basic and beneficial ownership information, subject to the limitations described above.[534]

4.4.5 COVID-19 Pandemic

Increased Risk of Money Laundering

The COVID-19 pandemic has led to diverse government responses that have inadvertently created new opportunities for illicit actors to exploit. These conditions have also fostered an evolving landscape of ML and TF threats. Key among them are the increasing reliance on online platforms for work and social interaction, a surge in online sales and demand for medical products, limited brick-and-mortar banking, and an economic recession. Furthermore, governments have focused their resources on dealing with the COVID-19 crisis, while other areas of focus have received less attention. Traditional criminal activities that exploit global supply chains have also been disrupted by a significant reduction in global trade and individual travel.

In particular, there has been an increase in fraudulent activities such as fundraising scams, where criminals solicit donations for COVID-19-related causes in the name of fake charities, and the counterfeiting of essential goods such as medical supplies, often facilitated by online

[533] cf. Financial Action Task Force, 2022, pp. 10, 29, 39, 51-52, 55-56, 59, 71-73, 233-236, 289; Bundesministerium der Finanzen, 2019, pp. 40, 42; Financial Intelligence Unit, 2022, pp. 58-65; GwG, 2023, § 51a.

[534] cf. Bundesministerium der Finanzen, 2019, pp. 39, 42, 52, 54; Financial Action Task Force, 2022, pp. 6, 13, 28, 92, 213-229; Financial Intelligence Unit, 2022, pp. 76-94.

fraud.[535] Official impersonation has also become a common strategy, with criminals posing as government[536] or hospital officials to obtain payments.[537] Additionally, investment scams have been identified, often claiming that the goods or services offered by publicly traded companies can effectively combat COVID-19.[538]

Cybercrime, including email and Short Message Service (SMS) phishing attacks, business email compromise scams, and ransomware attacks, has also increased, taking advantage of the fears and uncertainties surrounding the pandemic. These attacks often result in the acquisition of personal payment information, for example by introducing malware onto personal devices.[539]

In addition, the pandemic has affected other predicate crimes.[540] The risk of human trafficking and worker exploitation has increased due to the economic downturn and the suspension of regular government oversight.[541] The threat of online sexual exploitation of children has also reportedly increased, in part due to increased use of the Internet by both children and criminals during the shutdown.[542] Furthermore, reports indicate a rise in organized property crime, with a particular focus on medical facilities and commercial space.[543]

During the COVID-19 pandemic, there were significant changes in financial behavior, with more remote transactions due to the temporary closure of physical banking facilities. This poses challenges for identity verification, and some financial institutions may lack the infrastructure necessary for remote authentication, allowing for the concealment and laundering of illicit proceeds. Moreover, a lack of familiarity with digital banking platforms among certain demographic groups, such as the elderly, increases their susceptibility to fraud. In prolonged economic recessions, individuals may seek financing outside of the traditional economy and turn to non-standard or unlicensed lenders, including potentially

[535] cf. Murrar (COVID-19), 2022, p. 5; Financial Action Task Force (COVID-19), 2020, pp. 5-7; United States Department of the Treasury (TF Risk Assessment), 2022, p. 23; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 12-13, 71.
[536] cf. United States Department of the Treasury (COVID-19 Scams), n.d.
[537] cf. International Criminal Police Organization (Fraud linked to COVID-19), 2020.
[538] cf. Murrar (COVID-19), 2022, p. 5; European Union Agency for Law Enforcement Cooperation, 2021.
[539] cf. Murrar (COVID-19), 2022, p. 5; Financial Action Task Force (COVID-19), 2020, p. 7; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 1, 11, 17-21.
[540] cf. Financial Action Task Force (COVID-19), 2020, p. 8.
[541] cf. Buckley, Pietropaoli, Rosada, Harguth & Broom, 2022, pp. 5-9; Lumley-Sapanski & Schwarz, 2022, pp. 147-152; United Nations Office on Drugs and Crime (COVID-19 Pandemic), n.d., p. 1.
[542] cf. Oostrom, Cullen & Peters, 2022, p. 500; European Union Agency for Law Enforcement Cooperation (Exploiting Isolation), 2020, p. 4.
[543] cf. European Union Agency for Law Enforcement Cooperation (How criminals profit), 2020.

criminal groups. This shift could challenge traditional financial regulators with business continuity tasks, while still requiring them to monitor suspicious transactions.

Governments issuing stimulus packages has been a common response to the economic impact of COVID-19. In this context, there have been reports of potential fraudulent acquisition or diversion of these funds for ML purposes. Furthermore, international financial assistance could be adversely affected by corruption within the procurement or aid distribution channels.

Increased financial volatility creates new vulnerabilities. For example, economic downturns may prompt criminals to invest in struggling companies or real estate in order to generate cash and hide illicit funds. As a result, such downturns could also leave the private sector with fewer resources to fight financial crime and lead to an increase in subsistence crimes such as theft and burglary, particularly in developing countries. Additionally, an increase in physical cash transactions has been reported, which can be used as a cover for ML and TF activities, e.g. through the purchase of less traceable assets such as gold. The ML and TF risks associated with the concealment and transfer of illicit funds through virtual assets described above also exist in the context of the COVID-19 pandemic. As financial markets have become more unstable, there has been a reported increase in investor fraud and potential illicit financial market activities, such as insider trading, designed to profit from large fluctuations in value.[544]

Increased Risk of Terrorist Financing

According to the UN, the threat of terrorism remains and terrorist groups may take advantage of the COVID-19 situation to intensify their operations and sources of funding, particularly in the Sahel region.[545] More specifically, criminals could exploit the crisis to raise and transfer funds and to increase illicit activities to finance their objectives.[546] Given the global humanitarian and relief efforts to address the impact of COVID-19, it is critical that governments apply a risk-based approach to prevent the potential diversion of these funds to terrorist activities.[547]

Impact on AML and CFT Regimes

The COVID-19 pandemic has had a significant impact on the ability of governments and the private sector to implement AML and CFT obligations, particularly in countries with limited

[544] cf. Murrar (COVID-19), 2022, p. 5; Financial Action Task Force (COVID-19), 2020, pp. 8-10; United States Department of the Treasury (ML Risk Assessment), 2022, pp. 1, 8-10.
[545] cf. United Nations Secretary-General, 2020.
[546] cf. Financial Action Task Force (COVID-19), 2020, p. 10.
[547] cf. United States Department of the Treasury, 2020.

resources, due to social distancing measures such as widespread remote working and the diversion of resources to the pandemic response.

In this context, on-site AML and CFT inspections have largely been replaced by desk-based inspections. Even if reporting entities continue to comply with AML and CFT obligations and share the necessary data, flexibility has been provided in annual reporting and licensing has been delayed. In addition, various jurisdictions have suspended decisions such as the imposition of AML and CFT-related fines, and new business registrations have been slowed.[548]

The pandemic has also brought new AML and CFT legislative and policy initiatives to a halt, in part because meetings of various legislative decision-making bodies have been suspended or have given priority to COVID-19 emergencies.

Moreover, SARs continued to be filed, mostly without difficulty or delay, but some jurisdictions have allowed for extended filing because of the potential for delays in receiving and processing reports due to, among other things, paper-based reporting systems or inadequate database software.

FIUs remained largely operational, although there are anecdotal reports of reduced activity in countries with lower capacity.

The COVID-19 pandemic has disrupted operational collaboration worldwide, resulting in potential delays due to remote working and reprioritization. Formal cooperation like mutual legal assistance and extradition has been affected by court closures and travel restrictions, and some reports indicate a reduction or suspension of AML and CFT technical assistance.

Law enforcement authorities remain focused on AML and CFT efforts, but the suspension of court operations may result in some prosecutions being deferred. In high-risk, under-resourced countries, these conditions may inadvertently empower individuals involved in terrorist and TF activities.

In addition, financial institutions have activated continuity plans, including branch closures and staff redeployment. Banks in less affected countries face challenges in conducting due diligence on foreign entities. Non-banking sectors such as online gambling and insurance have seen increased activity, while other sectors such as real estate have declined. Money or value transfer services, which rely heavily on face-to-face interactions, have been

[548] cf. Financial Action Task Force, 2022, pp. 44, 49, 175; Bundesanstalt für Finanzaufsicht, 2021, p. 4; Financial Action Task Force (COVID-19), 2020, pp. 11-12; United States Department of the Treasury (ML Risk Assessment), 2022, p. 53.

significantly disrupted. As economic conditions deteriorate, financial institutions may shift their focus from AML and CFT to broader stability measures.[549]

Situation in Germany

In Germany, in the second year of the pandemic, 2021, patterns of fraudulent activity continued, particularly in relation to aid funds and offers of medical products. In addition, new scams emerged that took advantage of changes in government support mechanisms.

Fraudulent activity reported in 2021 was primarily in the form of billing fraud through COVID-19 testing centers. Particularly affected companies used these centers as an alternative source of revenue, leading to potential billing fraud due to ineffective initial controls. By analyzing SARs, the FIU identified individuals with pandemic-related revenue losses and others already implicated in other crimes who were likely to take advantage of fraud opportunities.[550]

Regarding TF and national security crimes, the FIU reported that extremist groups took advantage of the pandemic situation to raise funds, particularly through the use of social media, fundraising appeals, and paid membership. Funding was provided primarily through traditional bank transfers, crowdfunding platforms, and virtual assets.

In the context of Islamism, groups solicited donations to support regions severely affected by the pandemic, with some of these groups and individuals also suspected of fraudulently claiming government COVID-19 aid. Moreover, the entities under scrutiny were previously known for their involvement in related activities within the scene as well as their history of making donation payments in other contexts.

In addition, the movement of alternative thinkers, with a broad spectrum of supporters, protested the government's COVID-19 restrictions. Despite the movement's ideological diversity, it's characterized by an increasingly radical tone, a potential for violence, and an anti-democratic, state-delegitimizing sentiment. In response, in April 2021, the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz) created a new category known as *Delegitimization of the state relevant to constitutional protection* (Verfassungsschutzrelevante Delegitimierung des Staates), which targets key individuals within the alternative thinker scene. In 2021, more than 40 SARs were associated with this new category, mostly involving donations disguised as gifts. The funds are typically held in

[549] cf. Financial Action Task Force (COVID-19), 2020, pp. 12-13.
[550] cf. Financial Intelligence Unit, 2022, pp. 33-34.

cash, used to offset debts or bills, converted into virtual assets, or transferred to other accounts.[551]

Key Countermeasures Implemented

At the onset of the pandemic, Germany kept abreast of the emerging and evolving risks through consistent deliberations in the RÜST GW/TF.[552]

In response, in October 2020, Germany published an independent assessment examining the impact of the pandemic on its AML and CFT infrastructure and proposing future measures.[553]

In addition, BaFin recognized the limitations of physical audits and supervisory visits and adopted alternative digital approaches, such as remote inspections. It also suggested that firms use simplified due diligence procedures where risks allow, for example in the case of state aid loans.[554]

The FIU observed an increase in COVID-19-related SARs and prioritized them. Analysis revealed an increase in online criminal activity, including fraud cases. Based on these findings, the FIU provided a COVID-19-related fraud and ML typology report to obligated parties in May 2020, and reviewed the impact of COVID-19 in the 2021 annual report.[555]

Intelligence and law enforcement agencies established specialized units to address challenges related to COVID-19, including sharing information on emerging risks with international counterparts.

As a result of internal risk considerations, the AFCA has provided a white paper on COVID-19 for registered reporting entities, which has since been updated to reflect new findings, highlighting typologies and warning signs of cybercrime and fraud related to COVID-19.[556]

In 2021, the number of COVID-19-related fraud reports decreased significantly due to stricter documentation requirements for government subsidy recipients and improved control measures.

Furthermore, both regulators and reporting entities have become more adept at identifying process gaps and responding quickly, and cooperation among various relevant entities has

[551] cf. Golindano Acevedo & Pitters, 2021, p. 4; Financial Intelligence Unit, 2022, p. 38.
[552] cf. Financial Action Task Force, 2022, pp. 44, 51; Bundesministerium der Finanzen (Strategie gegen Geldwäsche und Terrorismusfinanzierung), 2020, pp. 5-6.
[553] cf. Financial Action Task Force, 2022, p. 44.
[554] cf. Bundesanstalt für Finanzaufsicht, 2021, p. 4; Financial Action Task Force, 2022, pp. 44, 49.
[555] cf. Financial Intelligence Unit, 2022, pp. 33-38; Financial Action Task Force, 2022, p. 44.
[556] cf. Financial Action Task Force, 2022, pp. 44, 139.

been enhanced to systematically review grant application and disbursement processes to prevent fraud.[557]

4.5 Terrorist Financing Threats and Vulnerabilities and Specific Countermeasures

4.5.1 Misuse of Non-Governmental Organizations and Non-Profit Organizations

Non-governmental organizations and NPOs, which are well-respected and operate globally with substantial financial resources, are attractive targets for TF abuse.[558]

Charitable organizations, which are diverse in nature but share a common mission to improve social conditions, are often the backbone of marginalized communities, human rights advocacy, and the delivery of essential services. They often operate in high-risk zones and challenging environments where even government intervention may be limited. Despite a common denunciation of terrorism, these organizations are not immune from exploitation for illicit activities.

Such exploitation can undermine public trust in charities, although the impact is not evenly distributed across the sector. Charities' high public profile, reliance on voluntary support, diversity and wide reach make them vulnerable to abuse. Their operations in conflict-prone areas or regions with poor infrastructure, combined with complex financial transactions and a wide range of programs, exacerbate this vulnerability. Furthermore, NGOs or NPOs may have irregular and unpredictable financial flows, making it difficult to identify suspicious transactions. They may also operate branches or projects that are not directly supervised or consistently monitored, as well as be subject to varying degrees of regulation around the world. Moreover, they often serve as effective tools for mobilizing individuals around a common goal and collective initiative, inadvertently providing a pre-existing social structure and platform of credibility for individuals spreading terrorism or extremist ideologies.

Additional risk factors, such as the nature of the charity's work, may increase the vulnerability of certain organizations. Thus, the immense diversity of the sector implies varying levels of risk, and the potential misuse of a charity's resources, facilities, and reputation for terrorist activities remains a significant concern.[559]

[557] cf. Financial Intelligence Unit, 2022, pp. 33-34.
[558] cf. Murrar (Non-profit organisations), 2022, pp. 19-21, 25-26; Financial Intelligence Unit, 2022, p. 31; Financial Action Task Force, 2022, p. 101.
[559] cf. Charity Commission, 2022; Financial Action Task Force (Ethnically or Racially Motivated TF), 2021, p. 19; United States Department of the Treasury (TF Risk Assessment), 2022, p. 23; European Commission,

Misuse can occur through the partial diversion of received charitable funds to terrorist groups or through completely fraudulent organizations controlled by these groups that direct all funds to support terrorist activities.[560]

In particular, as noted above, certain charitable organizations are targeted by terrorist groups to exploit their resources, funds, and networks through various methods, including diversion of donations, manipulation of the organizations' authorities, misuse of programs to support terrorist organizations, recruitment assistance, or fraudulent front organizations.[561]

Key Countermeasures Implemented

The NRA in Germany initiated a sectoral risk assessment for NPOs[562] based on a number of relevant sources, such as statistics and sector analyses, SARs and FIU analyses, case studies, information from intelligence services and law enforcement agencies, NPO self-assessments and experiences, and the NRA's own findings. The risks posed by the misuse of legitimate and sham NPOs were assessed separately, and specific characteristics and types of NPOs at high risk of TF misuse were identified.

As a result, there is a high level of understanding and targeted mitigation of TF risks in the German NPO sector using the risk-based approach.

Oversight of the non-profit status of the organization is carried out by the state tax authorities. Additionally, the Federal Office for the Protection of the Constitution has strategies and policies for dealing with high-risk NPOs and the BKA has established a department for religiously motivated terrorism. The German Central Institute for Social Issues (Deutsches Zentralinstitut für soziale Fragen) publishes warnings and reports on organizations identified as engaging in high-risk activities. Moreover, NPOs are subject to registration requirements, annual tax audits, and strict controls on the distribution of government grants. To further increase transparency and prevent abuse, a public register of NPOs is planned for 2024.

Sanctions are imposed for violations of NPO obligations, ranging from public exposure to outright bans on operations, particularly for organizations identified as extremist.

2022, p. 11; Jacobson, 2010, p. 356; Bundesministerium des Innern, für Bau und Heimat, 2020, pp. 20-22, 25-26; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 14.

[560] cf. Financial Intelligence Unit, 2022, p. 31; Bundesministerium der Finanzen, 2019, p. 48; Jacobson, 2010, p. 356; United States Department of the Treasury (TF Risk Assessment), 2022, p. 24; Financial Action Task Force, 2022, p. 23; Bundesministerium des Innern, für Bau und Heimat, 2020, p. 27; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 14, 31-32.

[561] cf. Financial Action Task Force (NPOs), 2014, p. 36.

[562] Bundesministerium des Innern, für Bau und Heimat, 2020.

Faced with de-risking in the banking sector, NPOs are increasingly resorting to less regulated or unregulated channels for transferring funds. To address this vulnerability, Germany is promoting a tripartite dialogue between NPOs, the financial sector, and the government. Furthermore, law enforcement agencies work with vulnerable NPO communities and directly with specific NPOs, often with the support of NPO umbrella organizations.[563]

In the context of international standards, Germany has been assessed by the FATF as largely compliant with FATF Recommendation 8, which contains CFT requirements for NPOs as defined by the FATF.[564]

4.5.2 Abuse of Money or Value Transfer Services

The financial system has also been exploited for TF, often involving large sums of money transferred through standard channels such as MVTS.[565]

Money or value transfer services within the meaning of § 1 (1) Sentence 2 No. 6 ZAG are services in which an amount of money is transferred from the payer to the payee without a payment account being opened in the name of the payer or the payee. In this respect, the 2018 ZAG has adopted the definition of money remittance from the Second Payment Services Directive of 2015[566] as part of its transposition into national law.[567]

Transaction processing through MVTS can be misused for TF, with cross-border transactions to high-risk countries posing heightened risks. The concern is that these funds could be diverted to conflict zones for terrorist use.[568] Terrorist groups typically raise funds from locations far from their operational bases. While traditional banking systems are often used to receive funds, channels that limit detection by leaving minimal trace are preferred in the distribution process.[569] In fact, terrorist organizations such as al-Shabaab, Al-Qaeda, and ISIL have regularly used MVTS to move funds to Somalia, Iraq, and Syria, for example.[570]

[563] cf. Financial Action Task Force, 2022, pp. 4, 8, 10, 19, 29, 50, 102, 125-128, 132, 253; Bundesministerium des Innern, für Bau und Heimat, 2020, p. 9-11, 14-15, 25, 35-36, 44-53; European Commission, 2022, p. 12.
[564] cf. Financial Action Task Force, 2019, p. 10; Financial Action Task Force, 2022, p. 256; Financial Action Task Force (40 Recommendations), 2023, Recommendation 8.
[565] cf. Levy & Yusuf, 2021, p. 1168; Financial Action Task Force, 2022, pp. 21-22; Bundesministerium der Finanzen, 2019, p. 47.
[566] cf. Document 32015L2366, 2015, Art. 4 (22).
[567] cf. Bundesministerium der Finanzen, 2019, p. 88; ZAG, 2023, § 1 (1) Sentence 2 No. 6.
[568] cf. Levy & Yusuf, 2021, p. 1168; Financial Intelligence Unit, 2022, p. 31; Bundesministerium der Finanzen, 2019, p. 58.
[569] cf. Financial Action Task Force, 2022, pp. 9, 22; Bundesministerium der Finanzen, 2019, pp. 46-47.
[570] cf. Levy & Yusuf, 2021, pp. 1175-1176; Financial Action Task Force (Ethnically or Racially Motivated TF), 2021, p. 22; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 22; United States Department of the Treasury (TF Risk Assessment), 2022, pp. 18-19.

Money or value transfer services are critical for those with limited access to traditional banking, often in conflict zones or areas with underdeveloped banking systems, and serve as a financial lifeline for those who depend on remittances for basic human needs. However, like banks, MVTS have been exploited by terrorists for global money transfers. Analysis shows that funds transferred through MVTS were primarily used for travel-related expenses or in connection with international travel. Given their ability to operate efficiently and quickly, minimal account setup requirements, less stringent identity verification for smaller transactions, and global reach, MVTS are expected to remain a common means of transferring terrorist funds.[571]

Furthermore, MVTS are vulnerable to TF because they may inadvertently facilitate the movement of terrorist funds or, in certain cases, complicit employees may intentionally engage in TF activities, in violation of relevant regulations and laws as well as the MVTS provider's AML and CFT protocols and policies. Complicit employees pose a particular challenge to MVTS providers operating through agents as they have a less direct relationship with the MVTS provider. This risk is heightened for smaller MVTS providers or those that offer financial services as an adjunct to their core business, such as check-cashing convenience stores. The limited resources available to MVTS providers can also result in inadequate AML and CFT controls, particularly for smaller MVTS providers that engage in person-to-person online money transfers without a full understanding of the TF risks. Effective compliance and oversight are therefore critical to addressing these issues. Moreover, detecting TF is challenging for MVTS providers without the assistance of law enforcement because transactions often have no visible connection to terrorism. Another risk is posed by MVTS provider’s partnerships with foreign agents or MVTS providers, particularly in conflict countries where terrorist groups are active and access to traditional banking is limited. In such regions, MVTS may serve as the dominant financial institutions facilitating cross-border remittances due to the lack of other options. In addition, the informal and cash-centric nature of some MVTS can make them vulnerable to TF risks.[572]

Islamic terrorist groups often use unconventional MVTS, including hawala banking, to raise funds. By their nature, these transfer systems pose a risk of facilitating TF, but informal systems pose a particularly potent risk because they often operate outside the conventional financial sphere and facilitate long-distance money transfers. They typically rely on trust, or

[571] cf. Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, pp. 21-22; United States Department of the Treasury (TF Risk Assessment), 2022, p. 18.
[572] cf. United States Department of Justice, 2021; United States Department of the Treasury (TF Risk Assessment), 2022, p. 19; Financial Action Task Force (Emerging Terrorist Financing Risks), 2015, p. 22; Bundesministerium der Finanzen, 2019, pp. 47-48, 68, 71, 89, 91.

operate in areas where banking systems are underdeveloped. Hawala banking, for example, is used for legitimate transactions, but it has also been used by terrorist groups to move funds with minimal detection. Because of the extensive network and scarce documentation associated with hawala banking, tracking these transactions is extremely difficult. Approximately USD 200 billion a year is moved through these systems worldwide, most of which, however, is not suspected of being TF. In Germany, the unlicensed operation of MVTS is punishable by law and prohibited by BaFin.[573]

Key Countermeasures Implemented

Under the ZAG, BaFin licenses and supervises providers of MVTS in Germany, including natural and legal persons, and investigates and sanctions unlicensed activities or violations of licensing requirements. Penalties can range from up to five years imprisonment or an unspecified fine to the suspension of business operations. Additionally, the BaFin monitors compliance with the GwG by MVTS providers as obligated parties.

Agents for MVTS providers must register with BaFin, and the respective providers are responsible for providing BaFin with the required agent information and updating any changes, as well as an overview of the agent's internal control systems, and for ensuring that these agents comply with the legal requirements.

With regard to the FATF assessment, Germany was rated as largely compliant with FATF Recommendation 14 on MVTS.[574]

Several multinational MVTS providers have advanced programs to detect potential TF, contributing to the fight against terrorism and its financing. Moreover, these companies may limit the size or number of transactions in higher risk areas.[575]

[573] cf. Rahimi, 2021, p. 146; Bundesministerium der Finanzen, 2019, p. 47; Financial Action Task Force, 2022, pp. 21, 23.
[574] cf. Financial Action Task Force, 2022, p. 265; Bundesministerium der Finanzen, 2019, pp. 58, 90. ZAG, 2023, §§ 7-8, 10 (1), 11 (1), 25, 63-64; GwG, 2023, §§ 2 (1), 50; Financial Action Task Force (40 Recommendations), 2023, Recommendation 14.
[575] cf. United States Department of the Treasury (TF Risk Assessment), 2022, p. 18; Bundesministerium der Finanzen, 2019, p. 74.

