Federal Ministry
of Finance

First National Risk Assessment

2018/2019

First National Risk Assessment

Anti-Money Laundering/ Countering the Financing of Terrorism

2018/2019

This working translation of the
Erste Nationale Risikoanalyse – Bekämpfung von Geldwäsche und Terrorismusfinanzierung
is provided by the Language Service of the Federal Ministry of Finance.
Only the German text is authoritative.

Summary

The purpose of the National Risk Assessment is to sharpen risk consciousness in Germany in the area of anti-money laundering/countering the financing of terrorism (AML/CFT). Under section 5 (1) sentence 2 of the Act on the detection of proceeds from serious crimes (*Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten – Geldwäschegesetz*; henceforth referred to as the Money Laundering Act), obliged entities under the Money Laundering Act must take the findings of this National Risk Assessment into account when compiling their own risk analysis, hence the Assessment has an impact on obliged entities' risk analyses.

In light of Germany's high economic attractiveness and the high cash intensity and diversity of the economy, the money laundering threat for Germany is rated as medium-high.[1] The threat potential is amplified by the availability of options for conducting transactions anonymously. To prevent money laundering, it is therefore especially important that obliged entities under the Money Laundering Act adequately fulfil due diligence requirements, in particular counterparty identification.

On the basis of the methodology underlying this NRA, the threat of