5 Approaches for Improvement in Combating Money Laundering and Terrorist Financing in Germany

5.1 Adapting the Kotter Framework for Sustainable Change

The comprehensive examination of current AML and CFT threats, vulnerabilities, and countermeasures in Germany highlights existing gaps and challenges in both understanding and addressing these issues. Therefore, the following chapters focus on different approaches to combating these illicit financial activities, with the goal of identifying effective strategies to strengthen Germany's defenses against these criminal practices.

Given the dynamic and complex nature of AML and CFT, applying a change management model to analyze and propose actionable changes enables successful transformation. Specifically, the Kotter Model serves as the theoretical framework for structuring the proposed improvements. The Kotter Model outlines an eight-step process for effective change, which is often aggregated intro three major phases:

- Phase 1: Creating a Climate for Change
    - Step 1: Create Urgency
    - Step 2: Build Coalition
    - Step 3: Create Vision
- Phase 2: Engaging and Enabling Stakeholders
    - Step 4: Communicate Vision
    - Step 5: Empower Others
    - Step 6: Generate Quick Wins
- Phase 3: Ensuring Sustainable Change
    - Step 7: Sustain Acceleration
    - Step 8: Institute Change[576]

For the purposes of this dissertation, the three major phases are used to make the approach more flexible, rather than seeing it as a sequential approach from step one to eight. Therefore, the suggested approaches for improvement are categorized in these three phases to allow for a successful and comprehensive transition to an effective AML and CFT framework.

It should be noted that while specific threats and vulnerabilities were identified in the previous chapter, this section aims to address high-priority, overarching measures that can

[576] cf. Kotter, 2012; Kotter, n.d.; Reiling, 2022.

improve the overall risk landscape associated with ML and TF in Germany. As such, there is not a one-to-one correspondence between individual risks and the proposed measures.

5.2 Creating a Climate for Change

5.2.1 Political Prioritization

Combating ML and TF is not only a matter of regulatory due diligence, but also requires a country's commitment to global financial security and transparency. The importance of addressing ML and TF issues requires that these issues be given high priority, including a holistic, multi-level approach. The role of the federal and state governments in this context is therefore of great importance.

At the top of the political hierarchy, there must be a deep commitment from both the federal and state governments. This commitment should not be a mere statement of intent, but rather requires ongoing accountability that fosters a culture of continuous collaboration in risk assessment and understanding, strategic mitigation, and prudent resource allocation.

At the official level, the role of the RÜST GW/TF is important and should be given a binding and formal mandate. Furthermore, the relevant authorities should be adequately represented, in particular tax authorities and support mechanisms that mobilize the participation of state governments.

However, AML and CFT efforts should not be exclusively top-down. There is a need to institutionalize the state coordinating offices and empower them with the authority and resources to ensure seamless synergy and coordination between the national and regional architectures, from policy formulation to field operations, including oversight and law enforcement directives.[577]

Conclusion and Further Recommendations

As described above, it is clear that political prioritization of the fight against ML and TF is critical to its success, and that federal and state governments in particular play a key role in this regard.

But while mechanisms, mandates and cooperation have been highlighted, a gap that requires attention is the element of communication. An effective AML and CFT framework is not only built on rules and regulations, but is deeply rooted in awareness and understanding

[577] cf. Financial Action Task Force, 2022, p. 14; Transparency International Deutschland e.V., 2022.

among stakeholders. In this context, one of the key criticisms is the reluctance of public institutions to articulate the profound significance of their initiatives.

For any transformative initiative to gain traction, the *why* and impact of its existence must be robustly articulated. Drawing parallels from successful change management paradigms in the corporate world can provide valuable insights. As a benchmark, complex IT or integration projects, such as the creation of a registry, platform or national integration of new communications technologies and frameworks, allocate nearly half of their budget to change management efforts. The same approach, with a significant increase in budget, could be catalytic in the AML and CFT arena. Prioritizing communication campaigns can reinforce the awareness matrix, leading to an activated stakeholder ecosystem. Coupled with specialized training and support, this can communicate the benefits and create an environment of informed and proactive participation.

Overall, the cascading effect of political commitment and prioritization is a key element in the fight against ML and TF. Its success and effectiveness will be enhanced by better communication, which can turn passive acceptance into active support for Germany's defense against ML and TF.

5.2.2 Reforms in Registration Systems and Legal Entities

To improve the accuracy of beneficial ownership data, the above-mentioned revisions to the transparency register should be fully implemented, with a focus on discrepancy reporting and re-registration compliance. Therefore, given the central role of the transparency register in maintaining up-to-date and accurate beneficial ownership data, a rigorous enforcement strategy, including dissuasive sanctions, should be put in place. In this regard, the transparency register requires the necessary human and technical capacity for updates and to efficiently manage large data submissions.

Germany must also improve its understanding of legal entities and arrangements related to ML and TF. A focus should therefore be placed on investigating the risks associated with foreign beneficial owners and shareholders, in particular foreign legal entities linked to German counterparties. Additionally, a comprehensive risk assessment of legal entities and arrangements should be conducted, combining knowledge of their vulnerabilities from the sector-specific risk assessment with empirical data on their misuse for ML and TF purposes collected from various stakeholders, including the FIU and the private sector, law enforcement and supervisory authorities.

In addition, it is critical to evaluate and implement additional risk mitigation strategies to address the vulnerabilities associated with bearer shares and nominee shareholders. In this context, there is a need to reduce the prevalence of bearer shares and promote their conversion to registered shares for greater transparency. At the same time, mechanisms to improve the enforcement of obligations should be put in place to address the risks associated with nominee shareholders and potential non-registration of beneficial ownership in the transparency register.[578]

Germany should make use of the automated account retrieval system and ensure that all relevant authorities, in particular the FIU, have direct automatic access, e.g. to increase requests when analyzing the beneficial owners of legal entities in connection with ML or TF.

Legal arrangements such as GbRs, which are currently outside the scope of full data access, must be integrated into an appropriate framework. This will ensure that authorities have timely access to the information they need, such as basic or beneficial ownership information, in accordance with FATF standards. While partnership law reforms have been passed in Germany, they will not take full effect until 2024, and requirements such as registration have yet to be fully implemented. In addition, legislative changes should be regularly reviewed, including to confirm their appropriateness and consistency with the FATF Recommendations.[579]

Using advances in technology, existing registries should be consolidated and synchronized to eliminate multiple overlapping records and improve data accuracy. This consolidated approach would therefore allow for greater transparency of property ownership without creating additional registries.[580] Given the possibilities offered by big data, innovative strategies should be adopted to improve transparency and ultimately combat ML and TF.[581]

Conclusion and Further Recommendations

The German registration systems and legal entities play a key role in the fight against ML and TF. Improving the accuracy of beneficial ownership data through methodological reforms of the transparency registry is necessary. Coupled with a rigorous enforcement strategy and backed by the right mix of human and technical capabilities, these reforms will

[578] cf. Knobel, 2023, pp. 18-21, 24; Financial Action Task Force, 2022, pp. 14, 199.
[579] cf. Financial Action Task Force, 2022, pp. 14, 198-199; Bundesrat (Verordnung), 2022; Bundesrat (Empfehlungen), 2022; MoPeG, 2021, Art. 137.
[580] Some call for a centralized land registry, see for example: Deutscher Bundestag (Lesung), 2022; Deutscher Bundestag (Antrag), 2022.
[581] cf. Transparency International Deutschland e.V., 2021, p. 22.

not only ensure compliance but also reduce the risks associated with ownership discrepancies.

The complex landscape of legal entities, especially those with foreign connections, presents a challenging threat. Addressing it requires a deeper understanding of their role and vulnerabilities in ML and TF. Drawing on sector-specific risk assessments, empirical data, and insights from multiple agencies, a deeper understanding that facilitates the detection and mitigation of potential threats can be gained.

Bearer and nominee shareholders, with their unique risk profiles, require special measures. Beyond legislative measures, such as banning such shareholdings, a broader cultural shift towards transparency and accountability is needed in this context. The move towards registered shares and the establishment of enhanced enforcement mechanisms could be crucial in curbing potential abuses.

Germany's use of the automated account retrieval system, with a focus on providing direct access to the FIU, is a strategic step in the fight against ML and TF. However, its effective use requires the implementation of robust cybersecurity measures to protect data integrity. Ongoing training of FIU personnel is also essential to ensure the skillful use of this technology. Regular system reviews should be conducted to ensure that the tool remains up-to-date with the latest financial developments.

With regard to concerns related to legal arrangements such as GbRs, mechanisms should be put in place to bridge any information gaps until the full implementation of the partnership law reforms. Furthermore, Germany should consider drawing on the experience and best practices of international FIUs to ensure a holistic and effective integration of all legal entities in its data access framework. Regular review mechanisms should also be put in place to monitor legislative changes.

In today's digital age, technological advances offer transformative solutions. Its use, especially in data management and retrieval, can streamline operations, eliminate redundancies, and strengthen data accuracy. In particular, the potential of big data can renew the approach, adding unprecedented depth to transparency efforts and further strengthening resolve in the fight against ML and TF. Moreover, the private sector is a reservoir of innovation. By building strategic partnerships, especially with large technology companies and innovative startups, new solutions can be developed, from cloud technologies and AI-driven analytics to secure blockchain infrastructures. Building on this, the age of big data, with its vast capabilities, is leading to a rethinking of current strategies. Rather than simply consolidating existing databases, there is potential to learn from data, make invisible patterns

visible, and predict and model future financial landscapes. New technologies, methodologies, and an emphasis on an agile mindset can help not only ensure transparency, but also prevent potential financial crime.

In addition, public awareness and active stakeholder engagement can play a critical role. Fostering an informed population can create an enabling environment characterized by robust compliance. Establishing regular review mechanisms will ensure that reforms remain agile and responsive to the evolving nature of ML and TF challenges. Training programs that bring together different agencies can contribute to a harmonized approach by improving collaboration and communication.

At the global level, collaboration with international partners can be a source of insight, best practices and shared knowledge. Therefore, aligning strategies with international standards can strengthen joint efforts.

Ultimately, periodic technology audits act as an evaluative check, identifying potential weaknesses while providing opportunities for continuous improvement. Such audits should also include technology diffusion assessments and effectiveness audits, which examine both the extent of technology use and its actual impact in relation to its intended objectives.

In sum, a mix of legislative measures, technological capabilities, and collective efforts, all aimed at transparency and accountability, can provide a solid foundation against ML and TF.

5.3 Engaging and Enabling Stakeholders

5.3.1 Money Laundering Detection, Investigation and Prosecution

Effectively combating ML and TF in Germany requires a robust and focused approach to ML detection, investigation, and prosecution. This includes prioritizing ML as a crime separate from predicate offenses and improving the prioritization and understanding of high-risk cases, such as those involving legal entities or foreign predicate offenses.[582]

In order to facilitate the investigation of complex ML models, especially in cases with international links, it is crucial to lower the thresholds for establishing initial suspicion, which is often hampered as described in chapter *4.3.10 Lack of Investigative Capacities*. For example, SAR standards that take into account all the particularities of financial transactions and deviations from the normal business conduct of economic actors could be adopted for initial suspicions in criminal proceedings, as proposed by the German Federal Prosecutor

[582] cf. Financial Action Task Force, 2022, p. 14.

General (Generalbundesanwalt). In this context, anomalies in business operations could compensate for a lack of evidence of a potential catalog offense. However, according to the Federal Constitutional Court's decision, separating the initial suspicion from the associated predicate offense is not considered effective in the context of German law. Therefore, in the same way that establishing links to a terrorist organization as a criminal offense serves as a catalyst for investigations under terrorism law, serious violations of the GwG should be defined as a separate offense that allows for ML investigations independent of the predicate offense. The classification of these serious violations can be influenced by both monetary parameters and structural characteristics, similar to the approach used for major tax evasion cases.[583]

In addition, a more comprehensive statistical basis should be ensured in order to improve the understanding of the problem, particularly in high-risk areas. In this regard, asset recovery should be tracked in a more transparent manner, categorized by offense, assets involved, and each step leading to final confiscation.[584] Furthermore, the FIU should conduct a more detailed evaluation of the results of the procedures related to SARs, including the type of information contained in the SARs, an analysis of the time of reporting in relation to the reported transaction, the scope of the reported transactions, and the assets subsequently seized.[585] While the separate documentation of ML statistics related to serious predicate offenses may distort the data at the expense of relevant cases where AML efforts were secondary, it may also promote a more thorough understanding of the scenario. In general, there is a need to improve criminal and legal statistics beyond ML. Suggestions include standardizing legal bases, conducting regular victim surveys, and improving academic access to statistics, as well as regular, comprehensive statistical analysis of various data sources, including police and judicial records.

Moreover, conducting proactive financial investigations can be a useful strategy, including the examination of real estate-related ownership structures and financial flows, with a particular focus on anonymous ownership or cash transactions. In this context, an in-depth study of the operations and revenues of cash-heavy companies, cross-referenced with the results of tax audits, would help identify patterns and avenues of abuse. Additionally, an analysis of the register of bank accounts maintained by BaFin and the capital flows recorded by the Central Bank would clarify the extent of hidden financial transactions. Such a deeper

[583] cf. Transparency International Deutschland e.V., 2021, p. 26.
[584] cf. Ibid., p. 14.
[585] Pursuant to § 42 GwG, the FIU receives information on the outcome of all proceedings related to SARs (cf. GwG, 2023, § 42).

understanding is critical to risk-informed AML management and to maintaining a continuously improving system.[586]

Effective detection, investigation and prosecution of ML also requires more specialized investigators and prosecutors. Examples at the state level show that they can be established at different levels and in different forms, such as a task force of the Ministries of Finance, Interior and Justice, a central and contact point for the prosecution of organized crime, or focal points in individual prosecutors' offices, as well as a special organization combining the BKA, the State Prosecutor's Office and the state financial administration. In this context, the federal government should coordinate and monitor all states to ensure regular and consistent progress.

It is also crucial to allocate additional human resources to conduct relevant investigations and facilitate asset recovery. It is expected that the judiciary will set limits in its jurisprudence where the predicate offenses are again relevant. Therefore, it would be more prudent to set these limits in law, for example by defining minimum thresholds independent of the predicate offenses. Furthermore, enhanced European cooperation should focus on strengthening investigative capabilities for cross-border cases. In this context, the federal government should strengthen its coordination efforts across different administrative levels, such as districts, municipalities, and states, to trace and repatriate illicit funds from abroad.[587]

Conclusion and Further Recommendations

The proposed methods for strengthening the detection, investigation, and prosecution of ML in the German context represent an intersection of several avenues for improvement, each of which is critical to the overall effectiveness of AML and CFT efforts.

It concludes that separating ML from its predicate offenses can be one way to set the stage for more effective enforcement. This separation can allow for the development of more precise tools and mechanisms for detection, while fostering a culture within law enforcement that views ML as a distinct crime with its own complexities and required expertise.

Achieving such a cultural shift, however, requires not only a change in policy, but also capacity building, particularly in terms of human resources, with the recruitment and training of specialized investigators and prosecutors dedicated to AML. It also underscores the need

[586] cf. Transparency International Deutschland e.V., 2021, pp. 14-15; Rat für Sozial- und Wirtschaftsdaten, 2020; Deutscher Bundestag, 2018.
[587] cf. Transparency International Deutschland e.V., 2021, pp. 26-27.

for state and federal governments to play a central coordinating role, facilitating consistent progress across jurisdictions and ensuring uniform application of AML laws.

At the same time, greater investment should be made in proactive financial investigations. As identified, these investigations have the potential to uncover complex ML schemes, particularly those with international links. The potential benefits of this approach should be further explored, with a focus on how to overcome existing legal and practical barriers.

On a broader level, there is a need to refine the understanding and application of statistical data in the AML arena. Improvements in the collection, categorization and analysis of data can enhance the understanding of problems and the subsequent formulation of targeted responses. Transparent and standardized tracking of asset recoveries, as well as comprehensive analysis of SARs, can reveal patterns, trends, and potential loopholes. In addition, Germany can improve the detection, investigation and prosecution of ML through the development of a learning system, for example by examining ownership structures, evaluating cash-intensive business models and analyzing hidden financial transactions.

In this context, the introduction of innovative technologies should be considered. Artificial intelligence and machine learning have potential in predictive policing, fraud detection and network analysis that would significantly enhance current AML and CFT practices. Such technologies could automate the analysis of large data sets, identify suspicious patterns more quickly, and help investigators focus their efforts on high-risk cases. However, strong oversight and clear guidelines must be established to ensure ethical use, protect privacy rights, and prevent discriminatory practices that may arise from algorithmic biases.

Asset recovery should also be pursued more vigorously, recognizing the potential influence of the judiciary on the process. Legislative measures should be considered to provide clear parameters for such procedures.

Finally, international cooperation and information sharing must be an integral part of the approach to combating ML and TF. Given the inherently transnational nature of these crimes, national efforts should be complemented by robust cross-border initiatives, which may include proactive financial intelligence sharing.

While this analysis attempts to encapsulate the critical facets of AML and CFT enforcement in Germany, it also recognizes the volatility and complexity of the issue. As such, it is essential to maintain a learning and evolving system that is responsive to emerging trends and able to refine strategies based on evolving realities in order to be sustainable and

effective in the long term. The path to a more effective AML and CFT regime is one of continuous improvement and innovation, which should be considered in future efforts.

5.3.2 Financial Intelligence

The nature of the challenges in the fight against ML and TF, such as the complex dynamics of today's financial systems and rapidly evolving technological platforms, underscores the need to strengthen financial intelligence as a primary tool in the fight against these illicit activities.

Therefore, current discourse suggests improving the availability and utility of financial intelligence in the fight against ML and TF. One way to do this is to further expand the FIU's access to comprehensive data sets and advanced analytical tools. Such enhancements would increase the effectiveness and efficiency of the FIU's analyses.

In addition, expanded access to tax data would strengthen the FIU's capabilities. Since much of the ML in the non-financial sector is detected during thorough tax audits, tax authorities should integrate ML risks into their audit strategies and promote cooperation with AML authorities and the police.

Furthermore, the federal government should provide access to state-level police databases to bridge the gap until national integration becomes feasible. Exploring additional ways to share non-personal market data with government agencies or private companies, such as through a state financial data platform, can provide valuable insights.

It is crucial to enhance cooperation and synergy between the FIU and law enforcement agencies to ensure that the FIU's intelligence models and tools effectively meet the operational needs of law enforcement agencies. In general, the above measures would enable the FIU to conduct effective in-depth analysis and assist law enforcement and supervisory authorities in the timely and targeted detection of suspicious activities. In this context, the quality and speed of processing should be continuously assessed in order to improve the FIU’s analysis.[588]

Another strategy to overcome the limitations of the current system in efficiently communicating suspicious activity data to law enforcement could be a two-pronged reporting method. The first category would be rapid unusual activity reports that address transactions that raise red flags or involve high-risk sectors. These reports, without in-depth

[588] cf. Stroligo, Hsu & Kouts, 2018, pp. 13-20; Financial Action Task Force, 2022, p. 14; Bundesministerium der Finanzen (Strategie gegen Geldwäsche und Terrorismusfinanzierung), 2020, p. 10; Bundesrechnungshof, 2020, p. 14; Transparency International Deutschland e.V., 2021, pp. 19-20; Bundesministerium der Finanzen, 2019, p. 41.

analysis, would support the FIU's strategic analysis without burdening business relationships. The second category would be comprehensive SARs, based on extensive analysis by reporting entities, that indicate probable ML, fraud, or links to specific criminal activities.

Finally, the current expectation that the FIU or law enforcement can conclusively determine the viability of a crime within a few days should be critically evaluated. Where there is reasonable suspicion, transactions should potentially be prohibited in principle. To ensure the constitutionality of the FIU's operations, especially when it operates outside the scope of suspicion, potential data sharing with law enforcement should be limited to cases that the FIU deems highly significant.[589]

Conclusion and Further Recommendations

The importance of expanding the availability and applicability of financial intelligence cannot be understated. The discourse suggests that it is imperative to provide FIUs with broader access to comprehensive data sets and advanced analytical tools. Such advances would improve the accuracy and effectiveness of FIUs' assessment capabilities. Consequently, the integration of more tax data into FIU operations, coupled with the promotion of symbiotic relationships between tax authorities and AML units, emerges as a prudent strategy.

Moreover, the case for a more harmonized relationship between the FIU and law enforcement is needed. Their synergy is paramount to ensure that intelligence models and methodologies meet the needs of the law enforcement operational framework. To facilitate effective cooperation between the FIU and law enforcement agencies, a structured feedback mechanism should be established whereby law enforcement agencies can provide regular feedback to the FIU to ensure that the information provided remains relevant and actionable. In addition, the two-pronged approach to reporting can reduce or eliminate the communication barriers of the current system. Given the transnational nature of these crimes, forging stronger links with international financial intelligence units can also provide a holistic picture and deter cross-border illicit activity.

Collaboration with the private sector can unlock a vast amount of non-personalized market data, providing a new perspective on how to detect financial irregularities. Therefore, a

[589] cf. Vogel (EU Anti-Money Laundering), 2020, pp. 985-989; Financial Action Task Force, 2022, p. 14; Transparency International Deutschland e.V., 2021, p. 20.

public-private partnership could combine the advantages of government and the private sector in terms of technology and innovation-driven AML and CFT.

Another concern is the expectation that FIUs and law enforcement will be able to conclusively determine the feasibility of a crime in an often limited timeframe. This needs to be critically examined. The implication is not simply to extend the timeframe, but to ensure that both entities operate under realistic and pragmatic expectations. Any initiatives should be based on a balance between upholding constitutional rights and achieving operational efficiency.

Moreover, the integration of emerging technologies, particularly AI, can enhance the analytical capabilities of FIUs by scanning large volumes of financial data and identifying hidden patterns and anomalies that may elude traditional analytical techniques. This capability could transform the landscape of AML and CFT operations, providing them with unprecedented speed and accuracy. In this context, large language models could be developed specifically for AML an CFT.[590] These models can serve as instant assistants to operators particularly trained in ML and TF topics, capable of rapid data analysis and generating human-like linguistic responses or quick visualizations. Such integration also facilitates more accessible and interpretable results for stakeholders. However, careful oversight is critical to ensure the ethical use of these technologies and to mitigate potential bias or misuse. Furthermore, blockchain's secure and encrypted framework can facilitate protected data dissemination, ensuring confidentiality in information sharing and tamper-proofing.

In addition, emphasis should be placed on the continuous training of FIU personnel. Incorporating capacity-building exercises provides staff and affiliated law enforcement agencies with the opportunity to familiarize themselves with financial intelligence methods and tools. Such an investment in knowledge capital not only ensures a proactive stance against emerging financial threats, but also strengthens the institutional resilience of agencies tasked with combating ML and TF, enabling them to stay ahead of the curve.

[590] For example, by analogy with BloombergGPT, Bloomberg's 50-billion-parameter large language model built specifically for finance, see: Bloomberg Finance L.P., 2023.

5.3.3 Measures against Cash-based Money Laundering and Terrorist Financing

5.3.3.1 Legal Cash Limits with Reporting and Monitoring

As noted above, Germany has a strong attachment to cash and many transactions are made in cash. In order to combat ML and TF, several countries, including EU countries, have introduced cash transaction limits starting at EUR 500, for example in Greece. Transactions above the limit require a cashless payment method. To date, there are no such general cash transaction limits in Germany.[591] Only in the real estate sector has the EUR 10,000 cash limit been introduced (see chapter *4.3.1 Real Estate*).

However, the European Commission has put forward a proposal for a regulation[592] to set a cash transaction limit of EUR 10,000 for commercial transactions, with individual countries allowed to set lower thresholds. In early December 2022, the EU member states in the Council of the EU reached a consensus on this proposal for a new regulation. The purpose of such a limit is to discourage the use of unusually large amounts of cash in individual transactions, a step aimed at mitigating the risks related to ML, its predicate offenses and TF.[593] At the end of March 2023, the relevant members of the European Parliament expressed their intention to support a further reduction of the cash payment limit to EUR 7,000 in the final discussions with the member states and the Commission.[594]

In Germany, this cash limit is controversial. Germany abstained in the Council vote due to divergent positions within the federal government. Despite the above-mentioned positive objective, critics argue that it could undermine civil liberties, encourage cybercrime, and lead to hidden price increases due to transaction fees for cashless payments. In particular, questions arise about the protection of financial privacy, the freedom to transact and the accessibility of banking services. In addition, a lack of empirical research on the effectiveness of cash limits in the fight against ML and TF is claimed.[595]

[591] cf. Schroth & Vyborny, 2022, pp. 112-113; Financial Action Task Force, 2022, p. 7; European Consumer Centre France, 2022.
[592] Proposal for a Regulation of the European Parliament and the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 2021.
[593] cf. McGuinness, 2023; Council of the European Union, 2022; Transparency International Deutschland e.V., 2021, p. 19; Ecorys, 2019.
[594] cf. European Parliament (New EU measures), 2023; Bayerisches Staatsministerium der Finanzen und für Heimat, 2023.
[595] cf. Rivera, 2019, pp. 354-357; Passas, 2018, pp. 11-17; Buyse, 2023; Bayerisches Staatsministerium der Finanzen und für Heimat, 2023; European Parliament (Parliamentary question), 2023.

Therefore, in order to accommodate individuals who do not have access to banking facilities and to ensure that they can still purchase services and goods, the proposal includes an exemption for transactions carried out on the premises of credit institutions. Furthermore, under Directive 2014/92/EU[596], legal residents of the EU are entitled to a basic payment account to promote financial inclusion. Additionally, the imposition of a limit on high-volume cash transactions is not expected to significantly compromise the financial privacy of individuals or increase the likelihood of other crimes, such as cybercrime. The average transaction value, which includes both cash and non-cash payments at points of sale or between individuals within the Euro Area, is EUR 25.55, which is significantly lower than the proposed cash transaction limit.[597]

Furthermore, mandatory reporting mechanisms for large cash transactions below the cash threshold could be a complementary option to reduce them and mitigate the risks of ML and TF. This should be accompanied by closer monitoring of cash movements leaving Germany and a better understanding of the risks associated with cross-border cash movements. Another strategy could be the anonymous and strategic recording of banknote serial numbers, a practice occasionally used in law enforcement, customs authentication or certain business processes.[598]

5.3.3.2 Promotion of Cashless Payments

Electronic payments offer benefits to both businesses and the economy. Key benefits include ease of use, which can increase revenue, increased security, simplified administration, cost efficiency and the potential to attract more customers.[599]

In addition, there is a growing consumer preference for electronic payments, particularly among the younger generation, due to the speed, ease and security of transactions.[600] In the retail sector, for example, the share of card payments has steadily increased in recent years, while cash payments have steadily declined.[601]

[596] Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, 2014.
[597] cf. McGuinness, 2023; Carvalho, Garcia, Hansen, Ortiz, Rodrigo, Rodríguez Mora & Ruiz, 2021; Transparency International Deutschland e.V., 2021, p. 19; European Central Bank, 2020, p. 27.
[598] cf. Transparency International Deutschland e.V., 2021, p. 19; Financial Action Task Force, 2022, p. 14; also discussed by: Naheem (Combating money laundering and terrorist financing), 2019, pp. 235-239.
[599] cf. Najib & Fahma, 2020, p. 1707; Kumari & Khanna, 2017, pp. 82-83, 85, 87, 95, 97; Economie, 2023.
[600] cf. Kadir, Shamsuddin & Rosa, 2015, p. 183; Economie, 2023.
[601] cf. Ahrens, 2023.

The COVID-19 pandemic has also accelerated the shift to contactless payments in Germany. Since the start of the pandemic, 26 percent of Germans have decided to stop using cash in shops, according to a survey by the Association of German Banks in 2020.[602]

In the context of reducing the use of cash for payments to mitigate the risks of ML and TF, Germany could therefore promote the use of digital payments to pave the way for a cashless society. One way to encourage cashless payments is through a legal obligation to offer digital payments. For example, as of July 1, 2022, Belgian law requires all consumer-facing businesses under Book VI of the Commercial Code to offer at least one electronic payment solution. Businesses are free to use any suitable electronic payment method, such as contactless payments, fixed terminals or bank transfers. They cannot charge extra for electronic payments or refuse them for transactions below a certain limit. This amendment is driven by the growing consumer preference for electronic payments and the fight against tax fraud.[603]

Another possibility to accelerate the transition to cashless transactions in Germany includes targeted incentives for digital payments. Customers could receive a direct discount of, for example, 0.75 percent of the purchase value when purchasing selected items digitally. In addition, bonus programs have been implemented in other countries, where digital payments are used to collect bonus or loyalty points for future discounts or other benefits, such as payment by points. Points earned could also be used for sustainable or social features, such as supporting green initiatives or giving to others.[604] Tax benefits for card payments, such as the establishment of a tax lottery that automatically records card payment receipts or partial VAT refunds or, are also options that have been implemented by various countries.[605] The combined impact of these incentives could significantly increase the adoption and penetration of cashless transactions in the economy.

Digital payment methods often incur various costs to the merchant, such as the cost of acquiring the devices or transaction costs of a certain inconsistent percentage, which is a reason for some to prefer cash, especially for small amounts.[606] In this regard, the European Commission has proposed measures to promote the use of the Euro as both a physical and a digital currency. These measures aim to ensure the accessibility and usability of Euro

[602] cf. Kotkowski & Polasik, 2021, p. 1; Bundesverband deutscher Banken, 2020, p. 3.
[603] cf. Economie, 2023.
[604] cf. Okina, 2022, p. 117; Chaudhuri, Gathinji, Tayar & Williams, 2022; Massi, Sullivan, Strauß & Khan, 2019; Jagtap, 2017, p. 4; Bilińska-Reformat & Kieżel, 2016, pp. 7-9.
[605] cf. Perciun, Iordachi & Timofei, 2020, p. 643; His Majesty's Treasury, 2019, p. 27.
[606] cf. Cabinakova, Knümann & Horst, 2019, pp. 84-108; Massi, Sullivan, Strauß & Khan, 2019; His Majesty's Treasury, 2019, pp. 5-6.

banknotes and coins, while creating a framework for a potential digital Euro, taking into account the increasing digitalization. The proposal for a digital Euro, which aims to provide consumers with more transaction options through a public, widely accepted, secure, low-cost and resilient alternative to private digital payment options, while ensuring privacy and data security, is subject to approval by the European Parliament and the Council, with the European Central Bank taking the final decision on whether to issue a digital Euro. Other positive aspects of the digital Euro are that it potentially strengthens the international role of the Euro, safeguards the monetary sovereignty of the EU and provides a basis for innovation.[607] The Swedish Riksbank is also considering the introduction of a digital currency, the e-krona, to adapt to these evolving payment trends. Sweden is a pioneer of a cashless society, and its transition has been greatly facilitated by the mobile app Swish, which enables instant payments between individuals. Together with Swedish fintech companies such as Klarna, Zettle or Trusty, as well as the Swedish BankID, this has led to a significant reduction in the use of cash.[608]

In addition, to effectively promote cashless payments, Germany could benefit from government-initiated educational initiatives. These campaigns would aim to explain the benefits of digital transactions to both consumers and merchants.[609]

Conclusion and Further Recommendations

The introduction of a cash transaction limit, even lower than the EUR 10,000 proposed by the EU, as in other EU countries, is a step towards curbing ML and TF. Given Germany's cultural bias toward cash, the transition may present a unique set of challenges. However, the potential benefits of a cashless society, such as improved traceability of transactions and reduced opportunities for illegal activities, are compelling and should be further considered as a measure against ML and TF.

Despite concerns about individual financial freedom and privacy, it should be emphasized that the proposed limit far exceeds the average transaction value, suggesting that everyday transactions would not be affected. Given Germany's deep-rooted cash-based culture, the country could benefit from a phased approach, allowing for a gradual transition that reduces social resistance while optimizing the effectiveness of AML and CFT measures. In addition, a cash transaction limit could be made more acceptable and effective by including specific

[607] cf. Thießen, 2021, pp. 529-531; Berentsen, 2020, pp. 2-6; European Commission (Single Currency), 2023; European Commission (Digital euro), 2023; Deutsche Bundesbank, 2021.
[608] cf. Jalkebro & Vlcek, 2023, pp. 113-121; Sveriges Riksbank, 2023; His Majesty's Treasury, 2019, p. 7; Ingves, 2018; Swedish Institute, 2022.
[609] cf. His Majesty's Treasury, 2019, p. 6.

exemptions for certain situations, such as clearly defined emergencies. This provision could address concerns about the potential difficulties that a cash limit might impose on the general population in urgent situations where access to cashless methods might be restricted. In this way, the potential for abuse can be minimized while ensuring that the primary objective of the legislation is not undermined.

Successful implementation will depend on comprehensive implementation, rigorous enforcement and an inclusive approach that takes into account individuals who do not have access to traditional banking services. Provisions for transactions at credit institutions and ensuring basic payment accounts for EU residents are steps in the right direction. Furthermore, an open dialogue between the government, the business sector and the public, underpinned by an emphasis on transparency and the protection of individual rights, plays a critical role in facilitating this transition.

The move to a lower cash threshold and ultimately a cashless society represents an evolution, rather than a disruption, of our financial transaction methods. If successfully implemented, it can be a sustainable, long-term measure that enhances financial transparency, efficiency and security, while protecting the rights and interests of all stakeholders. In this context, Germany could pave the way for a new standard in financial transactions and set an example for other cash-intensive societies.

Suggested methods to facilitate this transition include mandatory reporting of large cash transactions, e.g. to the FIU or tax authorities; increased monitoring of cross-border cash transactions, which will reduce cash smuggling, provided that sufficient investment is made in capacity building, tools and international cooperation; and the recording of banknote serial numbers. In addition, Germany should introduce enhanced AML and CFT obligations for high-risk dealers in high-value goods, such as art, antiques or luxury goods. These measures promise to create a robust audit trail that will make it increasingly difficult for criminals to remain anonymous and easier for authorities to identify and investigate suspicious transactions, while targeting known risk areas. Even if these regulations will inevitably create an additional layer of responsibility and effort for the parties involved, they offer solutions with high enforceability, a sustainable long-term outlook, and the potential for integration with existing systems.

At the same time, promoting the benefits of cashless transactions serves to organically reduce the volume of cash transactions over time. As seen with the younger generation and the surge in contactless payments due to the COVID-19 pandemic, there is an inherent preference for the speed, ease and security of electronic payments. Government initiatives

should encourage this trend, for example by making it a legal requirement for businesses to offer at least one digital payment option, or by providing incentives for businesses to switch to more electronic payment solutions. In addition, campaigns highlighting the positive uses of tax revenues can foster a stronger link between tax compliance, societal growth and overall economic prosperity. This can instill a sense of civic duty and pride in the population, encouraging voluntary compliance with tax laws and discouraging illicit cash transactions. Furthermore, it can enhance the public's perception of transparency and accountability in the government's use of tax revenues, further building trust in the financial system.

In addition, effective deterrence of illicit cash activities requires comprehensive training for both businesses and the public to increase understanding of the implications of ML and TF and to improve the ability to identify and report suspicious transactions. In particular, sector-specific training for businesses dealing with large cash transactions or high-value goods can strengthen their ability to identify potential illicit financing activities.

While the fight against ML and TF is a multifaceted challenge, the measures discussed are aimed at disrupting cash-based ML and TF and have a broader impact on mitigating risks in various sectors. These include the real estate and commercial sectors exposed to TBML, which would benefit from tighter cash transaction limits, improved reporting and increased scrutiny. Money or value transfer services, organized crime groups, tax evaders, and commercial fraudsters who regularly rely on cash could also face increased barriers to illicit activities. In addition, the gaming industry would experience increased security and transparency, and cross-border cash movements would be better monitored, reducing ML and TF risks associated with international interconnectedness.

Overall, a multi-pronged approach combining the proposed measures would provide a comprehensive solution to combat ML and TF. Effective implementation of these measures will require careful planning, a balanced approach between financial regulation, civil liberties and resources, logistical feasibility, and cultural acceptance of a more cashless society. The long-term success of these initiatives will depend on their ability to adapt to technological advances, societal changes, and the evolving financial crime landscape. Therefore, it is important to regularly review and update these measures to ensure their continued effectiveness against evolving threats.

5.3.4 Suspicious Activity Reporting

In order to strengthen the foundations of AML and CFT measures, the suspicious activity reporting framework should be improved. To this end, a reassessment of existing reporting

constraints, in particular those arising from legal professional privilege, is essential. Such a reassessment will determine whether these restrictions inadvertently impede the transparency and effectiveness of SARs. In this context, ensuring robust mechanisms, such as the establishment of comprehensive and clear guidelines, is essential to motivate sectors with inherently higher risks to comply with legal reporting obligations. In addition, guidance to obliged entities needs to be expanded, e.g. by strengthening Germany's commitment to collaborative initiatives, in particular with the AFCA public-private partnership.

Additionally, the increase in SARs from the banking sector warrants close scrutiny. A thorough examination of the reasons for this trend is essential to distinguish genuine concerns from possible defensive reporting practices. If patterns emerge that suggest the latter, guidance should be disseminated that clarifies the parameters that qualify transactions as suspicious. This would optimize the reporting mechanism and ensure that it serves as a tool for red-flagging concerns rather than a perfunctory exercise.[610]

Particularly in the area of TF, companies often find it difficult to identify related activities. This observation is supported by numerous discussions with private sector representatives. For example, credit institutions use red flags in their monitoring systems, such as the name of the sender or recipient, and check transactions against sanctions lists. However, transactions related to TF are often small and may be overlooked. Given these challenges, the quality of information available to obligated entities needs to be improved, for example through regular updates of TF typologies by authorities and training programs.[611] In addition, tools such as data visualization through link analysis can be used to further improve the detection of suspicious activity.[612]

Furthermore, the FIU aims to improve the quality of its analysis reports while reducing processing times. Suspicious activity reports that are not related to complex ML or TF structures will be forwarded to law enforcement authorities without delay, especially in cases such as the involvement of financial agents or fraud. In this regard, the FIU should not only conduct rigorous evaluations by regularly reviewing the quality of SAR submissions, but also foster an environment of continuous learning by providing comprehensive feedback.

[610] cf. Cotoc (Bodescu), Nițu, Șcheau & Cozma, 2021, pp. 7-8; Murr, Donovan & Yu, 2023, pp. 42-44, 55-56; Gaspareniene, Gagyte, Remeikiene & Matuliene, 2022, pp. 153, 156-157, 165; Financial Action Task Force, 2022, p. 15.
[611] cf. Murr, Donovan & Yu, 2023, pp. 42-44, 47, 52-53; Bundesministerium der Finanzen, 2019, p. 52.
[612] cf. Singh & Best, 2019.

This would inevitably improve the quality of reporting and align it with the overarching goals of AML and CFT measures.[613]

Conclusion and Further Recommendations

The fight against ML and TF in Germany requires a robust and continuously evolving suspicious activity reporting framework. Therefore, as outlined in this chapter, a re-evaluation of existing reporting restrictions is necessary in this context to ensure the transparency and effectiveness of SARs.

Moreover, there is a need for clearly defined guidelines tailored to high-risk sectors to ensure consistent legal reporting, as well as an increased commitment to cooperation, particularly with the AFCA, to improve guidance to obligated parties. The trend in SARs in the banking sector and the problems faced by companies in identifying transactions related to TF underscore the need for a nuanced understanding of how to distinguish between genuine alerts and potentially defensive reporting, and for continued refinement of typologies that should reflect the evolving global financial dynamics.

In addition, the FIU's efforts to enhance its analytical capabilities, coupled with its approach to rapid case diversion, should be accompanied by sustained self-assessment and the fostering of an environment that promotes continuous learning.

Based on these findings, investing in comprehensive training programs, particularly for companies in high-risk sectors, would not only increase their ability to detect suspicious activity, but also mitigate potential defensive reporting. These programs should emphasize real case studies and simulations to bridge the gap between theory and practice.

In addition, a systematic feedback mechanism should be established to provide companies with regular insight into the SARs they submit. This will improve the quality of subsequent reporting and create a sense of shared responsibility and cooperation between companies and regulators.

Furthermore, fostering a culture of interdisciplinary research and collaboration that brings together different relevant knowledge holders, such as financial experts, criminologists, and data scientists, provides new perspectives and innovative solutions.

At the same time, promoting public awareness of the consequences of ML and TF helps to shape a vigilant and informed society in which grassroots monitoring should act as a

[613] cf. Murr, Donovan & Yu, 2023, pp. 42-45; Financial Action Task Force, 2022, p. 15; Bundesministerium der Finanzen, 2019, pp. 40-41.

complementary detection mechanism. This can be achieved through educational initiatives, public campaigns or community engagement programs.

In conclusion, improved SARs can enhance the ability to detect ML and TF activities. As global financial dynamics change, Germany's fight against ML and TF requires agile adaptation of its suspicious activity reporting strategies, supported by collaborative and interdisciplinary efforts, robust enforcement, and innovative detection mechanisms to ensure continued effectiveness and sustainability.

5.3.5 Data Collection and Usage

A key step in improving Germany's AML and CFT framework is to enhance the country's capacity and effectiveness in data collection and its analytical use. The resilience and adaptability of an AML and CFT system is related to its ongoing ability to self-assess and evaluate its performance metrics, which would be enhanced by improved data collection and use. This is particularly important in areas as complex as ML and TF investigations and prosecutions, areas of decentralized or shared responsibilities, and harmonized international cooperation.

In the rapidly evolving financial landscape, it is important to harness the potential of sophisticated data management paradigms and integrate advanced analytics. Going beyond the mere aggregation of data and analyzing it in depth would provide a deeper understanding of underlying patterns and anomalies and could significantly improve the effectiveness of the AML and CFT infrastructure. Therefore, by integrating advanced analytics, the AML and CFT system can proactively address emerging challenges and strengthen the financial ecosystem against potential threats.[614]

A notable Franco-German initiative in this context is Gaia-X, which represents a joint effort by Europe's business, academic and political representatives to build an innovative next-generation European data infrastructure. This collaboration aims to create a federated and secure data ecosystem that promotes digital sovereignty, interoperability and open-source principles and allows data to be made available, shared and used in a secure and reliable environment. In addition, the collaboration extends to AI and a common approach to a data infrastructure to strengthen Europe's digital sovereignty.[615] In the fight against ML and TF,

[614] cf. Levi, Reuter & Halliday, 2018, pp. 310-311; Financial Action Task Force, 2022, p. 15.
[615] cf. Kraemer, Niebel & Reiberg, 2023, pp. 4-6; Rusche, 2022, pp. 8-18; Autolitano & Pawlowska, 2021, pp. 12-14; Bundesministerium für Wirtschaft und Klimaschutz, n.d.

Gaia-X could provide a valuable platform for streamlined data sharing and analysis, thereby strengthening Germany's AML and CTF efforts.

Conclusion and Further Recommendations

To advance the fight against ML and TF, it is necessary to improve the data collection framework and its analytical use. This requires a rigorous, multi-faceted exploration of statistical nuances. The use of advanced analytics can help understand previously opaque areas of ML and TF and contribute to greater transparency and security. As outlined above, the foundation of a resilient AML and CFT system also lies in its constant capacity for introspection and ongoing evaluation of its functional metrics. In this context, Gaia-X underlines the efforts of European cooperation to promote a federated, secure and interoperable data environment.

Broader European or even global cooperation can improve data sharing, analysis and ML and TF prevention strategies. As global threats can be most effectively addressed with global solutions, sharing knowledge between countries will lead to more robust defenses against ML and TF.

As new technologies, particularly from the private sector, mature and are commercialized, there remains a legislative mandate to strengthen financial institutions. The focus should be on creating agile and democratic structures that can quickly adapt to emerging needs. In addition, the goal should be to shape technological and methodological standards through broad consensus, thereby facilitating collective adoption and implementation.

In general, there appears to be a lack of consensus on the release of data, its technological format, the identification of a trusted authority, the entities at the forefront that can share lessons learned, the equitable moderation of such efforts, and the tangible benefits to participants beyond the imposition of additional tasks.

Additionally, as data collection and analysis increases, establishing ethical guidelines for the use of data, particularly in financial surveillance, is critical to building public trust and ensuring legal compliance.

In summary, the proposed data collection and use measures can improve the understanding of ML and TF risks and increase the effectiveness of mitigation efforts. With detailed evaluation of the various measures, they will be effective and sustainable in the long term.

5.4 Ensuring Sustainable Change

5.4.1 Supervision and Compliance of Financial Institutions

Improving the supervision and compliance of financial institutions is important in the fight against ML and TF.[616]

In terms of supervision, BaFin has demonstrated a strong commitment to combating ML and TF. Nevertheless, there are opportunities for improvement. In order to strengthen the integrity of the financial market, BaFin should expand its internal audit capabilities and conduct more on-site examinations, thereby addressing organizational structure deficiencies in the banking sector with respect to AML. In this context, the scope of BaFin's inspections, in particular of high-risk non-bank financial institutions, should be regularly assessed in order to ensure continuous supervision. In addition, it is suggested that BaFin's legal powers be expanded and that it be equipped with a robust unit explicitly dedicated to detecting and investigating potential threats to the markets' integrity that go beyond its preventive mandate. This includes potential manipulation and fraudulent activities. In addition, BaFin should conduct careful reviews of past customer assessments, particularly in cases where there may be a deliberate failure to comply with customer due diligence procedures or instances of compromised employees. These assessments should be correlated with specific suspicious cases to increase detection efficiency.[617]

The AML strategies are constantly refined by BaFin, taking into account the individual risks of each regulated entity across all sectors, and plans to foster a closer dialogue with them. In the insurance sector, for example, the current risk assessment system based on internal audit reports and on-site inspections requires a more systematic approach that would not only save resources but could also increase the effectiveness of supervision. At the same time, a greater focus should be placed on the risk adequacy of the oversight systems for electronic money.[618]

Furthermore, BaFin needs to adopt a more assertive strategy to exclude and identify unauthorized MVTS operators, including hawala operators. In this context, the supervisory approach must also focus on the importance and risk of each agent. Systemic deficiencies in agent networks need to be addressed by the network operators and should therefore be the

[616] cf. Murr, Donovan & Yu, 2023, pp. 45, 49-50; Yeoh, 2020, p. 128.
[617] cf. Murr, Donovan & Yu, 2023, p. 49; Transparency International Deutschland e.V., 2021, p. 23; Bundesministerium der Finanzen, 2019, p. 62; Financial Action Task Force, 2022, p. 15.
[618] cf. Bundesministerium der Finanzen, 2019, pp. 38, 86, 96; Dobler, Garrido, Grolleman, Khiaonarong & Nolte, 2021, p. 6.

subject of their attention. In addition, operators should be required to establish contact points for liaison with the supervisory authority.[619]

Another recommendation is to broaden the application of sanctions by BaFin to include methods such as business restrictions and personal liability measures, depending on their deterrent potential. Such a proactive strategy will ensure timely remediation of non-compliance and prevent recurrence.[620]

Moreover, there is considerable potential for improvement in the area of coordination with state-level stock exchange supervision as well as European cooperation. The supervisory approach of BaFin, which focuses primarily on general correspondent banking requirements, is challenged by differences in EU AML laws that require further harmonization. These differences may inadvertently encourage supervisory arbitrage in this context. Furthermore, the national jurisdiction of supervisory authorities often delays the detection and investigation of cross-border ML. It is therefore crucial that BaFin maintains and strengthens its cooperation with competent domestic law enforcement agencies, the FIU and other international supervisory authorities.[621]

In order to implement these improvements efficiently, it is crucial that BaFin is provided with adequate resources, which must be prioritized by the government.[622]

Other measures that would strengthen the ability of supervisors to effectively carry out their supervisory and enforcement functions include the implementation of more stringent checks to verify the accuracy and completeness of the data in the German bank account register, which has been successful and is expanding globally through automatic information exchange. Additionally, the data must be accessible for AML and anti-corruption purposes, not just for tax purposes. Regular analysis and checks need to be carried out to ensure the quality of data, in particular from traditional secrecy jurisdictions and high-risk financial institutions. The gradual extension of automatic information exchange to other types of assets, in particular real estate, is also recommended.[623]

[619] cf. Murr, Donovan & Yu, 2023, pp. 45-46; Financial Action Task Force, 2022, pp. 5, 15; Bundesministerium der Finanzen, 2019, pp. 92-93.
[620] cf. Murr, Donovan & Yu, 2023, p. 49; Financial Action Task Force, 2022, pp. 5, 15.
[621] cf. Transparency International Deutschland e.V., 2021, p. 23; Bundesministerium der Finanzen, 2019, p. 59; Mugarura, 2018, pp. 188, 190, 198, 200-201. Kang, 2018, pp. 698, 701-702, 708-709.
[622] cf. Bundesministerium der Finanzen, 2019, p. 38.
[623] cf. Transparency International Deutschland e.V., 2021, pp. 22-23.

Conclusion and Further Recommendations

The proposed improvements in supervision and compliance have the potential to directly mitigate ML and TF risks associated with financial institutions. However, the effectiveness of these measures should be subject to rigorous and ongoing evaluation.

While expanding BaFin's examination capabilities and conducting more on-site examinations are critical, these measures would gain further traction if coupled with the implementation of an integrated risk management framework. This, combined with a regular assessment of the scope of inspections, would allow for a more effective pooling of efforts such as internal audits, risk assessments and on-site inspections, leading to a more efficient allocation of resources. Furthermore, a more holistic, risk-based approach would provide a more nuanced understanding of where vulnerabilities exist and how to effectively address them, particularly in high-risk sectors.

In addition to expanding BaFin's legal powers and establishing more robust units to detect potential threats, a parallel focus should be placed on fostering a culture of compliance within the institutions themselves. The emphasis on detecting and investigating potential threats should be complemented by measures to encourage self-monitoring and self-reporting.

In this context, a robust and transparent reporting mechanism can also enhance the supervision and compliance of financial institutions. Regularly published reports detailing the compliance status of supervised entities can enhance transparency, promote accountability, and provide valuable insights for both the public and the supervised entities themselves.

The introduction of stricter controls on the German bank account register and the gradual extension of the automatic exchange of information to other assets, such as real estate, are targeted initiatives. This tool would provide authorities with a comprehensive and structured view of existing accounts and associated persons, facilitating the timely detection and follow-up of suspicious activity. At the same time, these measures can be further enhanced by incorporating advanced analytics and machine learning algorithms to sift through large volumes of data, thereby increasing the speed, efficiency, and accuracy of detecting anomalous patterns that may indicate ML and TF activity.

Strengthening cooperation between BaFin, domestic law enforcement, FIUs and international supervisors is critical and should be complemented by more robust cross-border data sharing and joint investigation mechanisms. Automating the exchange of information

and enabling the seamless transfer of account information between jurisdictions or institutions can enhance the oversight and compliance of financial institutions and promote compliance by financial institutions by facilitating the identification and reporting of suspicious activity.

Any effort to improve supervision and compliance must be underpinned by a robust human capital strategy. As such, a commitment to regular training and capacity building initiatives for both BaFin staff and financial institution staff is key to ensuring that all parties involved are adequately equipped with the necessary skills and knowledge to combat ML and TF.

As the landscape of financial crime evolves, so should the legal and regulatory measures to combat it. Regular reviews of the legal and regulatory framework and the adoption of internationally recognized best practices must be an integral part of the broader strategy to enhance the supervision and compliance of financial institutions.

In conclusion, the proposed measures are iterative improvements, as the fight against ML and TF requires sustained efforts, dynamic strategies that evolve in response to changing patterns of financial crime, and a commitment to enhancing the integrity of the nation's financial systems. Ultimately, a comprehensive strategy aimed at fostering a culture of accountability and proactive compliance, accompanied by punitive measures for non-compliance, will be key to reducing ML and TF risks in Germany.

5.4.2 Supervision of Designated Non-Financial Businesses and Professions

In order to target ML and TF in high-risk sectors, it is necessary to strengthen the supervision of DNFBPs, such as real estate agents, casinos, dealers in precious stones and metals, notaries, lawyers and other independent accountants and legal professionals, and trust and company service providers.[624]

The transition to a risk-based AML and CFT model for DNFBPs faces obstacles, mainly due to the coordination of a large number of supervisors, the management of large regulated sectors and resource constraints. As a strong risk orientation of obligated parties and supervisors is essential in the DNFBP sector, measures providing for a harmonized risk-based approach should be adopted. In addition, the establishment of a national oversight mechanism for the supervision of DNFBPs should be considered.[625]

[624] cf. Murr, Donovan & Yu, 2023, pp. 45-46, 49-50; Friedrich & Quick, 2019, pp. 1103, 1131; Transparency International Deutschland e.V., 2021, p. 19; Financial Action Task Force, 2022, pp. 5, 12, 14; Financial Intelligence Unit, 2023; Financial Action Task Force, 2021, p. 3.
[625] cf. Friedrich & Quick, 2019, pp. 1107, 1131; Financial Action Task Force, 2022, p. 14; Bundesministerium der Finanzen (Strategie gegen Geldwäsche und Terrorismusfinanzierung), 2020, p. 12; Bundesministerium der Finanzen, 2019, pp. 38-39.

Furthermore, a significant increase in DNFBP supervisory resources, both human and technological, is needed to effectively monitor potential cash limits and existing reporting obligations. This should include the establishment of a robust human resource framework through increased staff resources coupled with an environment that promotes improved coordination and risk-based planning. In addition to the coordinating function of the FIU, the establishment of the RÜST GW/TF and the introduction of the coordinating offices provide a platform for strategic planning and coordination of AML and CFT initiatives. Such coordination efforts should be intensified and possibly refined through structural adjustments to enhance inter-agency cooperation and communication.

Moreover, it is essential to improve the information available to DNFBP supervisors. In this context, there is a need for improved information sharing among AML supervisors, tax authorities, and police. The intelligence provided by the FIU should serve as the basis for targeted supervision, allowing for effective disruption of ML and TF activities. The focus within regulatory structures should shift from mere formal compliance with AML obligations to a more effective application of these rules, with an explicit focus on penalizing non-compliance and violations. In addition, there should be more feedback from law enforcement to supervisors and more sharing of relevant data from financial and customs authorities to non-financial supervisors. The success of ML prevention in Germany depends on cooperation between the federal and state levels, especially in the supervision of the non-financial sector, and on the early involvement of state authorities' expertise in the legislative process. Another measure could be to ensure access to international standards and analysis as they help to improve the risk-based approach of obligated entities and supervisors.[626]

In order to encourage an increase in the number and quality of SARs from DNFBPs, misunderstandings regarding the reporting threshold, lack of awareness, implementation of preventive measures and restrictions on the use of professional secrecy as a refuge for non-compliance need to be addressed. Therefore, a robust framework that identifies and penalizes non-reporting should be prioritized. At the same time, DNFBPs need adequate support to comply with their obligations, which need to be well defined, legally binding and communicated through clear, practical case examples. In this context, the GwGMeldV-Immobilien, the real estate examples in the FIU's annual report, and the AML task force within Berlin's notary supervision, which are further described in chapter *4.3.1 Real Estate*, are first step examples. Furthermore, the FIU plays a central role in streamlining AML

[626] cf. Murr, Donovan & Yu, 2023, pp. 49-50; Friedrich & Quick, 2019, pp. 1103, 1131; Financial Action Task Force, 2022, p. 14; Transparency International Deutschland e.V., 2021, p. 19; Bundesministerium der Finanzen (Strategie gegen Geldwäsche und Terrorismusfinanzierung), 2020, pp. 5-6, 12-14.

efforts among regional authorities. The FIU strengthens practices nationwide through best practice sessions and provides analysis of SARs and lessons learned from national and international collaborations to support risk-based supervision and compliance.[627]

In August 2022, the German Minister of Finance outlined a comprehensive plan to combat financial crime, especially ML and TF, and to enforce sanctions more effectively. Key measures include the creation of a new Federal Agency for Combating Financial Crime (Bundesoberbehörde zur Bekämpfung der Finanzkriminalität), which encompasses a Federal Financial Criminal Police Office (Bundesfinanzkriminalamt), the FIU, and a Central Office for ML Supervision (Zentralstelle für Geldwäscheaufsicht) to consolidate key competencies, manage complex financial crime cases, and analyze SARs. In particular, the Central Office for ML Supervision will streamline supervision of the non-financial sector in Germany, with the aim of reducing the number of supervisory authorities, developing uniform risk-based supervisory standards, and acting as a liaison with the future European Anti-Money Laundering Authority. In addition, the plan also emphasizes the need for highly trained financial investigators and increased digital connectivity of all relevant registers.[628]

Conclusion and Further Recommendations

Efforts to strengthen the supervision of DNFBPs in Germany can significantly reduce the risks associated with ML and TF in high-risk sectors, including real estate, gambling and high-value goods, as described above. The adoption of a harmonized, risk-based approach provides DNFBPs with a robust and consistent framework for identifying and mitigating financial crime risks. In addition, by establishing effective oversight mechanisms that incentivize compliance and deter non-compliance, a more resilient and compliant DNFBP sector should be cultivated, thereby strengthening Germany's overall financial integrity.

Consideration should be given to incorporating regular external audits and evaluations into AML and CFT oversight processes, as is the case for financial institutions. Regular independent reviews ensure the ongoing relevance, effectiveness and compliance of DNFBPs with evolving AML and CFT regulations and help identify areas for improvement.

In addition, it is essential to deepen the ongoing dialogue between regulators and DNFBPs. Improving consultation processes can foster a symbiotic relationship, ensuring that regulation meets the operational needs of DNFBPs while remaining consistent with the

[627] cf. Friedrich & Quick, 2019, p. 1103; Transparency International Deutschland e.V., 2021, p. 19; GwGMeldV-Immobilien, 2020; Financial Action Task Force, 2022, pp. 5, 11, 47; Financial Intelligence Unit, 2022, pp. 39-42; Bundesministerium der Finanzen (Strategie gegen Geldwäsche und Terrorismusfinanzierung), 2020, p. 12.
[628] cf. Bundesministerium der Finanzen, n.d.; Deutscher Bundestag, 2023; Friedrich & Quick, 2019, p. 1103.

broader goal of combating ML and TF. Strengthening international partnerships can also enable the sector to more effectively address emerging global trends and threats.

In this regard, regular updates of risk assessments and trends specific to DNFBPs would allow for a more targeted supervisory focus and efficient allocation of resources. Training programs for DNFBP staff should integrate these evolving trends and risks to promote an informed and proactive approach to combating ML and TF. Given the need to expand technical resources, the integration of advanced technologies such as machine learning can significantly improve risk assessment capabilities and the detection of suspicious activity.

In the long term, enhanced supervision of DNFBPs could reshape the operational and strategic framework of the sector. While harmonizing a risk-based approach to DNFBP supervision in Germany poses challenges in terms of coordination, resource allocation, and multi-stakeholder engagement, the benefits in terms of improved effectiveness, enforceability and sustainability in the fight against ML and TF are substantial. This approach can foster a culture of compliance with AML and CFT laws, leading to a more cohesive landscape where risk identification and mitigation strategies are consistent across sectors, ultimately reducing ML and TF risks in Germany.

5.4.3 Targeted Financial Sanctions System

Due to the lack of effective use of TFS, as described in chapter *4.4.4 Cooperation and Coordination Challenges*, another strategy to reduce the risk of ML and especially TF is a targeted and effectively implemented sanctions framework.[629] In this context, the use of the TFS system should be promoted in order to strengthen it. Specifically, Germany should be more proactive in nominating entities for inclusion under UN Security Council Resolution 1373 (2001)[630] designations, where appropriate, and consider establishing a separate German listing process in addition to the implementation of the EU sanctions list[631] in Germany.

Moreover, technical gaps in the system can undermine the effectiveness of sanctions, particularly when UN listings are announced on weekends or during national holidays. It is therefore critical to mitigate potential procedural gaps and overcome technical barriers to ensure immediate enforcement and reduce vulnerabilities during such periods. In this regard, technical improvements should be implemented at relevant entities, such as financial institutions, in the form of an automated electronic system that has the capacity to operate

[629] cf. Le & Doan, 2023, pp. 365-366; Purcell, Schantz & Shire, 2023, pp. 114-119; Jentleson, 2022, p. 11; Honda, 2020, pp. 18-19.
[630] Resolution 1373 (2001), 2001.
[631] European Commission (Financial Sanctions List), 2023.

without timeouts due to system or database updates. This would allow entities to be immediately updated on new sanctions published by the UN. In addition, this system must be programmed to automatically detect anomalies or suspicious activity related to sanctioned entities based on the most recent updates. Bridging the gaps associated with manual operations and reducing or eliminating delays caused by weekends or national holidays would ensure prompt implementation of UN lists, such as timely asset freezes. Regular automated re-screening of past transactions after updates could also identify past suspicious transactions of recently sanctioned entities.

Furthermore, DNFBPs should comply with TFS in a manner commensurate with the risks they pose or are exposed to. In this regard, supervisors, particularly those overseeing higher-risk sectors, should be strengthened to raise awareness of TFS mandates and be vigilant in informing entities of new listings.

Another key element is to ensure the active participation and commitment of all relevant government authorities, including the transparency register as well as legal person and arrangement registries. Their diligence in checking sanctions lists and their proactive involvement are critical to identifying and promptly freezing assets, thereby thwarting potential illicit financial activity.[632]

Conclusion and Further Recommendations

The proposed measures to strengthen the system of TFS represent an opportunity to disrupt criminal financing networks. A key recommendation is to proactively initiate designations. This can be accomplished by establishing an interagency task force that systematically identifies, evaluates, and proposes potential sanction targets using a mix of intelligence reports, law enforcement data, and open-source information. In addition, the creation of a national listing process, in addition to the existing EU and UN systems, would allow for more rapid and targeted responses to domestic threats. The design of such a process should prioritize agile and effective action and ensure that it adds value to, rather than duplicates, existing international efforts.

In addition, increased proactivity in the implementation of TFS, particularly among supervisors and government authorities, will not only expedite the implementation of sanctions, but will also promote a comprehensive understanding of the TFS landscape, thereby fostering more efficient and informed decision-making in the fight against TF.

[632] cf. Purcell, Schantz & Shire, 2023, pp. 120-126, 130-151; Financial Action Task Force, 2022, pp. 15, 103.

Finally, as with any robust system, periodic reviews and adjustments are essential to maintain its effectiveness over time. These should include assessments of the legal, operational, and technical elements of the TFS system, which would facilitate timely revisions and adjustments to evolving TF and ML challenges. In this regard, feedback sessions should be conducted with key stakeholders, including banks, non-bank financial institutions, and other affected sectors, as their experiences can provide invaluable insights and highlight challenges and opportunities for improvement. In addition, regular assessments of global best practices in TFS can be beneficial. By benchmarking against leading countries and adopting their most effective strategies, Germany would ensure that its TFS framework remains effective.

In summary, the successful implementation of these measures requires a multi-faceted approach combined with an ongoing commitment to adapt to the dynamic financial crime landscape. In this way, Germany can further strengthen its TFS system and make significant progress in its ongoing fight against ML and TF.

6 Conclusions and Outlook

In summary, the dissertation provides a comprehensive analysis of the phenomena of ML and TF, with a particular focus on Germany, and examines, specifies, and proposes improvements to the instruments used to combat them.

There are several relevant definitions of ML and TF. Of importance in this context is the comprehensive breakdown of the ML cycle, highlighting the stages of placement, layering and integration, and the stages of TF, which are the raising, storage, movement and use of funds. In addition, it is important to noted that there is an interrelationship between ML and TF, as well as differences in the origin and ultimate purpose of the funds and the timing of the illicit activity.

The instruments currently in place to combat ML and TF include international and transnational instruments, in particular those of the FATF, the UN, the Egmont Group of FIUs, the OECD, the Basel Committee on Banking Supervision, the International Monetary Fund, and the World Bank Group, as well as European and EU instruments and national instruments, such as those of the U.S. and Germany. Throughout the analysis, special emphasis is placed on the respective institutions and legal instruments.

Identifying and analyzing the most significant current threats and vulnerabilities to ML and TF in Germany is critical to improving countermeasures in the fight against financial crime. The threats and vulnerabilities relate to a variety of sectors and can be categorized according to their specific relevance to ML, TF, and those that affect both. The main risks identified in the context of ML are real estate, TBML, organized crime, serious tax crimes, the gambling sector, commercial fraud, legal arrangements and legal persons, international interconnectedness, lack of understanding of the problem and lack of investigative capacity. Dual threats and vulnerabilities to ML and TF include the use of cash, virtual assets and innovative payment methods, challenges to cooperation and coordination, and the recent COVID-19 pandemic that has reshaped economies and financial transactions. Moreover, the misuse of NGOs and NPOs and the misuse of MVTS pose TF risks. The measures already implemented to address the specific risks described are explained in the relevant subsections.

The results show a significant need for improvement at various levels. On this basis, and using the Kotter Model for effective and sustainable change, key approaches have been identified to improve the fight against ML and TF in Germany by strengthening its defenses against financial crime. They range from political prioritization, improving the detection,

investigation and prosecution of ML, improving financial intelligence, combating cash-based ML and TF, improving the supervision and compliance of financial institutions, strengthening the supervision of DNFBPs, improving suspicious activity reporting, reforming the German registration systems and legal entities, collecting and using data, and improving the effectiveness of the TFS regime.

The results of the research have far-reaching implications beyond the academic arena. Politically, they provide a basis for policymakers to revise existing AML and CFT laws and policies. In this context, improving Germany's efforts to combat ML and TF is not only a domestic imperative, but also has geopolitical implications. As a major economy in the EU, Germany's policies can influence the policy directions of neighboring countries. Furthermore, unaddressed vulnerabilities and threats in the financial system not only facilitate ML and TF, but also undermine the economic integrity of the nation, thereby threatening international financial stability. Therefore, ensuring a transparent and resilient financial infrastructure that discourages ML and TF can attract foreign investment and foster confidence among international stakeholders. At the societal level, there is a need to increase public understanding of these phenomena and to mitigate the threat of ML and TF by disrupting the flow of funds to criminal activities and terrorism. Effective countermeasures are not only the responsibility of government agencies, but also require public awareness and vigilance. It is in society's interest to deter ML and TF activities because their success often has an impact on other forms of social crime, such as drug trafficking, corruption, and even terrorism.

In the future, these recommendations can be seen as a starting point for deeper examination and reform, both at the national level and in the context of broader international efforts to combat financial crime. The fight against ML and TF is an evolving challenge that requires continued research, innovation, and cooperation among all stakeholders. Because the dissertation is based on data available at the time of the research, such as existing literature or official reports, and because ML and TF techniques are becoming more sophisticated, enabled in part by technological advances, the study of real-time issues may be limited, which is a challenge for any research in this area. Therefore, future focus could be on a real-time or longitudinal study using primary data collection to provide a more accurate picture of the current ML and TF landscape. In addition, an in-depth, sector-specific analysis would provide targeted insights into vulnerabilities and thus more actionable recommendations regarding specific micro-areas.

In conclusion, this dissertation serves both as an account of the current ML and TF landscape in Germany and as a recommended course of action for stakeholders. The increasingly complex networks that facilitate these crimes require equally complex solutions. The recommendations provided can ensure a safer, more transparent financial ecosystem. While the results and recommendations of this work are largely specific to Germany, the methods and findings can be adapted for broader, more global application.

The fight against ML and TF is not just a legal or financial challenge, but a social issue that requires collective vigilance and action across multiple sectors and levels of government. As new threats emerge and old ones evolve, the need for continued research and practical solutions becomes ever more apparent.

Bibliography

1. 18 United States Code § 1956 - Laundering of monetary instruments (18 USC § 1956). (January 2, 2001). *United States of America.* Retrieved October 24, 2023 from Office of the Law Revision Councel: https://uscode.house.gov/view.xhtml?req=granuleid:USC-2000-title18-section1956&num=0&edition=2000.
2. 18 United States Code § 1957 - Engaging in monetary transactions in property derived from specified unlawful activity (18 USC § 1957). (January 2, 2001). *United States of America.* Retrieved October 24, 2023 from Office of the Law Revision Councel: https://uscode.house.gov/view.xhtml?hl=false&edition=2000&req=granuleid%3AUSC-2000-title18-section1957&num=0&saved=%7CZ3JhbnVsZWlkOlVTQy0yMDAwLXRpdGxlMTgtc2VjdGlvbjE5NTY%3D%7C%7C%7C0%7Cfalse%7C2000.
3. Abgabenordnung (AO). (December 20, 2022). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/ao_1977/inhalts_bersicht.html.
4. Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. (July 27, 2010). *USA/EU.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22010A0727(01)&from=EN.
5. Ahrens, S. (May 10, 2023). *Anteil der Zahlungsarten am Einzelhandelsumsatz in Deutschland in den Jahren 2009 bis 2022.* Retrieved October 24, 2023 from Statista: https://de.statista.com/statistik/daten/studie/1129255/umfrage/umsatzanteil-zahlunsgarten-einzelhandel-in-deutschland/#:~:text=Während%20im%20Jahr%202009%20mit,Jahr%202022%20mit%20Kartenzahlung%20erzielt.
6. Akartuna, E. A., Johnson, S. D. & Thornton, A. E. (September 19, 2022). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal, 35*(3). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1057/s41284-022-00356-z.
7. Albers, M. & Groth, L. (2015). Globales Recht und Terrorismusfinanzierungsbekämpfung. In M. Albers & L. Groth, *Globales Recht und Terrorismusfinanzierungsbekämpfung: Zur Einführung* (pp. 9-35). Baden-Baden: Nomos Verlagsgesellschaft.
8. Albrecht, C., Duffin, K. M., Hawkins, S. & Morales Rocha, V. M. (September 30, 2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control, 22*(2), pp. 210-216. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-12-2017-0074.
9. Alshantti, A. & Rasheed, A. (December 14, 2021). Self-Organising Map Based Framework for Investigating Accounts Suspected of Money Laundering. *Frontiers in Artificial Intelligence, 4*, pp. 68-73. Retrieved October 24, 2023 from Frontiers: https://doi.org/10.3389/frai.2021.761925.
10. Amonovna, S. G. & Feruzbek, A. (February 2023). International Principles of Corporate Governance. *International Scientific Research Journal, 4*(2), pp. 539-543. Retrieved October 24, 2023 fromWeb of Scientist: https://doi.org/10.17605/OSF.IO/9SVB6.
11. Anti-Money Laundering Act (Geldwäschegesetz - GwG). (September 29, 2020). *Federal Financial Supervisory Authority.* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_gwg_en.html.
12. Außenwirtschaftsgesetz (AWG). (December 20, 2022). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/awg_2013/BJNR148210013.html.

13. Autolitano, S. & Pawlowska, A. (April 1, 2021). *Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study*. Retrieved October 24, 2023 from Istituto Affari Internazionali (IAI): https://www.iai.it/sites/default/files/iaip2114.pdf.
14. Aydan, S., Bayin Donar, G. & Arikan, C. (July 4, 2022). Impacts of Economic Freedom, Health, and Social Expenditures on Well-Being Measured by the Better Life Index in OECD Countries. *Social Work in Public Health, 37*(5), pp. 435-447. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/19371918.2021.2018083.
15. Bürgerliches Gesetzbuch (BGB). (October 16, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/bgb/BJNR001950896.html.
16. Bank for International Settlements. (December 12, 1988). *Prevention of criminal use of the banking system for the purpose of money-laundering.* Retrieved October 24, 2023 from BIS: https://www.bis.org/publ/bcbsc137.pdf.
17. Bank for International Settlements. (n.d.). *History of the Basel Committee.* Retrieved October 24, 2023 from BIS: https://www.bis.org/bcbs/history.htm.
18. Bannenberg, B. (2022). Clankriminalität – Clanstrukture. In F.-A. Richter, *Phänomen Clankriminalität: Grundlagen - Bekämpfungsstrategien - Perspektiven* (pp. 69-83). Stuttgart: Richard Boorberg Verlag.
19. Bayerisches Staatsministerium der Finanzen und für Heimat. (April 13, 2023). *Pressemitteilung Nr. 106 - Füracker und Huml: Bargeld-Obergrenze ist direkter Eingriff in Freiheitsrechte.* Retrieved October 24, 2023 from Bayerisches Staatsministerium der Finanzen und für Heimat: https://www.stmfh.bayern.de/internet/stmf/aktuelles/pressemitteilungen/25127/.
20. Bayerisches Staatsministerium der Justiz. (February 7, 2023). *Entwicklung eines bundeseinheitlichen Datenbankgrundbuchs - Projekt "dabag".* Retrieved October 24, 2023 from Grundbuch: https://www.grundbuch.eu/beschreibung/.
21. Bayerisches Staatsministerium des Innern, für Sport und Integration. (May 10, 2023). *Glücksspiel; Durchführung der Geldwäscheaufsicht.* Retrieved October 24, 2023 from Dienstleistungsportal Bayern: https://www.eap.bayern.de/informationen/leistungsbeschreibung/5392714945135.
22. Beck-aktuell. (March 5, 2021). *Strafrechtliche Vermögensabschöpfung trotz Verfolgungsverjährung zulässig.* Retrieved October 24, 2023 from beck-aktuell: https://rsw.beck.de/aktuell/daily/meldung/detail/bverfg-strafrechtliche-vermoegensabschoepfung-auch-bei-verfolgungsverjaehrung-zulaessig.
23. Beka, A. (2019). Money Laundering. *Acta Universitatis Danubius. Juridica, 15*(1), pp. 229-239. Retrieved October 24, 2023 from Danubius University: https://journals.univ-danubius.ro/index.php/juridica/article/view/5274/4916.
24. Berentsen, A. (December 2020). *Plädoyer für den E-Euro - Implikationen für die Gesellschaft, WWZ Working Paper, No. 2020/17.* Retrieved October 24, 2023 from Econstor: https://www.econstor.eu/bitstream/10419/240426/1/2020-17.pdf.
25. Bilińska-Reformat, K. & Kieżel, M. (January 2016). Retail Banks and Retail Chains Cooperation for the Promotion of the Cashless Payments in Poland. *Proceedings of the International Marketing Trends Conference.* Retrieved October 24, 2023 from ResearchGate: https://www.researchgate.net/publication/299533628_Retail_Banks_and_Retail_Chains_Cooperation_for_the_Promotion_of_the_Cashless_Payments_in_Poland.
26. Bin Sulaiman, R., Schetinin, V. & Sant, P. (May 5, 2022). Review of Machine Learning Approach on Credit Card Fraud Detection. *Human-Centric Intelligent Systems, 2*(1-2), pp. 55–68. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s44230-022-00004-0.
27. Bloomberg Finance L.P. (March 30, 2023). *Introducing BloombergGPT, Bloomberg's 50-billion parameter large language model, purpose-built from scratch for finance.* Retrieved October 24, 2023 from Bloomberg: https://www.bloomberg.com/company/press/bloomberggpt-50-billion-parameter-llm-tuned-finance/.

28. Bock, C. (January 15, 2020). „Know your customer“ – Betrugsprävention im E-Commerce. *Wirtschaftsinformatik & Management, 12*(1), pp. 43-46. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1365/s35764-019-00229-y.
29. Buckley, P., Pietropaoli, L., Rosada, A., Harguth, B. & Broom, J. (June 25, 2022). How has COVID-19 affected migrant workers vulnerability to human trafficking for forced labour in Southeast Asia?—a narrative review. *Journal of Public Health and Emergency, 6*(19). Retrieved October 24, 2023 from JPHE: https://doi.org/10.21037/jphe-21-108.
30. Bundesanstalt für Finanzaufsicht (About). (n.d.). *About BaFin.* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/EN/DieBaFin/diebafin_node_en.html.
31. Bundesanstalt für Finanzaufsicht (Europäischer Pass). (April 8, 2022). *Europäischer Pass für Kreditinstitute.* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/DE/Aufsicht/BankenFinanzdienstleister/Passporting/Kreditinstitute/kreditinstitute_node.html.
32. Bundesanstalt für Finanzaufsicht (Guidance). (January 5, 2022). *Interpretation and Application Guidance on the German Money Laundering Act (October 2021).* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/SharedDocs/Downloads/EN/Auslegungsentscheidung/dl_ae_auas_gw2021_en.html.
33. Bundesanstalt für Finanzaufsicht (Meldung). (November 10, 2022). *Meldung von Betrugsdaten.* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/DE/Aufsicht/ZahlungsdienstePSD2/MeldungBetrugsdaten/MeldungBetrugsdaten_node.html.
34. Bundesanstalt für Finanzaufsicht (Prevention). (n.d.). *Prevention of money laundering and terrorist financing.* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/EN/Aufsicht/Geldwaeschepraevention/geldwaeschepraevention_node_en.html.
35. Bundesanstalt für Finanzaufsicht. (September 8, 2021). *Subnationale Risikoanalyse 2021/2022 (SRA 3.0).* Retrieved October 24, 2023 from BaFin: https://www.bafin.de/SharedDocs/Downloads/DE/Bericht/dl_sra_21_gw.html.
36. Bundeskriminalamt (Richtiges Verhalten). (n.d.). *Richtiges Verhalten bei….* Retrieved October 24, 2023 from BKA: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/richtigesverhalten_node.html.
37. Bundeskriminalamt (BKA). (n.d.). *The BKA.* Retrieved October 24, 2023 from BKA: https://www.bka.de/EN/Home/home_node.html.
38. Bundeskriminalamt (Warnhinweise). (n.d.). *Warnhinweise.* Retrieved October 24, 2023 from BKA: https://www.bka.de/DE/IhreSicherheit/Warnhinweise/warnhinweise_node.html.
39. Bundeskriminalamt. (December 4, 2018). *BaFin und BKA warnen vor Abzocke bei Geldanlagen im Internet.* Retrieved October 24, 2023 from BKA: https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Warnhinweise/181204_OnlineGeldanalage.html.
40. Bundeskriminalamt. (September 21, 2022). *Organisierte Kriminalität: Bundeslagebild 2021.* Retrieved October 24, 2023 from BKA: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/OrganisierteKriminalitaet/organisiertekriminalitaet_node.html.
41. Bundesministerium der Finanzen. (October 19, 2019). *Erste Nationale Risikoanalyse 2018/2019.* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.pdf?__blob=publicationFile&v=18.
42. Bundesministerium der Finanzen. (n.d.). *Voller Einsatz gegen Finanzkriminalität.* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Geldwaesche-bekaempfen/voller-einsatz-gegen-finanzkriminalitaet.html.
43. Bundesministerium der Finanzen (Sanktionsdurchsetzungsgesetz II). (December 16, 2022). *Sanktionsdurchsetzungsgesetz II: Sanktionen konsequent umsetzen.* Retrieved October 24, 2023 from Bundesfinanzministerium:

https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Geldwaesche-bekaempfen/sanktionsdurchsetzungsgesetz-II.html.

44. Bundesministerium der Finanzen (Sektorspezifische Risikoanalyse). (December 31, 2020). *Sektorspezifische Risikoanalyse 2020.* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/sektorspezifische-risikoanalyse-2020.pdf?__blob=publicationFile&v=9.
45. Bundesministerium der Finanzen (Strategie gegen Geldwäsche und Terrorismusfinanzierung). (January 17, 2020). *Strategie gegen Geldwäsche und Terrorismusfinanzierung.* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2020-01-17-strategie-geldwaesche-terrorismusfinanzierung.pdf?__blob=publicationFile&v=9.
46. Bundesministerium der Finanzen (Zweites Gesetz zur effektiveren Durchsetzung von Sanktionen). (December 27, 2022). *Zweites Gesetz zur effektiveren Durchsetzung von Sanktionen (Sanktionsdurchsetzungsgesetz II).* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_IV/20_Legislaturperiode/2022-12-27-SanktionsdurchsetzungsG-II/0-Gesetz.html.
47. Bundesministerium der Finanzen. (June 30, 2021). *Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenzregister- und Finanzinformationsgesetz).* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-06-30-TraFinG/0-Gesetz.html.
48. Bundesministerium der Justiz und für Verbraucherschutz. (December 4, 2015). *Vermögensabschöpfung im deutschen Recht.* Retrieved October 24, 2023 from Bundesministerium der Justiz und für Verbraucherschutz: https://www.bmj.de/SharedDocs/Publikationen/DE/Vermoegensabschoepfung_im_deutschen_Recht.pdf?__blob=publicationFile&v=17.
49. Bundesministerium des Innern, für Bau und Heimat. (December 28, 2020). *Sektorale Risikoanalyse - Terrorismusfinanzierung durch (den Missbrauch von) Non-Profit-Organisationen in Deutschland.* Retrieved October 24, 2023 from BMI: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/sektorale-risikoanalyse.pdf?__blob=publicationFile&v=12.
50. Bundesministerium für Wirtschaft und Klimaschutz. (n.d.). *Das Gaia-X Ökosystem - Souveräne Dateninfrastruktur für Europa.* Retrieved October 24, 2023 from BMWK: https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html.
51. Bundesrat (Empfehlungen). (December 5, 2022). *Drucksache 560/1/22: Empfehlungen der Ausschüsse - Verordnung über die Einrichtung und Führung des Gesellschaftsregisters und zur Änderung der Handelsregisterverordnung.* Retrieved October 24, 2023 from Bundesrat: https://www.bundesrat.de/SharedDocs/drucksachen/2022/0501-0600/560-1-22.pdf?__blob=publicationFile&v=1.
52. Bundesrat (Verordnung). (November 2, 2022). *Drucksache 560/22: Verordnung des Bundesministeriums der Justiz - Verordnung über die Einrichtung und Führung des Gesellschaftsregisters und zur Änderung der Handelsregisterverordnung.* Retrieved October 24, 2023 from Bundestag: https://dserver.bundestag.de/brd/2022/0560-22.pdf.
53. Bundesrechnungshof. (October 12, 2020). *Bericht an den Haushaltsausschuss des Deutschen Bundestages nach § 88 Abs. 2 BHO - Information über die Entwicklung des Einzelplans 08 (Bundesministerium der Finanzen) für die Beratungen zum Bundeshaushalt 2021.* Retrieved October 24, 2023 from Bundesrechnungshof: https://www.bundesrechnungshof.de/SharedDocs/Downloads/DE/Berichte/2020/entwicklung-einzelplan-08-bundeshaushalt-2021-volltext.pdf?__blob=publicationFile&v=1.

54. Bundesregierung. (December 16, 2022). *Sanktionsdurchsetzungsgesetz II - Effektive Durchsetzung von Sanktionen.* Retrieved October 24, 2023 from Bundesregierung: https://www.bundesregierung.de/breg-de/suche/sanktionsdurchsetzungsgesetz-2-2133904.
55. Bundesverband deutscher Banken. (April 27, 2020). *Die Corona-Krise als Katalysator: Kontaktloses Bezahlen auf dem Vormarsch.* Retrieved October 24, 2023 from Bankenverband: https://cms.bankenverband.de/sites/default/files/2022-08/migration/files/2020_04_27_Charts_U-Kontaktlos_vs_Barzahlen.pdf.
56. Bundesverfassungsgericht. (February 10, 2021). *Beschluss vom 10. Februar 2021 - 2 BvL 8/19.* Retrieved October 24, 2023 from Bundesverfassungsgericht: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2021/02/ls20210210_2bvl000819.html.
57. Bussmann, K.-D. (April 18, 2018). *Geldwäscheprävention im Markt - Funktionen, Chancen und Defizite.* Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/978-3-662-56185-0.
58. Buyse, J. (March 22, 2023). *Cash Payment Limits disempower citizens.* Retrieved October 24, 2023 from International Currency Association: https://currencyassociation.org/article/cash-payment-limits-disempower-citizens/.
59. Cabinakova, J., Knümann, F. & Horst, F. (March 28, 2019). *Kosten der Bargeldzahlung im Einzelhandel - Studie zur Ermittlung und Bewertung der Kosten, die durch die Bargeldzahlung im Einzelhandel verursacht werden.* Retrieved October 24, 2023 from Bundesbank: https://www.bundesbank.de/resource/blob/776464/d0ff995f570846f130e425a4bf003bd9/mL/kosten-der-bargeldzahlung-im-einzelhandel-data.pdf.
60. Carvalho, V. M., Garcia, J. R., Hansen, S., Ortiz, Á., Rodrigo, T., Rodríguez Mora, J. V. & Ruiz, P. (August 11, 2021). *Tracking the COVID-19 crisis with high-resolution transaction data.* Retrieved October 24, 2023 from The Royal Society Publishing: https://royalsocietypublishing.org/doi/full/10.1098/rsos.210218.
61. Cassella, S. D. (October 1, 2018). Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete? *Journal of Money Laundering Control, 21*(4), pp. 494-497. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-09-2017-0045.
62. Castellano, R., De Bernardo, G. & Punzo, G. (February 7, 2023). Well-being in OECD countries: an assessment of technical and social efficiency using data envelopment analysis. *International Review of Economics, 70*(2), pp. 141–176. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s12232-023-00413-y.
63. Charity Commission. (November 9, 2022). *Compliance toolkit chapter 1: Charities and Terrorism.* Retrieved October 24, 2023 from Government UK: https://www.gov.uk/government/publications/charities-and-terrorism/compliance-toolkit-chapter-1-charities-and-terrorism#how-might-a-charity-be-abused-for-terrorist-purposes.
64. Chaudhuri, R., Gathinji, C., Tayar, G. & Williams, E. (October 13, 2022). *Sustaining digital payments growth: Winning models in emerging markets.* Retrieved October 24, 2023 from McKinsey & Company: https://www.mckinsey.com/industries/financial-services/our-insights/sustaining-digital-payments-growth-winning-models-in-emerging-markets.
65. Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis. (August 1, 2006). *The Commission of the European Communities.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:214:0029:0034:EN:PDF.
66. Common Register Portal of the German Federal States. (n.d.). *Ministerium der Justiz Nordrhein-Westfalen.* Retrieved October 24, 2023 from Handelsregister: https://www.handelsregister.de/rp_web/welcome.xhtml.
67. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Strasbourg Convention). (November 8, 1990). *The Council of Europe.* Retrieved October 24, 2023 from Council of Europe: https://rm.coe.int/168007bd23.

68. Cotoc (Bodescu), C.-N., Nițu, M., Șcheau, M. C. & Cozma, A.-C. (June 17, 2021). Efficiency of Money Laundering Countermeasures: Case Studies from European Union Member States. *Risks, 9*(6), pp. 1-19. Retrieved October 24, 2023 from MDPI: https://doi.org/10.3390/risks9060120.
69. Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences. (September 29, 2005). *The Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32005D0671.
70. Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the member states in respect of exchanging information (2000/642/JHA). (October 17, 2000). *The Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000D0642.
71. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (Document 31991L0308). (June 10, 1991). *The Council of the European Communities.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31991L0308&from=EN.
72. Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA) (Document 32002F0475). (June 13, 2002). *The Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0475&from=EN.
73. Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (2001/500/JHA) (Document 32001F0500). (June 26, 2001). *The Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001F0500.
74. Council of Europe (Economic Crime and Cooperation Division). (n.d.). *Economic Crime and Cooperation Division.* Retrieved October 24, 2023 from Council of Europe Portal: https://www.coe.int/en/web/corruption/approach.
75. Council of Europe (MONEYVAL). (n.d.). *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.* Retrieved October 24, 2023 from Council of Europe Portal: https://www.coe.int/en/web/moneyval.
76. Council of Europe. (November 8, 1990). *Explanatory Report to the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.* Retrieved October 24, 2023 from Council of Europe: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cb5de.
77. Council of Europe. (May 16, 2005). *Explanatory Report to the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.* Retrieved October 24, 2023 from Council of Europe: https://rm.coe.int/16800d3813.
78. Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention). (May 16, 2005). *The Council of Europe.* Retrieved October 24, 2023 from Council of Europe: https://rm.coe.int/168008371f.
79. Council of the European Union. (December 7, 2022). *Anti-money laundering: Council agrees its position on a strengthened rulebook.* Retrieved October 24, 2023 from Consilium Europa: https://www.consilium.europa.eu/en/press/press-releases/2022/12/07/anti-money-laundering-council-agrees-its-position-on-a-strengthened-rulebook/.
80. Criminal Intelligence Service Canada. (October 28, 2022). *2022 Report: Organized crime in Canada.* Retrieved October 24, 2023 from CISC: https://cisc-scrc.gc.ca/media/2022/2022-10-28-eng.htm.
81. Currency and Foreign Transactions Reporting Act (Bank Secrecy Act). (October 26, 1970). *United States of America.* Retrieved October 24, 2023 from U.S. Government Information:

https://www.govinfo.gov/content/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf#page=15.

82. Dühnfort, A. M., Zitzmann, M., Hundebeck, M., Hlavica, C. & Kühne, D. (2017). Tax Fraud. In C. Hlavica, F. M. Hülsberg & U. Klapproth, *Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität* (Second Edition, pp. 77-158). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/978-3-658-07840-9.
83. Deutsche Bank. (May 15, 2023). *General Statement on Observance of Anti-Money Laundering Requirements.* Retrieved October 24, 2023 from Deutsche Bank: https://www.db.com/files/documents/General-Statement-on-Observance-of-Anti-Money-Laundering-Requirements.pdf?language_id=1.
84. Deutsche Bundesbank (Payment institutions). (n.d.). *Payment institutions and e-money institutions.* Retrieved October 24, 2023 from Bundesbank: https://www.bundesbank.de/en/tasks/banking-supervision/individual-aspects/payment-institutions/payment-institutions-and-e-money-institutions-622962.
85. Deutsche Bundesbank (Payments statistics). (n.d.). *Payments statistics.* Retrieved October 24, 2023 from Bundesbank: https://www.bundesbank.de/en/service/reporting-systems/banking-statistics/payments-statistics-620072.
86. Deutsche Bundesbank (PSD2). (n.d.). *PSD2.* Retrieved October 24, 2023 from Bundesbank: https://www.bundesbank.de/en/tasks/payment-systems/psd2/psd2-775954.
87. Deutsche Bundesbank. (October 26, 2021). *Diskussion um digitalen Euro kommt bei Verbraucherinnen und Verbrauchern nur langsam an.* Retrieved October 24, 2023 from Bundesbank: https://www.bundesbank.de/de/aufgaben/themen/diskussion-um-digitalen-euro-kommt-bei-verbraucherinnen-und-verbrauchern-nur-langsam-an-878916#:~:text=Demnach%20hatten%2077%20Prozent%20der,den%20Befragten%20schon%20deutlich%20höher.
88. Deutscher Bundestag (Antrag). (April 27, 2022). *Drucksache 20/1513: Antrag - Zentrales Immobilienregister sofort einführen.* Retrieved October 24, 2023 from Bundestag: https://dserver.bundestag.de/btd/20/015/2001513.pdf.
89. Deutscher Bundestag (Lesung). (April 29, 2022). *Linke fordert ein zentrales Immobilienregister.* Retrieved October 24, 2023 from Bundestag: https://www.bundestag.de/dokumente/textarchiv/2022/kw17-de-immobilienregister-889586.
90. Deutscher Bundestag. (June 12, 2002). *Drucksache 14/9200: Schlussbericht der Enquete-Kommission: Globalisierung der Weltwirtschaft - Herausforderungen und Antworten.* Retrieved October 24, 2023 from Bundestag: https://dserver.bundestag.de/btd/14/092/1409200.pdf.
91. Deutscher Bundestag. (May 7, 2018). *Drucksache 19/2000: Entwurf eines Gesetzes zur fortlaufenden Untersuchung der Kriminalitätslage und ergänzenden Auswertung der polizeilichen Kriminalitätsstatistik (Kriminalitätsstatistikgesetz – KStatG).* Retrieved October 24, 2023 from Bundestag: https://dserver.bundestag.de/btd/19/020/1902000.pdf.
92. Deutscher Bundestag. (December 9, 2020). *Gespaltene Meinung zum Regierungsentwurf zur Geldwäschebekämpfung.* Retrieved October 24, 2023 from Bundestag: https://www.bundestag.de/dokumente/textarchiv/2020/kw50-pa-recht-geldwaesche-808834.
93. Deutscher Bundestag. (January 25, 2023). *Lindner stellt Vorhaben für 2023 vor.* Retrieved October 24, 2023 from Bundestag: https://www.bundestag.de/presse/hib/kurzmeldungen-931158.
94. Dienstbühl, D. (2022). Kriminelle Subkulturen als Risiko für die deutsche Wirtschaft – Auswirkungen von Clankriminalität auf KMU. In C. Vogt, P. Hennies, C. Endreß & P. Peters, *Wirtschaftsschutz in der Praxis: Herausforderungen an die Sicherheit im Zeitalter von Digitalisierung und Krise* (pp. 3-20). Retrieved October 24, 2023 from Springer Nature: https://doi-1org-15ww5t0ts0ab2.erf.sbb.spk-berlin.de/10.1007/978-3-658-35123-6.
95. Dinh, V. D. (May 1, 2004). USA Patriot Act. *German Law Journal, 5*(5), pp. 461-467. Retrieved October 24, 2023 from Cambridge University Press: https://doi.org/10.1017/S2071832200012633.
96. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

(Document 32015L2366). (December 23, 2015). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

97. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Document 32015L0849). (May 20, 2015). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849.
98. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (Document 32017L0541). (March 31, 2017). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541.
99. Directive (EU) 2018/1673 of the European Parliament and of the council of 23 October 2018 on combating money laundering by criminal law (Document 32018L1673). (October 23, 2018). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=DE.
100. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Document 32018L0843). (June 19, 2018). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.
101. Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (Document 32019L1153). (July 11, 2019). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L1153.
102. Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering (Document 32001L0097). (December 4, 2001). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0097.
103. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Document 32005L0060). (October 26, 2005). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0060&from=DE.
104. Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features. (July 23, 2014). *The European Parliament and the Council.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32014L0092.
105. Dobler, M., Garrido, J., Grolleman, D. J., Khiaonarong, T. & Nolte, J. (December 14, 2021). *E-Money: Prudential Supervision, Oversight, and User Protection.* Retrieved October 24, 2023 from International Monetary Fund: https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2021/12/13/E-Money-Prudential-Supervision-Oversight-and-User-Protection-464868.
106. Duncan Jr., R. M. (April 2004). Surreptitious Search Warrants and the USA Patriot Act: "Thinking Outside the Box and Within the Consitution", or a Violation of Fourth Amendment

Protections? *City University of New York Law Review, 7*(1), pp. 1-38. Retrieved October 24, 2023 from CUNY Law Review: https://doi.org/10.31641/clr070101.

107. Economie. (June 28, 2023). *Obligation to offer an electronic means of payment.* Retrieved October 24, 2023 from Economie: https://economie.fgov.be/en/themes/sales/payments/obligation-offer-electronic.
108. Ecorys. (April 18, 2019). *European Commission publishes Ecorys study on an EU initiative for a restriction on payments in cash.* Retrieved October 24, 2023 from Ecorys: https://www.ecorys.com/global/latest-news/european-commission-publishes-ecorys-study-eu-initiative-restriction-payments.
109. Egmont Group of Financial Intelligence Units (FAQs). (n.d.). *FAQs.* Retrieved October 24, 2023 from Egmont Group: https://egmontgroup.org/faqs/.
110. Egmont Group of Financial Intelligence Units (FIUs). (n.d.). *Financial Intelligence Units.* Retrieved October 24, 2023 from Egmont Group: https://egmontgroup.org/about/financial-intelligence-units/.
111. Egmont Group/World Customs Organization. (2020). *Customs - FIU Cooperation Handbook.* Retrieved October 24, 2023 from Egmont Group: https://egmontgroup.org/wp-content/uploads/2021/09/2020_CUSTOMS_-_FIU_Cooperation_Handbook.pdf.
112. European Banking Authority. (n.d.). *Anti-Money Laundering and Countering the Financing of Terrorism.* Retrieved October 24, 2023 from EBA: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism.
113. European Banking Federation (Structure of the Banking Sector). (n.d.). *Structure of the Banking Sector.* Retrieved October 24, 2023 from EBF: https://www.ebf.eu/facts-and-figures/structure-of-the-banking-sector/#:~:text=Germany%20is%20the%20country%20with,present%20in%20Italy%20and%20France.
114. European Banking Federation (Tackling Financial Crime). (n.d.). *Tackling Financial Crime.* Retrieved October 24, 2023 from EBF: https://www.ebf.eu/priorities/ebfactions/anti-money-laundering-and-counter-financing-terrorism/.
115. European Central Bank. (December 2020). *Study on the payment attitudes of consumers in the euro area (SPACE).* Retrieved October 24, 2023 from ECB: https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf.
116. European Commission. (n.d.). *EU context of anti-money laundering and countering the financing of terrorism.* Retrieved October 24, 2023 from European Commission: https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en.
117. European Commission (Action plan). (May 7, 2020). *Action plan for a comprehensive Union policy on preventing money laundering and terrorism financing.* Retrieved October 24, 2023 from European Commission: https://finance.ec.europa.eu/publications/action-plan-comprehensive-union-policy-preventing-money-laundering-and-terrorism-financing_en.
118. European Commission (Communication from the Commission). (May 13, 2020). *Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing (2020/C 164/06).* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0513(03)&from=EN.
119. European Commission (Digital euro). (June 28, 2023). *Digital euro package.* Retrieved October 24, 2023 from European Commission: https://finance.ec.europa.eu/publications/digital-euro-package_en.
120. European Commission (Financial Sanctions List). (October 27 2023). *European Union Consolidated Financial Sanctions List.* Retrieved October 27, 2023 from Data Europa: https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en.
121. European Commission (Single Currency). (June 28, 2023). *Single Currency Package: new proposals to support the use of cash and to propose a framework for a digital euro.* Retrieved October 24, 2023 from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3501.

122. European Commission. (June 26, 2017). *Commission Staff Working Document on improving cooperation between EU Financial Intelligence units (SWD(2017) 275 final).* Retrieved October 24, 2023 from European Commission: https://ec.europa.eu/newsroom/document.cfm?doc_id=45319.
123. European Commission. (July 20, 2021). *Anti-money laundering and countering the financing of terrorism legislative package.* Retrieved October 24, 2023 from European Commission: https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.
124. European Commission. (October 27, 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 cross-border activities* . Retrieved October 24, 2023 from Eur-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554.
125. European Consumer Centre France. (September 29, 2022). *Cash payment limitations.* Retrieved October 24, 2023 from ECC: https://www.europe-consommateurs.eu/en/shopping-internet/cash-payment-limitations.html.
126. European Council (Timeline). (May 16, 2023). *Timeline: EU action against money laundering and terrorist financing.* Retrieved October 24, 2023 from Consilium Europa: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/timeline/.
127. European Council. (June 20, 2019). *A new strategic agenda 2019-2024.* Retrieved October 24, 2023 from Consilium Europa: https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/.
128. European Council (Fight against ML and TF). (June 6, 2023). *Fight against money laundering and terrorist financing.* Retrieved October 24, 2023 from Consilium Europa: https://www.consilium.europa.eu/en/policies/fight-against-terrorism/fight-against-terrorist-financing/.
129. European Council. (n.d.). *European Council.* Retrieved October 24, 2023 from European Union: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/european-council_en.
130. European Parliament (Money laundering through real estate). (February 2019). *Understanding money laundering through real estate transactions.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/cmsdata/161094/7%20-%2001%20EPRS_Understanding%20money%20laundering%20through%20real%20estate%20transactions.pdf.
131. European Parliament (New EU measures). (March 28, 2023). *New EU measures against money laundering and terrorist financing.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/news/en/press-room/20230327IPR78511/new-eu-measures-against-money-laundering-and-terrorist-financing.
132. European Parliament (Parliamentary question). (March 28, 2023). *Parliamentary question - E-001048/2023: Cash payment limit.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/doceo/document/E-9-2023-001048_EN.html.
133. European Parliament (Tax fraud). (June 28, 2019). *The fight against tax fraud.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/633153/EPRS_BRI(2019)633153_EN.pdf.
134. European Parliament. (July 10, 2020). *2020/2686(RSP) Resolution on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments.* Retrieved October 24, 2023 from European Parliament: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2686(RSP).
135. European Parliament. (December 8, 2021). *Cooperation in the fight against organised crime in the Western Balkans.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698838/EPRS_ATA(2021)698838_EN.pdf.

136. European Parliament. (November 23, 2022). *European Parliament declares Russia to be a state sponsor of terrorism.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/news/en/press-room/20221118IPR55707/european-parliament-declares-russia-to-be-a-state-sponsor-of-terrorism.
137. European Union (Council). (n.d.). *Council of the European Union.* Retrieved October 24, 2023 from European Union: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/council-european-union_en.
138. European Union (Parliament). (n.d.). *European Parliament.* Retrieved October 24, 2023 from European Union: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/european-parliament_en.
139. European Union Agency for Law Enforcement Cooperation (Centres). (n.d.). *Centres.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu.
140. European Union Agency for Law Enforcement Cooperation (ECTC). (January 11, 2023). *European Counter Terrorism Centre - ECTC.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc.
141. European Union Agency for Law Enforcement Cooperation (EFECC). (May 2, 2023). *European Financial and Economic Crime Centre - EFECC.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/about-europol/european-financial-and-economic-crime-centre-efecc.
142. European Union Agency for Law Enforcement Cooperation (Exploiting Isolation). (June 19, 2020). *Exploiting Isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/cms/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf.
143. European Union Agency for Law Enforcement Cooperation (How criminals profit). (March 27, 2020). *How criminals profit form the COVID-19 pandemic.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/media-press/newsroom/news/how-criminals-profit-covid-19-pandemic.
144. European Union Agency for Law Enforcement Cooperation (Money Laundering). (n.d.). *Money Laundering.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/money-laundering.
145. European Union Agency for Law Enforcement Cooperation. (June 27, 2019). *European Union - Terrorism Situation and Trend Report 2019.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2019_final.pdf.
146. European Union Agency for Law Enforcement Cooperation. (December 7, 2021). *COVID-19: Fraud.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/covid-19/covid-19-fraud.
147. European Union Agency for Law Enforcement Cooperation. (January 20, 2022). *EU Policy Cycle - EMPACT.* Retrieved October 24, 2023 from Europol: https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact.
148. European Union AML/CFT Global Facility. (n.d.). *Launch of the EU Global Facility on AML/CFT.* Retrieved October 24, 2023 from EU AML/CFT Global Facility: https://www.global-amlcft.eu/how-we-work/.
149. Euskirchen, J. (April 18, 2017). *Geldwäscheprävention und Compliance Management Systeme - Praxisleitfaden für Unternehmen.* Hamburg: Igel Verlag.
150. Fülbier, A., Aepfelbach, R. & Langweg, P. (2006). *GwG: Kommentar zum Geldwäschegesetz.* (Fifth Edition). Köln: RWS Verlag Kommunikationsforum.
151. Federal Bureau of Investigation. (January 28, 2020). *Oregon FBI Tech Tuesday: Building a Digital Defense Against Synthetic ID Theft.* Retrieved October 24, 2023 from FBI: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-synthetic-id-theft.

152. Federal Bureau of Investigation. (n.d.). *Romance Scams*. Retrieved October 24, 2023 from FBI: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/romance-scams.
153. Federal Office for Information Security (Home). (n.d.). *Home*. Retrieved October 24, 2023 from BSI: https://www.bsi.bund.de/EN/Home/home_node.html.
154. Federal Office for Information Security (Mandate). (n.d.). *The BSI's Mandate*. Retrieved October 24, 2023 from BSI: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/auftrag_node.html.
155. Federal Reserve. (n.d.). *Synthetic Identity Fraud Defined.* Retrieved October 24, 2023 from FedPayments Improvement: https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/synthetic-identity-fraud-defined/.
156. Fiedler, I., Krumma, I., Zanconato, U. A., McCarthy, K. J. & Reh, E. (2017). Theorie: Glücksspiele und Geldwäsche. In *Das Geldwäscherisiko verschiedener Glücksspielarten* (pp. 149-164). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/978-3-658-16625-0_8.
157. Financial Action Task Force. (1990). *The Forty Recommendations of the Financial Action Task Force on Money Laundering.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf.
158. Financial Action Task Force (40 Recommendations). (February 2023). *The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.
159. Financial Action Task Force (About). (n.d.). *About - Who we are*. Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/the-fatf/who-we-are.html.
160. Financial Action Task Force (Afghan opiates). (June 2014). *FATF Report: Financial flows linked to the production and trafficking of Afghan opiates.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Financial-flows-linked-to-production-and-trafficking-of-afghan-opiates.pdf.coredownload.pdf.
161. Financial Action Task Force (Annual Report). (January 30, 2023). *FATF Annual Report 2021-2022*. Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/annual-reports/Annual-Report-2021-2022.pdf.coredownload.pdf.
162. Financial Action Task Force (Countries). (n.d.). *Countries.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/countries/.
163. Financial Action Task Force (COVID-19). (May 4, 2020). *COVID-19-related Money Laundering and Terrorist Financing.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/fatfgeneral/documents/covid-19-ml-tf.html.
164. Financial Action Task Force (Emerging Terrorist Financing Risks). (October 2015). *FATF Report: Emerging Terrorist Financing Risks.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Emerging-Terrorist-Financing-Risks.pdf.coredownload.pdf.
165. Financial Action Task Force (Ethnically or Racially Motivated TF). (June 2021). *FATF Report: Ethnically or Racially Motivated Terrorism Financing.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ethnically-racially-motivated-terrorism-financing.html.
166. Financial Action Task Force (FAQs). (n.d.). *Frequently asked questions - Money Laundering.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/pages/frequently-asked-questions.html#tabs-36503a8663-item-6ff811783c-tab.
167. Financial Action Task Force (ISIL). (February 2015). *FATF Report: Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL).* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf.

168. Financial Action Task Force (Methodology). (June 2023). *Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.coredownload.pdf.
169. Financial Action Task Force (Mutual Evaluations). (n.d.). *Mutual Evaluations.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/Mutualevaluations/More-about-mutual-evaluations.html.
170. Financial Action Task Force (NPOs). (June 2014). *FATF Report: Risk of Terrorist Abuse in Non-Profit Organisations.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf.coredownload.pdf.
171. Financial Action Task Force (OECD). (n.d.). *Organisation for Economic Cooperation and Development (OECD).* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatfgaf.org/pages/organisationforeconomiccooperationanddevelopmentoecd.html.
172. Financial Action Task Force (Private Sector). (n.d.). *Private Sector - Risk and Trends Reports and Guidance.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/pages/Private-sector.html#accordion-b7a4140c7f-item-79c6556ad9.
173. Financial Action Task Force (Terrorist Financing in West Africa). (October 2013). *FATF Report: Terrorist Financing in West Africa.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/reports/TF-in-West-Africa.pdf.
174. Financial Action Task Force (The Role of Hawala). (October 2013). *FATF Report: The Role of Hawala and other similar Service Providers in Money Laundering and Terrorist Financing.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf.
175. Financial Action Task Force (Virtual Assets Red Flag Indicators). (September 14, 2020). *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.
176. Financial Action Task Force (Virtual Assets). (October 28, 2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.
177. Financial Action Task Force. (1996). *The Forty Recommendations.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201996.pdf.
178. Financial Action Task Force. (October 2001). *FATF IX Special Recommendations.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.
179. Financial Action Task Force. (June 20, 2003). *The Forty Recommendations.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202003.pdf.
180. Financial Action Task Force. (July 2011). *FATF Report: Organised Maritime Piracy and Related Kidnapping for Ransom.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/reports/organised%20maritime%20piracy%20and%20related%20kidnapping%20for%20ransom.pdf.
181. Financial Action Task Force. (October 2016). *FATF Guidance: Criminalising Terrorist Financing (Recommendation 5).* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Criminalising-Terrorist-Financing.pdf.

182. Financial Action Task Force. (July 2018). *FATF Report: Professional Money Laundering.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf.
183. Financial Action Task Force. (July 2019). *Terrorist Financing Risk Assessment Guidance.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html.
184. Financial Action Task Force. (October 2021). *FATF Recommendations 18 and 23: The Application of Group-Wide Programmes by Non-Financial Business and Professions.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/Fatfgeneral/Explanatory-materials-r18-r23.html.
185. Financial Action Task Force. (August 2022). *Anti-money laundering and counter-terrorist financing measures - Germany, Mutual Evaluation Report.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-germany-2022.html.
186. Financial Action Task Force/Egmont Group. (December 9, 2020). *Trade-based Money Laundering: Trends and Developments.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade-Based-Money-Laundering-Trends-and-Developments.pdf.
187. Financial Action Task Force/ Organization for Economic Cooperation and Development. (June 23, 2006). *Trade-Based Money Laundering.* Retrieved October 24, 2023 from FATF/GAFI: https://www.fatf-gafi.org/en/publications/methodsandtrends/documents/trade-basedmoneylaundering.html.
188. Financial Crimes Enforcement Network (Bank Secrecy Act). (n.d.). *The Bank Secrecy Act.* Retrieved October 24, 2023 from FinCEN: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act.
189. Financial Crimes Enforcement Network (History). (n.d.). *History of Anti-Money Laundering Laws.* Retrieved October 24, 2023 from FinCEN: https://www.fincen.gov/history-anti-money-laundering-laws.
190. Financial Crimes Enforcement Network (International Programs). (n.d.). *International Programs.* Retrieved October 24, 2023 from FinCEN: https://www.fincen.gov/resources/international-programs.
191. Financial Intelligence Unit. (August 2022). *Jahresbericht 2021.* Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html.
192. Financial Intelligence Unit. (May 30, 2023). *Geldwäscheprävention im Nichtfinanzsektor* . Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Aktuelles-FIU-Meldungen/2023/fiu_geldwaeschepraevention%20_nichtfinanzsektor.html.
193. Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). (June 2021). *Money laundering and terrorist financing indicators—Casinos.* Retrieved October 24, 2023 from FINTRAC: https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/indicators-indicateurs/casinos_mltf-eng.
194. Findeisen, M. (2009). Geldwäschegesetz. In P. Derleder, K.-O. Knops, H. G. Bamberger, *Handbuch zum deutschen und europäischen Bankrecht.* (Second Edition, pp. 2121-2141). Berlin/Heidelberg: Springer.
195. Friedrich, C. & Quick, R. (February 13, 2019). An analysis of anti-money laundering in the German non-financial sector. *Journal of Management and Governance, 23*(4), pp. 1099-1137. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s10997-019-09453-5.
196. Gürkan, D. (2019). *Der risikoorientierte Ansatz zur Geldwäscheprävention und seine Folgen - Geldwäschegesetz und Kreditwesengesetz im Lichte von Rechtsdogmatik und Rechtsökonomie.* Berlin: Duncker & Humblot.
197. Garcia Alvarado, F. & Antoine, M. (November 29, 2019). *The network structure of global tax evasion Evidence from the Panama Papers.* Retrieved October 24, 2023 from SSRN: http://dx.doi.org/10.2139/ssrn.3527765.

198. Gaspareniene, L., Gagyte, G., Remeikiene, R. & Matuliene, S. (January 2022). Clustering of the European Union member states based on money laundering measuring indices. *Economics and Sociology, 15*(2), pp. 153-171. Retrieved October 24, 2023 from Economics & Sociology: https://doi.org/10.14254/2071-789X.2022/15-2/10.
199. German Criminal Code (Strafgesetzbuch - StGB). (November 22, 2021). *Federal Ministry of Justice/Federal Office of Justice*. Retrieved October 24, 2023 from Gesetze im Internet: http://www.gesetze-im-internet.de/englisch_stgb/.
200. Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG). (October 29, 1993). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl193s1770.pdf%27%5D__1696425135572.
201. Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz - GwG). (May 31, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/gwg_2017/BJNR182210017.html.
202. Gesetz über das Kreditwesen (Kreditwesengesetz – KWG). (February 22, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/kredwg/BJNR008810961.html.
203. Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz - VAG). (May 31, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/vag_2016/inhalts_bersicht.html.
204. Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz - ZAG). (October 8, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/zag_2018/BJNR244610017.html.
205. Gesetz über die Verwahrung und Anschaffung von Wertpapieren (Depotgesetz - DepotG). (June 3, 2021). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/wpapg/BJNR001710937.html.
206. Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz – GwBekErgG). (August 20, 2008). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl108s1690.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl108s1690.pdf%27%5D__1696428191141.
207. Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenzregister- und Finanzinformationsgesetz). (June 30, 2021). *Bundestag.* Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-06-30-TraFinG/3-Verkuendetes-Gesetz.pdf?__blob=publicationFile&v=2.
208. Gesetz zur Modernisierung des Personengesellschaftsrechts (Personengesellschaftsrechtsmodernisierungsgesetz - MoPeG). (August 17, 2021). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl121s3436.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s3436.pdf%27%5D__1695977334835.
209. Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung. (April 21, 2017). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27943247%27%5D&skin=pdf&tlevel=-2&nohist=1&sinst=9D15889C.

210. Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie. (December 19, 2019). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl119s2602.pdf%27%5D__1696430057565.
211. Gesetz zur Umsetzung der Vierten EU-Geldwäschelinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen. (June 24, 2017). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl117s1822.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1822.pdf%27%5D__1696533629589.
212. Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen. (June 24, 2017). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1822.pdf%27%5D__1696425804441.
213. Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche. (March 17, 2021). *Bundestag.* Retrieved October 24, 2023 from Bundesgesetzblatt: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id=%27bgbl121s0327.pdf%27%5d#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s0327.pdf%27%5D__1696330072144.
214. Golindano Acevedo, R. & Pitters, J. (February 2021). Staat versus Querdenker: Eine sozial- und kommunikationspsychologische Betrachtung der Coronavirus-Pandemie. *IUBH Discussion Papers - Sozialwissenschaften, 2*(3). Retrieved October 24, 2023 from Econstor: https://www.econstor.eu/bitstream/10419/231774/1/1751199444.pdf.
215. Government of Western Australia. (n.d.). *False billing.* Retrieved October 24, 2023 from WA ScamNet: https://www.scamnet.wa.gov.au/scamnet/Scam_types-Buying_or_selling-False_billing.htm.
216. Groth, L. (2016). *Globales Finanzmarktrecht gegen Terrorismusfinanzierung.* Baden-Baden: Nomos Verlagsgesellschaft.
217. Grundgesetz für die Bundesrepublik Deutschland (GG). (December 19, 2022). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/gg/BJNR000010949.html.
218. Hanley-Giersch, J. (June 1, 2019). *Handelsbasierte Geldwäsche– Risikofaktoren und Sorgfaltspflichten.* Retrieved October 24, 2023 from ACAMS Today: https://www.acamstoday.org/handelsbasierte-geldwasche-risikofaktoren-und-sorgfaltspflichten/.
219. Hardouin, P. (July 17, 2009). Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing. *Journal of Financial Crime, 16*(3), pp. 199-209. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/13590790910971757.
220. Heitmüller, U. & Von Lampe, K. (2020). The 'rocker' phenomenon in Germany: Perceptions and government responses to out- law bikers in historical perspective. In P. Van Duyne, D. Siegel, G. A. Antonopoulos, J. H. Harvey & K. Von Lampe, *Criminal Defiance in Europe and beyond: from organised crime to crime-terror nexus* (pp. 477-503). The Hague: Eleven International Publishing.
221. Herzog, F., & Achtelik, O. (2014). *Kommentar zum Geldwäschegesetz (GwG).* (Second Edition). München: C.H. Beck.
222. His Majesty's Treasury. (May 2019). *Cash and digital payments in the new economy: summary of responses.* Retrieved October 24, 2023 from Government UK: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799548/CfE_-_Cash___Digital_Payments_Response_020519_vf_digicomms.pdf.
223. Hlavica, C., Thomann, D. & Martenstein, I. (2017). Grundlagen zum Phänomen Wirtschaftskriminalität. In C. Hlavica, F. M. Hülsberg & U. Klapproth, *Tax Fraud & Forensic*

Accounting - Umgang mit Wirtschaftskriminalität (Second Edition, pp. 37-76). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/978-3-658-07840-9.

224. Holá, A., Arltová, M. & Zídková, H. (May 12, 2022). VAT Listings within the EU Member States and Their Impact on Tax Evasion. *CESifo Economic Studies, 68*(3), pp. 297–318. Retrieved October 24, 2023 from Oxford University Press: https://doi.org/10.1093/cesifo/ifac002.
225. Honda, M. (2020). "Smart sanctions" by the UN and financial sanctions. In S. Yoshimura, *United Nations Financial Sanctions* (pp. 18-33). London: Routledge. Retrieved October 24, 2023 from Taylor & Francis Group: https://doi-1org-1gxsabj8h03d0.erf.sbb.spk-berlin.de/10.4324/9780429260315.
226. Human Rights Watch. (March 14, 2006). *Funding the "Final War" - LTTE Intimidation and Extortion in the Tamil Diaspora.* Retrieved October 24, 2023 from HRW: https://www.hrw.org/report/2006/03/14/funding-final-war/ltte-intimidation-and-extortion-tamil-diaspora.
227. Hunter, L. Y. & Biglaiser, G. (April 2022). The Effects of the International Monetary Fund on DomesticTerrorism. *Terrorism and Political Violence, 34*(3), pp. 489–513. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/09546553.2019.1709448.
228. Husabø, E. J. & Bruce, I. (2009). *Fighting Terrorism through Multilevel Criminal Legislation.* Leiden/Boston: Martinus Nijhoff Publishers. Retrieved October 24, 2023 from Brill: https://doi.org/10.1163/ej.9789004177574.i-488.2.
229. Ingves, S. (June 2018). *Going Cashless.* Retrieved October 24, 2023 from IMF: https://www.imf.org/en/Publications/fandd/issues/2018/06/central-banks-and-digital-currencies-point.
230. International Convention for the Suppression of the Financing of Terrorism. (December 2, 1999). *United Nations.* Retrieved October 24, 2023 from Treaties United Nations: https://treaties.un.org/doc/db/terrorism/english-18-11.pdf.
231. International Criminal Police Organization (Fraud linked to COVID-19). (March 13, 2020). *INTERPOL warns of financial fraud linked to COVID-19.* Retrieved October 24, 2023 from Interpol: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19.
232. International Criminal Police Organization (Non-delivery scams). (August 6, 2020). *5 reasons non-delivery scams work.* Retrieved October 24, 2023 from Interpol: https://www.interpol.int/News-and-Events/News/2020/5-reasons-non-delivery-scams-work.
233. International Monetary Fund. (June 29, 2016). *Germany: Financial Sector Assessment Program-Anti-Money Laundering and Combating the Financing of Terrorism-Technical Notes.* Retrieved October 24, 2023 from IMF: https://www.imf.org/en/Publications/CR/Issues/2016/12/31/Germany-Financial-Sector-Assessment-Program-Anti-Money-Laundering-and-Combating-the-44014.
234. International Monetary Fund. (n.d.). *Anti-Money Laundering/Combating the Financing of Terrorism.* Retrieved October 24, 2023 from IMF: https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm.
235. International Money Laundering Information Network. (n.d.). *About Us.* Retrieved October 24, 2023 from IMoLIN: https://www.imolin.org/imolin/en/about_us.html.
236. Irwin, A. S. & Turner, A. B. (July 2, 2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of Money Laundering Control, 21*(3), pp. 297-313. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-07-2017-0031.
237. Jacobson, M. (March 9, 2010). Terrorist Financing and the Internet. *Studies in Conflict & Terrorism, 33*(4), pp. 353-363. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/10576101003587184.
238. Jagtap, M. V. (March 2017). Situational Analysis of Cashless Society. *Conference: Digitization: Impact on Indian Society, Rajarambapu Institute of Technology, Islampur.* Retrieved October 24, 2023 from ResearchGate: https://www.researchgate.net/publication/314214443_Situational_Analysis_of_Cashless_Society.

239. Jakobi, A. P. (2015). Normbildung - Terrorismusfinanzierungsbekämpfung als Referenzgebiet? In M. Albers & L. Groth, *Globales Recht und Terrorismusfinanzierungsbekämpfung* (pp. 67-83). Baden-Baden: Nomos Verlagsgesellschaft.
240. Jalkebro, R. & Vlcek, W. (2023). The future of criminal finance: 'bin Ladens' and the cashless society. In D. Jasinski, A. Phillips & E. Johnston, *Organised Crime, Financial Crime, and Criminal Justice: Theoretical Concepts and Challenges* (pp. 104-121). London: Routledge. Retrieved October 24, 2023 from Taylor & Francis Group: https://doi-1org-1gxsabj8h06e6.erf.sbb.spk-berlin.de/10.4324/9781003020813.
241. Jentleson, B. W. (2022). *Sanctions: what everyone needs to know.* New York: Oxford University Press. Retrieved October 24, 2023 from ProQuest Ebook Central: https://ebookcentral-1proquest-1com-1008dea8h093c.erf.sbb.spk-berlin.de/lib/staatsbibliothek-berlin/detail.action?docID=7075522#.
242. Jiao, M. (May 21, 2023). Big Data Analytics for Anti-Money Laundering Compliance in the Banking Industry. *Highlights in Science, Engineering and Technology, 49*, pp. 302–309. Retrieved October 24, 2023 from Darcy & Roy Press: https://drpress.org/ojs/index.php/HSET/article/view/8522/8295.
243. Jo, H., Hsu, A., Llanos-Popolizio, R. & Vergara-Vega, J. (March 25, 2021). Corporate Governance and Financial Fraud of Wirecard. *European Journal of Business & Management Research, 6*(2), pp. 96-106. Retrieved October 24, 2023 from EJBMR: https://doi.org/10.24018/ejbmr.2021.6.2.708.
244. John, H. & Naaz, S. (April 30, 2019). Credit Card Fraud Detection using Local Outlier Factor and Isolation Forest. *International Journal of Computer Sciences and Engineering, 7*(4), pp. 1060-1064. Retrieved October 24, 2023 from JCSE: https://doi.org/10.26438/ijcse/v7i4.10601064.
245. Kadir, E. A., Shamsuddin, S. M. & Rosa, S. L. (August 19-20, 2015). Application of NFC Technology for Cashless Payment System in Canteen. *Proceeding of International Conference on Electrical Engineering, Computer Science and Informatics (EECSI 2015)*, pp. 180–183. Retrieved October 24, 2023 from CORE: https://core.ac.uk/download/pdf/296975687.pdf.
246. Kang, S. (April 20, 2018). Rethinking The Global Anti-Money Laundering Regulations to Deter Corruption. *International and Comparative Law Quarterly, 67*(3), pp. 695-720. Retrieved October 24, 2023 from Cambridge University Press: https://doi.org/10.1017/S0020589318000106.
247. Kapitalanlagegesetzbuch (KAGB). (February 22, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/kagb/BJNR198110013.html.
248. Kaufmann, A. (2017). Unternehmen im Fokus von Geldwäscheaktivitäten. In C. Hlavica, F. M. Hülsberg & U. Klapproth, *Tax Fraud & Forensic Accounting - Umgang mit Wirtschaftskriminalität* (Second Edition, pp. 159-200). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/978-3-658-07840-9.
249. Kersten, A. (2002). Financing of Terrorism - A Predicate Offence to Money Laundering? In M. Pieth, *Financing Terrorism* (pp. 49-56). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/0-306-48044-1_4.
250. Kleemans, E. & Van Koppen, V. (February 2020). Organized Crime and Criminal Careers. *Crime and Justice, 49*, pp. 385-423. Retrieved October 24, 2023 from University of Chicago Press Journals: https://doi.org/10.1086/707318.
251. Klein, P. (2009). *International Convention for the Suppression of the Financing of Terrorism.* Retrieved October 24, 2023 from United Nations Audiovisual Library of International Law: https://legal.un.org/avl/pdf/ha/icsft/icsft_e.pdf.
252. Knobel, A. (February 6, 2023). *Roadmap to Effective Beneficial Ownership Transparency (REBOT).* Retrieved October 24, 2023 from SSRN: http://dx.doi.org/10.2139/ssrn.4470178.
253. Korejo, M. S., Rajamanickam, R. & Said, M. H. (August 24, 2021). The concept of money laundering: a quest for legal definition. *Journal of Money Laundering Control, 24*(4), pp. 725-736. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-05-2020-0045.

254. Koseli, M., Ekici, N., Eren, M. E. & Bitner, C. (March 26, 2020). Use of kidnapping and extortion as a tool for financing terrorism: the case of the PKK. *Behavioral Sciences of Terrorism and Political Aggression, 13*(3), pp. 215-230. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/19434472.2020.1745257.
255. Kotkowski, R. & Polasik, M. (December 2021). COVID-19 pandemic increases the divide between cash and cashless payment users in Europe. *Economic Letters, 209*. Retrieved October 24, 2023 from ScienceDirect: https://www.sciencedirect.com/science/article/pii/S016517652100416X.
256. Kotter. (n.d.). *The 8 Steps for Leading Change.* Retrieved October 24, 2023 from Kotter Inc.: https://www.kotterinc.com/methodology/8-steps/.
257. Kotter, J. P. (November 2012). *Accelerate!* Retrieved October 24, 2023 from Harvard Business Review: https://hbr.org/2012/11/accelerate.
258. Kraemer, P., Niebel, C. & Reiberg, A. (February 2023). *Gaia-X and Business Models: Types and Examples.* Retrieved October 24, 2023 from Gaia-X Hub Germany: https://gaia-x-hub.de/wp-content/uploads/2023/02/Whitepaper-Gaia-X-Business-Models.pdf.
259. Kriminalpolizei. (n.d.). *Betrug.* Retrieved October 24, 2023 from Kriminalpolizei: https://www.kriminalpolizei.de/service/praevention-kompakt.html?tx_dpnglossary_glossary%5Baction%5D=show&tx_dpnglossary_glossary%5Bcontroller%5D=Term&tx_dpnglossary_glossary%5Bterm%5D=272&cHash=e392b5cd2584064435a2b9067f8b879c.
260. Kumari, N. & Khanna, J. (2017). Cashless payment: A behaviourial change to economic growth. *Qualitative and Quantitative Research Review, 2*(2), pp. 83–103. Retrieved October 24, 2023 from NFCT: https://nfct.co.uk/wp-content/uploads/journal/published_paper/volume-2/issue-2/LS0q4m3F.pdf.
261. Le, T. H. & Doan, N. T. (April 2023). Economic sanctions and global banking flows: the moderating roles of financial market properties and insitutional quality. *The Journal of International Trade & Economic Development, 32*(3), pp. 365-390. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/09638199.2022.2119486.
262. Lénártová, G. (2020). The Economic and Social Consequences of Tax Havens in the World. *SHS Web of Conferences, 83*. Retrieved October 24, 2023 from EDP Sciences: https://doi.org/10.1051/shsconf/20208301041.
263. Levi, M. (July 1, 2002). Money Laundering and Its Regulation. *The ANNALS of the American Academy of Political and Social Science, 582*(1), pp. 181-194. Retrieved October 24, 2023 from Sage Journals: https://doi.org/10.1177/000271620258200113.
264. Levi, M. (January 28, 2010). E-gaming and money laundering risks: a European overview. *ERA Forum, 10*(4), pp. 533-546. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s12027-009-0143-2.
265. Levi, M. (July 17, 2022). Lawyers as money laundering enablers? An evolving and contentious relationship. *Global Crime, 23*(2), pp. 126–147. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/17440572.2022.2089122.
266. Levi, M. & Soudijn, M. R. J. (March 2020). Understanding the laundering of organized crime money. *Crime and Justice, 49*(2), pp. 579-631. Retrieved October 24, 2023 from University of Chicago Press Journals: https://doi.org/10.1086/708047.
267. Levi, M., Reuter, P. & Halliday, T. (March 2018). Can the AML system be evaluated without better data? *Crime Law Soc Change, 69*(4), pp. 307–328. Retrieved October 24, 2023 Springer Nature: https://doi.org/10.1007/s10611-017-9757-4.
268. Levy, I. & Yusuf, A. (December 2, 2021). How Do Terrorist Organizations Make Money? Terrorist Funding and Innovation in the Case of al-Shabaab. *Studies in Conflict & Terrorism, 44*(12), pp. 1167-1189. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/1057610X.2019.1628622.
269. Lindsay, M. G. (2023). International Rise of Cryptocurrency: A Comparative Review of the United States, Mexico, Singapore, and Switzerland's Anti-Money Laundering (AML) Regulation. *South Carolina Journal of International Law and Business, 19*(2), pp. 161-185. Retrieved October 24, 2023 from SCJILB: https://scholarcommons.sc.edu/scjilb/vol19/iss2/8/.

270. Lumley-Sapanski, A. & Schwarz, K. (2022). Increased vulnerability to human trafficking of migrants during the COVID-19 pandemic in the IGAD–North Africa region. In International Organization for Migration, *The Impacts of COVID-19 on Migration and Migrants from a Gender Perspective* (pp. 145-157). Retrieved October 24, 2023 from IOM: https://publications.iom.int/system/files/pdf/impacts-of-COVID-19-gender_1.pdf.
271. Macdonald, S. (July 2009). The Unbalanced Imagery of Anti-Terrorism Policy. *Cornell Journal of Law and Public Policy*, *18*(2), pp. 519-540. Retrieved October 24, 2023 from ResearchGate: https://www.researchgate.net/publication/256668924_The_Unbalanced_Imagery_of_Anti-Terrorism_Policy.
272. Massi, M., Sullivan, G., Strauß, M. & Khan, M. (May 28, 2019). *How Cashless Payments Help Economies Grow.* Retrieved October 24, 2023 from Boston Consulting Group: https://www.bcg.com/publications/2019/cashless-payments-help-economies-grow.
273. Matthes, J. (June 13, 2022). Gegenseitige Abhängigkeit im Handel zwischen China, der EU und Deutschland: Eine empirische Faktensammlung. *IW-Report, No. 35/2022*, Retrieved October 24, 2023 from Institut der deutschen Wirtschaft: https://www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2022/IW-Report-2022-Gegenseitige-Abhaengigkeiten.pdf.
274. McClean, D. (March 2007). *Transnational Organized Crime, A Commentary on the UN Convention and its Protocols.* Retrieved October 24, 2023 from Oxford University Press: https://doi.org/10.1093/law/9780199217724.001.0001.
275. McFadden, S. W. (February 2019). German citizenship law and the Turkish diaspora. *German Law Journal, 20*(1), pp. 72–88. Retrieved October 24, 2023 from Cambridge University Press: https://doi.org/10.1017/glj.2019.7.
276. McGuinness, M. (May 12, 2023). *Parliamentary question - E-001048/2023(ASW) - Answer given by Ms McGuinness on behalf of the European Commission.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/doceo/document/E-9-2023-001048-ASW_EN.html#:~:text=At%20present%2C%20no%20EU%2Dwide,in%20place%20to%20maintain%20them.
277. Meißner, M. (2017). Die Reform der strafrechtlichen Vermögensabschöpfung – ein Ehrgeizprojekt oder: Höher, schneller, weiter… das neue Abschöpfungsrecht aus Sicht des Strafverteidigers. *Kriminalpolitische Zeitschrift, 2*(4), pp. 237-243. Retrieved October 24, 2023 from KriPoZ: https://kripoz.de/wp-content/uploads/2017/07/meissner-die-reform-der-strafrechtlichen-vermoegensabschoepfung.pdf.
278. Middel, S. (2007). *Innere Sicherheit und präventive Terrorismusbekämpfung.* Baden-Baden: Nomos Verlagsgesellschaft.
279. Mileusnic, M. (October 2023). *Anti-money laundering measures in national recovery and resilience plans.* Retrieved October 24, 2023 from European Parliament: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/753967/EPRS_BRI(2023)753967_EN.pdf.
280. Miller, R. S., Rosen, L. W. & Jackson, J. K. (June 22, 2016). *Trade-Based Money Laundering: Overview and Policy Issues.* Retrieved October 24, 2023 from Congressional Research Service: http://goodtimesweb.org/industrial-policy/2016/R44541.pdf.
281. Mugarura, N. (January 2, 2018). Can "harmonization" antidote tax avoidance and other financial crimes globally? *Journal of Financial Crime, 25*(1), pp. 187-209. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JFC-06-2016-0045.
282. Murr, A., Donovan, T. & Yu, Y. M. (2023). The Role of the Private Sector in Detecting and Disrupting Terrorist Financing Activities. In C. El Khoury, *Countering the financing of terrorism: good practices to enhance effectiveness* (pp. 41-62). Retrieved October 24, 2023 from IMF eLIBRARY: https://doi.org/10.5089/9798400204654.071.
283. Murrar, F. (COVID-19). (March 14, 2022). Fraud schemes during COVID-19: a comparison from FATF countries. *Journal of Financial Crime, 29*(2), pp. 533-540. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JFC-09-2021-0203.

284. Murrar, F. (Non-profit organisations). (January 3, 2022). Adopting a risk-based approach for non-profit organisations. *Journal of Money Laundering Control, 25*(1), pp. 19-26. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-12-2020-0144.
285. Naheem, M. A. (2016). Trade based money laundering: A primer for banking staff. *International Journal of Disclosure and Governance, 14*(2), pp. 95-117. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1057/jdg.2015.21.
286. Naheem, M. A. (AML, digital currencies and blockchain technology). (July 2, 2019). Exploring the links between AML, digital currencies and blockchain technology. *Journal of Money Laundering Control, 22*(3), pp. 515-526. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-11-2015-0050.
287. Naheem, M. A. (Combating money laundering and terrorist financing). (May 7, 2019). Saudi Arabia's efforts on combating money laundering and terrorist financing (Review undertaken in September 2017). *Journal of Money Laundering Control, 22*(2), pp. 233-246. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-10-2018-0065.
288. Najib, M. & Fahma, F. (2020). Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium enterprises. *International Journal on Advanced Science Engineering Information Technology, 10*(4), pp. 1702–1708. Retrieved October 24, 2023 from INSIGHT - Indonesian Society for Knowledge and Human Development: https://doi.org/10.18517/ijaseit.10.4.11616.
289. National Crime Agency. (May 25, 2021). *National Strategic Assessment of Serious and Organised Crime.* Retrieved October 24, 2023 from National Crime Agency: https://nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file.
290. Oberste Aufsichtsbehörden der Länder im Glücksspielsektor. (November 2020). *Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG).* Retrieved October 24, 2023 from Gemeinsame Glücksspielbehörde der Länder: https://www.gluecksspiel-behoerde.de/images/pdf/AuA%20GwG%20-%20Gluecksspiel%20Final%20Stand%2010.11.2020.pdf.
291. Oftedal, E. (January 6, 2015). *The financing of jihadi terrorist cells in Europe.* Retrieved October 24, 2023 from Forsvarets forskningsinstitutt: https://publications.ffi.no/nb/item/asset/dspace:2469/14-02234.pdf.
292. O'Donovan, J., Wagner, H. F. & Zeume, S. (February 11, 2019). The Value of Offshore Secrets: Evidence from the Panama Papers. *The Review of Financial Studies, 32*(11), pp. 4117-4155. Retrieved October 24, 2023 from Oxford University Press: https://doi.org/10.1093/rfs/hhz017.
293. Okina, Y. (February 27, 2022). Digitalization of Payment Instruments: Cashless Payments and Loyalty Points Systems. In M. Heckel & F. Waldenberger, *The Future of Financial Systems in the Digital Age - Perspectives in Law, Business and Innovation* (pp. 117–131). Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/978-981-16-7830-1_7.
294. Oostrom, T. G., Cullen, P. & Peters, S. A. (March 10, 2022). The indirect health impacts of the COVID-19 pandemic on children and adolescents: A review. *Journal of Child Health Care, 27*(3), pp. 488–508. Retrieved October 24, 2023 from Sage Journals: https://doi.org/10.1177/13674935211059980.
295. Opitek, P. (September 30, 2021). Real estate agent as the institution obliged to counteract money laundering (Part Two). *Nieruchomości@, 3*(3), pp. 115-131. Retrieved October 24, 2023 from Index Copernicus International: https://doi.org/10.5604/01.3001.0015.2483.
296. Organization for Economic Cooperation and Development (About). (n.d.). *About - Who we are.* Retrieved October 24, 2023 from OECD: https://www.oecd.org/about/.
297. Organization for Economic Cooperation and Development (Global Forum). (n.d.). *Global Forum on Transparency and Exchange of Information for Tax Puposes.* Retrieved October 24, 2023 from OECD: https://www.oecd.org/tax/transparency/.
298. Organization for Economic Cooperation and Development. (November 21, 1997). *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.* Retrieved October 24, 2023 from OECD: https://www.oecd.org/daf/anti-bribery/ConvCombatBribery_ENG.pdf.

299. Organization for Economic Cooperation and Development. (2007). *Report on Tax Fraud and Money Laundering Vulnerabilities involving the Real Estate Sector.* Retrieved October 24, 2023 from OECD: https://www.oecd.org/ctp/exchange-of-tax-information/42223621.pdf.
300. Organization for Economic Cooperation and Development. (2015). *G20/OECD Principles of Corporate Governance.* Retrieved October 24, 2023 from OECD: https://www.oecd.org/daf/ca/Corporate-Governance-Principles-ENG.pdf.
301. Organization for Economic Cooperation and Development. (2019). *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors.* Retrieved October 24, 2023 from OECD: https://www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf.
302. Passas, N. (January 2, 2018). Report on the debate regarding EU cash payment limitations. *Journal of Financial Crime*, *25*(1), pp. 5-27. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JFC-06-2017-0058.
303. Perciun, R., Iordachi, V. & Timofei, O. (May 14-15, 2020). Non-cash payment - a stringent necessity in pandemic conditions. *International Symposium: Experience. Knowledge. Contemporary Challenges - „Humanity at a crossroad. Between digital Economy and Need for a Paradigm of going back to Nature"*, pp. 630-646. Retrieved October 24, 2023 from DSpace: http://dspace.ince.md/xmlui/bitstream/handle/123456789/1399/Non-cash_payment-a_stringent_necessity_in_pandemic_conditions.pdf?sequence=1&isAllowed=y.
304. Pintaske, P. M. (2014). *Das Palermo-Übereinkommen und sein Einfluss auf das deutsche Strafrecht, Eine Untersuchung der UN-Konvention gegen grenzüberschreitende organisierte Kriminalität und ihrer Zusatzprotokolle.* Göttingen: V & R unipress.
305. Preble, K. A. & Early, B. R. (September 8, 2023). Enforcing economic sanctions by tarnishing corporate reputations. *Business and Politics*, pp. 1-22. Retrieved October 24, 2023 from Cambridge University Press: https://doi.org/10.1017/bap.2023.22.
306. President's Commission on Organized Crime. (October 1984). *The Cash Connection: Organized crime, financial institutions and money laundering.* Retrieved October 24, 2023 from Office of Justice Programs: https://www.ojp.gov/pdffiles1/Digitization/166517NCJRS.pdf.
307. Primoratz, I. (November 2, 2022). *Terrorism.* Retrieved October 24, 2023 from Stanford Encyclopedia of Philosophy: https://plato.stanford.edu/entries/terrorism/.
308. Proposal for a Regulation of the European Parliament and the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. (July 20, 2021). *European Commission.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420.
309. Purcell, J., Schantz, D. & Shire, J. (2023). Terrorism-Related Targeted Financial Sanctions. In C. El Khoury, *Countering the financing of terrorism: good practices to enhance effectiveness* (pp. 113-152). Retrieved October 24, 2023 from IMF eLIBRARY: https://doi.org/10.5089/9798400204654.071.
310. Rahimi, H. (April 8, 2021). How to create better Hawala regulations: a case study of Hawala regulations in Afghanistan. *Crime, Law and Social Change*, *76*(2), pp. 131–148. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s10611-021-09959-w.
311. Rat für Sozial- und Wirtschaftsdaten. (February 28, 2020). *Weiterentwicklung der Kriminal- und Strafrechtspflegestatistik in Deutschland - Output 7(6).* Retrieved October 24, 2023 from RatSWD: https://www.konsortswd.de/wp-content/uploads/RatSWD_Output7.6_Kriminalstatistik.pdf.
312. Rebscher, E. & Vahlenkamp, W. (1988). *Organisierte Kriminalität in der Bundesrepublik Deutschland: Bestandsaufnahme, Entwicklungstendenzen und Bekämpfung aus der Sicht der Polizeipraxis.* Wiesbaden: Bundeskriminalamt.
313. Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds (Document 32006R1781). (November 15, 2006). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1781&from=DE.
314. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006

(Document 32015R0847). (May 20, 2015). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN.

315. Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls on cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005 (Document 32018R1672). (October 23, 2018). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1672&qid=1680259158984&from=en.
316. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Document 32023R1113). (June 9, 2023). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1113.
317. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Document 32023R1114). (June 9, 2023). *The European Parliament and the Council of the European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114.
318. Reiling, J. (April 26, 2022). *The John Kotter Change Management Model for Strategic PM's.* Retrieved October 24, 2023 from The Strategic Project Manager: https://bethestrategicpm.com/the-john-kotter-change-management-model-for-strategic-pms/.
319. Resolution 1373 (2001). (September 28, 2001). *United Nations Security Council.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf.
320. Resolution 1377 (2001). (November 12, 2001). *United Nations Security Council.* Retrieved October 24, 2023 from UN: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/633/01/PDF/N0163301.pdf?OpenElement.
321. Resolution 1566 (2004). (October 8, 2004). *United Nations Security Council.* Retrieved October 24, 2023 from UN: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement.
322. Reuter, P. & Truman, E. (2004). *Chasing Dirty Money – The Fight Against Money Laundering.* Washington, D.C.: Peterson Institute for International Economics.
323. Rivera, J. W. (May 7, 2019). Potential negative effects of a cashless society: Turning citizens into criminals and other economic dangers. *Journal of Money Laundering Control, 22*(2), pp. 350-358. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-04-2018-0035.
324. Rohde, P., Dienstbühl, D. & Labryga, S. (September 2019). *Clankriminalität in Deutschland - Eine Bestandsaufnahme (Teil 1)*. Retrieved October 24, 2023 from Kriminalpolizei: https://www.kriminalpolizei.de/ausgaben/2019/september/detailansicht-september/artikel/clankriminalitaet-in-deutschlandeine-bestandsaufnahme-teil-1.html.
325. Rusche, C. (March 15, 2022). Einführung in Gaia-X: Hintergrund, Ziele und Aufbau. *IW-Report, No. 10/2022*. Retrieved October 24, 2023 from Institut der deutschen Wirtschaft: https://www.iwkoeln.de/studien/christian-rusche-einfuehrung-in-gaia-x-hintergrund-ziele-und-aufbau.html.
326. Saenz, M. & Lewer, J. J. (December 1, 2022). Estimates of Trade Based Money Laundering within the European Union. *Applied Economics, 55*(51), pp. 5991–6003. Retrieved October 24, 2023 from Taylor & Francis Online: https://doi.org/10.1080/00036846.2022.2141444.
327. Schäfer, D. (August 21, 2020). Wirecard – ein Menetekel für die Wirtschaftsprüfung. *Wirtschaftsdienst: Zeitschrift für Wirtschaftspolitik, 100*(8), pp. 562-563. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s10273-020-2705-4.
328. Schallbruch, M. (March 16, 2021). Mehr Unabhängigkeit für das BSI? Aufgaben und Steuerung des Bundesamtes für Sicherheit in der Informationstechnik. *Datenschutz und*

Datensicherheit - DuD, 45(4), pp. 229-233. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s11623-021-1424-3.

329. Schleswig-Holstein Finanzministerium. (August 12, 2020). *Wichtige Änderungen des Geldwäschegesetzes zum 01.01.2020.* Retrieved October 24, 2023 from Schleswig-Holstein: https://www.schleswig-holstein.de/DE/fachinhalte/M/marktueberwachung/Downloads/Geldwaesche/aenderungen_gwg_pdf.pdf?__blob=publicationFile&v=1.
330. Schneider, F., Dreer, E. & Riegler, W. (2006). *Geldwäsche: Formen, Akteure, Größenordnung - und warum die Politik machtlos ist.* Wiesbaden: Gabler Verlag.
331. Scholz, Y. J. (October 20, 2020). *Die Auswirkungen des Geldwäschegesetzes (GwG) auf die leichtfertige Geldwäsche gemäß § 261 Abs. 5 StGB*. Retrieved October 24, 2023 from University Bonn: https://bonndoc.ulb.uni-bonn.de/xmlui/bitstream/handle/20.500.11811/8695/5934.pdf?sequence=1&isAllowed=y.
332. Schroth, M. & Vyborny, M. Z. (June 2022). Should the use of cash be limited? In Österreichische Nationalbank, *Monetary Policy & The Economy Q1-Q2/22* (pp. 109-119). Retrieved October 24, 2023 from OeNB: https://www.oenb.at/dam/jcr:59eef5a1-77af-4103-9d66-07ba021a0b47/08_Mop_Q1-2_22_Should-the-use-of-cash-be-limited.pdf.
333. Schunck, C. H., Sellung, R. & Rossnagel, H. (March 2021). *KI zur Verhinderung von Identitätsbetrug.* Retrieved October 24, 2023 from Fraunhofer-Insitut für Arbeitswirtschft und Organisation IAO: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/1da2b9c5-a80b-40d8-83a4-b83e5c3480c4/content.
334. Sellhorn, T. (August 3, 2020). Wirecard – der Weckruf. *Der Betrieb, 31*, pp. M4-M5. Retrieved October 24, 2023 from Ludwig-Maximilian-Universität München: https://www.rwp.bwl.uni-muenchen.de/aktuelles/aktuelles-forschung/sonstige-forschung/sellhorn-wirecard-der-berieb/sellhorn_wirecard_der-betrieb.pdf.
335. Senatsverwaltung für Justiz und Verbraucherschutz. (October 6, 2022). *Task-Force Geldwäsche schult fast 400 Notarinnen und Notare.* Retrieved October 24, 2023 from Berlin: https://www.berlin.de/sen/justv/presse/pressemitteilungen/2022/pressemitteilung.1251413.php.
336. Senatsverwaltung für Wirtschaft, Energie und Betriebe. (April 26, 2021). *Berliner Risikoanalyse - Geldwäsche und Terrorismusfinanzierung, Kurzfassung Nicht-Finanzsektor*. Retrieved October 24, 2023 from Berlin: https://www.berlin.de/sen/wirtschaft/wirtschaftsrecht/geldwaesche/downloads/.
337. Sergi, A. (August 2019). The Calabrian 'Ndrangheta: Between Tradition and Mobility. In R. M. Lombardo, *Organized Crime: Causes and Consequences - Criminal Justice, Law Enforcement and Corrections* (pp. 115-132). New York: Nova Science Publishers.
338. Shetterly, D. (2006). Starving the Terrorists of Funding: How the United States Treasury is Fighting the War on Terror. *Regent University Law Review, 18*(2), pp. 327-348. Retrieved October 24, 2023 from Regent University: https://www.regent.edu/acad/schlaw/student_life/studentorgs/lawreview/docs/issues/v18n2/6%20Shetterly.pdf.
339. Sieber, U. & Vogel, B. (2015). *Terrorismusfinanzierung - Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht.* Berlin: Duncker & Humblot.
340. Singh, K. & Best, P. (September 2019). Anti-Money Laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems, 34*. Retrieved October 24, 2023 from ScienceDirect: https://doi.org/10.1016/j.accinf.2019.06.001.
341. Soudijn, M. R. J. (July 4, 2016). Rethinking money laundering and drug trafficking - Some implications for investigators, policy makers and researchers. *Journal of Money Laundering Control, 19*(3), pp. 298-310. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-07-2015-0028.
342. Staatsvertrag zur Neuregulierung des Glücksspielwesens in Deutschland (Glücksspielstaatsvertrag 2021 – GlüStV 2021) vom 29. Oktober 2020. (October 29, 2020). *Die Länder*. Retrieved October 24, 2023 from Gesetze Bayern: https://www.gesetze-bayern.de/Content/Document/StVGlueStV2021/true.

343. Statista Research Department (Credit institutions). (February 8, 2023). *Number of credit institutions in the Eurozone as of September 2022, by country*. Retrieved October 24, 2023 from Statista: https://www.statista.com/statistics/349129/eu-18-credit-institutions-number/.
344. Statista Research Department (Frankfurt Stock Exchange). (May 10, 2023). *Frankfurt Stock Exchange - statistics & facts.* Retrieved October 24, 2023 from Statista: https://www.statista.com/topics/10784/frankfurt-stock-exchange/#:~:text=With%20a%20market%20capitalization%20of,and%20the%20London%20Stock%20Exchange.
345. Statista Research Department. (May 5, 2023). *Verteilung der dominierenden Staatsangehörigkeiten in Gruppierungen der Clankriminalität im Umfeld der Organisierten Kriminalität in Deutschland im Jahr 2021*. Retrieved October 24, 2023 from Statista: https://de.statista.com/statistik/daten/studie/1058034/umfrage/verteilung-der-staatsangehoerigkeiten-bei-der-clankriminalitaet-in-deutschland/.
346. Strafgesetzbuch (StGB). (July 26, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/stgb/BJNR001270871.html#BJNR001270871BJNG000102307.
347. Stroligo, K., Hsu, C.-L. & Kouts, T. (2018). *Financial Intelligence Units Working With Law Enforcement Authorities and Prosecutors.* Retrieved October 24, 2023 from World Bank: https://documents1.worldbank.org/curated/en/741651547823413372/pdf/133871-WP-PUBLIC-17-1-2019-17-40-44-fiusreportsk.pdf.
348. Suendorf, U. (2001). *Geldwäsche - Eine kriminologische Untersuchung.* Neuwied/Kriftel: Luchterhand Verlag.
349. Sullivan, C. & Smith, E. (February 2, 2012). Trade-Based Money Laundering: Risks and Regulatory Responses. *AIC Reports: Research and Public Policy Series, 115*. Retrieved October 24, 2023 from Australian Institute of Criminology: https://www.aic.gov.au/sites/default/files/2020-05/rpp115.pdf.
350. Sveriges Riksbank. (April 4, 2023). *E-krona.* Retrieved October 24, 2023 from Riksbank: https://www.riksbank.se/en-gb/payments--cash/e-krona/.
351. Swedish Institute. (November 25, 2022). *In Sweden, technology is close to making cash a thing of the past. All aboard with the cashless society?* Retrieved October 24, 2023 from Sweden: https://sweden.se/life/society/a-cashless-society.
352. Syring, T. (June 2012). Protecting the Protectors or Victimizing the Victims Anew? "Material Support of Terrorism" and Exclusion from Refugee Status in U.S. and European Courts. *ILSA Journal of International & Comparative Law, 18*(2), pp. 597-614. Retrieved October 24, 2023 from NSUWorks: https://nsuworks.nova.edu/ilsajournal/vol18/iss2/14.
353. Tax Justice Network. (2022). *Financial Secrecy Index 2022.* Retrieved October 24, 2023 from Tax Justice Network: https://fsi.taxjustice.net.
354. Teichmann, F. M. (May 2, 2017). Twelve methods of money laundering. *Journal of Money Laundering Control, 20*(2), pp. 130-137. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-05-2016-0018.
355. Teichmann, F. M. (Financing terrorism through cryptocurrencies). (October 1, 2018). Financing terrorism through cryptocurrencies – a danger for Europe? *Journal of Money Laundering Control, 21*(4), pp. 513-519. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-06-2017-0024.
356. Teichmann, F. M. (Real estate money laundering). (July 2, 2018). Real estate money laundering in Austria, Germany, Liechtenstein and Switzerland. *Journal of Money Laundering Control, 21*(3), pp. 370-375. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-09-2017-0043.
357. Teichmann, F. M. (March 2020). Recent trends in money laundering. *Crime, Law and Social Change, 73*(4), pp. 237-247. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s10611-019-09859-0.
358. Thießen, F. (July 2021). Digitaler Euro: Funktionsweise und kritische Würdigung. *Wirtschaftsdienst, 101*(7), pp. 529-535. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s10273-021-2960-z.

359. Transparency International. (September 6, 2019). *Three ways to stop money laundering through real estate.* Retrieved October 24, 2023 from Transparency International: https://www.transparency.org/en/news/three-ways-to-stop-money-laundering-through-real-estate.
360. Transparency International Deutschland e.V. (Publikationen). (n.d.). *Publikationen: Geldwäschebekämpfung in Deutschland – Probleme, Lösungsvorschläge und Beispielfälle*. Retrieved October 24, 2023 from Transparency International Deutschland: https://www.transparency.de/publikationen/detail/article/geldwaeschebekaempfung-in-deutschland-probleme-loesungsvorschlaege-und-beispielfaelle-1.
361. Transparency International Deutschland e.V. (Who we are). (n.d.). *Who we are*. Retrieved October 24, 2023 from Transparency International Deutschland: https://www.transparency.de/en.
362. Transparency International Deutschland e.V. (December 2018). *Geldwäsche bei Immobilien in Deutschland - Umfang des Problems und Reformbedarf.* Retrieved October 24, 2023 from Transparency International Deutschland: https://www.transparency.de/fileadmin/Redaktion/Publikationen/2019/Studie_Geldwa__sche_web.pdf.
363. Transparency International Deutschland e.V. (July 2021). *Geldwäschebekämpfung in Deutschland - Probleme, Lösungsvorschläge und Beispielfälle.* Retrieved October 24, 2023 from Transparency International Deutschland: https://www.transparency.de/fileadmin/Redaktion/Publikationen/2021/Studie_Geldwa__sche-in-Deutschland_210826.pdf.
364. Transparency International Deutschland e.V. (August 25, 2022). *Neuer Bericht zur Geldwäschebekämpfung: FATF kritisiert mangelnde politische Priorisierung.* Retrieved October 24, 2023 from Transparency International Deutschland: https://www.transparency.de/aktuelles/detail/article/neuer-bericht-zur-geldwaeschebekaempfung-fatf-kritisiert-mangelnde-politische-priorisierung/.
365. Treaty on the Functioning of the European Union (Document 12012E/TXT). (October 26, 2012). *European Union.* Retrieved October 24, 2023 from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.
366. Trinchera, T. (January 27, 2020). Confiscation And Asset Recovery: Better Tools To Fight Bribery And Corruption Crime. *Criminal Law Forum, 31*(1), pp. 49–79. Retrieved October 24, 2023 from Springer Nature: https://doi.org/10.1007/s10609-020-09382-1.
367. Unger, B. (2011). Money laundering regulation: from Al Capone to Al Qaeda. In D. Levi-Faur, *Handbook on the politics of regulation* (pp. 615-628). Cheltenham: Edward Elgar Publishing.
368. Unger, B., Addink, H., Walker, J., Ferwerda, J., Van Den Broek, M. & Deleanu, I. (February 2013). *Project 'ECOLEF' - The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy.* Retrieved October 24, 2023 from Utrecht University: http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf.
369. United Nations (Protocol against the Smuggling of Migrants). (November 15, 2000). *Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/documents/middleeastandnorthafrica/smuggling-migrants/SoM_Protocol_English.pdf.
370. United Nations (Protocol to Prevent, Suppress and Punish Trafficking in Persons). (November 15, 2000). *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/documents/treaties/Special/2000_Protocol_to_Prevent_2C_Suppress_and_Punish_Trafficking_in_Persons.pdf.
371. United Nations Commission on International Trade Law. (September 2013). *Recognizing and Preventing Commercial Fraud - Indicators of Commercial Fraud Prepared by the*

UNCITRAL Secretariat. Retrieved October 24, 2023 from UNCITRAL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/recognizing-and-preventing-commercial-fraud-e.pdf.

372. United Nations Convention against Corruption. (October 31, 2003). *United Nations.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/documents/brussels/UN_Convention_Against_Corruption.pdf.
373. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention). (December 20, 1988). *United Nations.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/pdf/convention_1988_en.pdf.
374. United Nations Convention against Transnational Organized Crime (Palermo Convention). (November 15, 2000). *United Nations.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf.
375. United Nations Office of Counter-Terrorism (Compact). (n.d.). *UN Global Counter-Terrorism Coordination Compact.* Retrieved October 24, 2023 from UN: https://www.un.org/counterterrorism/global-ct-compact.
376. United Nations Office of Counter-Terrorism (Legal Instruments). (n.d.). *International Legal Instruments.* Retrieved October 24, 2023 from UN: https://www.un.org/counterterrorism/international-legal-instruments.
377. United Nations Office of Counter-Terrorism (What we do). (n.d.). *What we do.* Retrieved October 24, 2023 from UN: https://www.un.org/counterterrorism/what-we-do.
378. United Nations Office on Drugs and Crime (About). (n.d.). *About the United Nations Office on Drugs and Crime.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/unodc/en/about-unodc/index.html.
379. United Nations Office on Drugs and Crime (COVID-19 Pandemic). (n.d.). *Impact of the COVID-19 Pandemic on Trafficking in Persons.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf.
380. United Nations Office on Drugs and Crime (GPML). (n.d.). *Global Programme against Money Laundering.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/unodc/en/money-laundering/global-programme-against-money-laundering/.html.
381. United Nations Office on Drugs and Crime (Overview). (n.d.). *Money-laundering Overview.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/unodc/en/money-laundering/overview.html.
382. United Nations Office on Drugs and Crime (Palermo Convention). (n.d.). *United Nations Convention against Transnational Organized Crime and the Protocols Thereto.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
383. United Nations Office on Drugs and Crime (TPB). (n.d.). *Terrorism Prevention Branch.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/unodc/en/terrorism/index.html.
384. United Nations Office on Drugs and Crime (Transnational organized crime threat assessments). (n.d.). *Transnational organized crime threat assessments.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/unodc/data-and-analysis/TOC-threat-assessments.html.
385. United Nations Office on Drugs and Crime (Transnational organized crime). (n.d.). *Transnational organized crime: the globalized illegal economy.* Retrieved October 24, 2023 from UNODC: https://www.unodc.org/toc/en/crimes/organized-crime.html.
386. United Nations Secretary-General. (April 9, 2020). *Secretary-General's remarks to the Security Council on the COVID-19 Pandemic.* Retrieved October 24, 2023 from UN: https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered.

387. United Nations Security Council (Current Members). (n.d.). *Current Members.* Retrieved October 24, 2023 from UN: https://www.un.org/securitycouncil/content/current-members.
388. United Nations Security Council (Security Council). (n.d.). *What is the Security Council?* Retrieved October 24, 2023 from UN: https://www.un.org/securitycouncil/content/what-security-council.
389. United States Department of Justice (Agencies). (n.d.). *Agencies.* Retrieved October 24, 2023 from U.S. Department of Justice: https://www.justice.gov/agencies/chart/grid.
390. United States Department of Justice (MLARS). (n.d.). *Money Laundering and Asset Recovery Section (MLARS).* Retrieved October 24, 2023 from U.S. Department of Justice: https://www.justice.gov/criminal-mlars.
391. United States Department of Justice (Our Work). (n.d.). *Our Work.* Retrieved October 24, 2023 from U.S. Department of Justice: https://www.justice.gov/our-work.
392. United States Department of Justice. (March 19, 2021). *Iranian Nationals Charged with Conspiring to Evade U.S. Sanctions on Iran by Disguising $300 Million in Transactions Over Two Decades.* Retrieved October 24, 2023 from U.S. Department of Justice: https://www.justice.gov/opa/pr/iranian-nationals-charged-conspiring-evade-us-sanctions-iran-disguising-300-million.
393. United States Department of State. (February 27, 2023). *Country Reports on Terrorism 2021.* Retrieved October 24, 2023 from U.S. Department of State: https://www.state.gov/wp-content/uploads/2023/02/Country_Reports_2021_Complete_MASTER.no_maps-011323-Accessible.pdf.
394. United States Department of the Treasury (COVID-19 Scams). (n.d.). *COVID-19 Scams.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams.
395. United States Department of the Treasury (ML Risk Assessment). (February 2022). *National Money Laundering Risk Assessment.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf.
396. United States Department of the Treasury (OFAC). (n.d.). *Office of Foreign Assets Control - Sanctions Programs and Information.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.
397. United States Department of the Treasury (Role of the Treasury). (n.d.). *Role of the Treasury.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/about/general-information/role-of-the-treasury.
398. United States Department of the Treasury (Terrorism and Financial Intelligence). (n.d.). *Terrorism and Financial Intelligence.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/about/offices/terrorism-and-financial-intelligence.
399. United States Department of the Treasury (TF Risk Assessment). (March 1, 2022). *2022 National Terrorist Financing Risk Assessment.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/system/files/136/2022-National-Terrorist-Financing-Risk-Assessment.pdf.
400. United States Department of the Treasury (TFTP). (n.d.). *Terrorist Finance Tracking Program (TFTP).* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp.
401. United States Department of the Treasury. (2015). *National Terrorist Financing Risk Assessment.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/system/files/246/National-Terrorist-Financing-Risk-Assessment-06-12-2015.pdf.
402. United States Department of the Treasury. (April 9, 2020). *Treasury Underscores Commitment to Global Flow of Humanitarian Aid in Face of COVID-19 Pandemic.* Retrieved October 24, 2023 from U.S. Department of the Treasury: https://home.treasury.gov/news/press-releases/sm969.

403. United States Government Accountability Office. (April 2020). *Report to Congressional Requesters - Trade-Based Money Laundering.* Retrieved October 24, 2023 from GAO: https://www.gao.gov/assets/gao-20-333.pdf.
404. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. (October 26, 2001). *United States of America.* Retrieved October 24, 2023 from U.S. Government Publishing Office: https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.
405. Usman Kemal, M. (October 2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control, 17*(4), pp. 416-427. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-06-2013-2022.
406. Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung – KryptoWTransferV). (May 22, 2023). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/kryptowtransferv_2023/BJNR0870A0023.html.
407. Verordnung zu den nach dem Geldwäschegesetz meldepflichtigen Sachverhalten im Immobilienbereich (Geldwäschegesetzmeldepflichtverordnung-Immobilien – GwGMeldV-Immobilien). (August 20, 2020). *Bundesministerium der Justiz/Bundesamt für Justiz.* Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/imgwgmeldv/BJNR196500020.html.
408. Vogel, B. (EU Anti-Money Laundering). (2020). Reinventing EU Anti-Money Laundering - Towards a Holistic Legal Framework. In B. Vogel & J.-B. Maillart, *National and International Anti-Money Laundering Law - Developing the Architecture of Criminal Justice, Regulation and Data Protection* (pp. 883-1027). Cambridge/Antwerp/Chicago: Intersentia.
409. Vogel, B. (Reform des Geldwäscheparagraphen). (August 24, 2020). *Warum die Reform des Geldwäscheparagraphen ihr Ziel verfehlt.* Retrieved October 24, 2023 from Verfassungsblog: https://verfassungsblog.de/warum-die-reform-des-geldwaescheparagraphen-ihr-ziel-verfehlt/.
410. Ward, C. A. (October 2003). Building Capacity to Combat International Terrorism: The Role of the United Nations Security Council. *Journal of Conflict & Security Law, 8*(2), pp. 289-305. Retrieved October 24, 2023 from Oxford University Press: http://www.jstor.org/stable/26294277.
411. Werner, G. (1996). *Bekämpfung der Geldwäsche in der Kreditwirtschaft.* Freiburg im Breisgau: Edition iuscrim, Max-Planck-Institut für Ausländisches und Internationales Strafrecht.
412. Wolfsberg Group. (n.d.). *Wolfsberg Principles.* Retrieved October 24, 2023 from Wolfsberg Group: https://www.wolfsberg-principles.com.
413. World Bank (Financial Integrity). (n.d.). *Financial Integrity.* Retrieved October 24, 2023 from World Bank: https://www.worldbank.org/en/topic/financialmarketintegrity.
414. World Bank (Who we are). (n.d.). *Who we are.* Retrieved October 24, 2023 from World Bank: https://www.worldbank.org/en/who-we-are.
415. World Bank. (2015). *Disclaimer and Terms of Use: National Money Laundering and Terrorist Financing Risk Assessment Toolkit.* Retrieved October 24, 2023 from World Bank: https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use.
416. Yeoh, P. (January 15, 2020). Banks' vulnerabilities to money laundering activities. *Journal of Money Laundering Control, 23*(1), pp. 122-135. Retrieved October 24, 2023 from Emerald Publishing: https://doi.org/10.1108/JMLC-05-2019-0040.
417. Zdanowicz, J. S. (December 31, 2009). Trade-Based Money Laundering and Terrorist Financing. *Review of Law & Economics, 5*(2), pp. 855-878. Retrieved October 24, 2023 from De Gruyter: https://doi.org/10.2202/1555-5879.1419.
418. Zoll (AFCA). (n.d.). *Pressemitteilung zur Gründung der AFCA.* Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Anti-Financial-Crime-Alliance/pm_bargeld_2019_z90.html?faqCalledDoc=348658.
419. Zoll (FIU). (n.d.). *Financial Intelligence Unit (Historie, rechtliche Grundlagen etc.).* Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Fragen-Antworten/fragen-antworten_node.html;jsessionid=B221A5C7F29B0AD55677718D24B2C6BB.internet732.

420. Zoll (Jahresberichte). (n.d.). *Jahresberichte der FIU*. Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Fachliche-Informationen/Jahresberichte/jahresberichte_node.html.
421. Zoll (Public Private Partnership). (n.d.). *Public Private Partnership - Anti Financial Crime Alliance*. Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Anti-Financial-Crime-Alliance/anti-financia-crime-alliance_node.html.
422. Zoll. (December 3, 2020). *Prävention und Bekämpfung von Geldwäsche und Terrorismusfinanzierung in der Praxis*. Retrieved October 24, 2023 from Zoll: https://www.zoll.de/DE/FIU/Aktuelles-FIU-Meldungen/2020/fiu_praevention_bekaempfung_geldwaesche_terrorismusbekaempfung_praxis.html.
423. Zollverwaltungsgesetz (ZollVG). (July 5, 2021). *Bundesministerium der Justiz/Bundesamt für Justiz*. Retrieved October 24, 2023 from Gesetze im Internet: https://www.gesetze-im-internet.de/zollvg/BJNR121250992.html.
424. Zweites Gesetz zur effektiveren Durchsetzung von Sanktionen (Sanktionsdurchsetzungsgesetz II). (December 27, 2022). *Bundestag*. Retrieved October 24, 2023 from Bundesfinanzministerium: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_IV/20_Legislaturperiode/2022-12-27-SanktionsdurchsetzungsG-II/4-Verkuendetes-Gesetz.pdf?__blob=publicationFile&v=4.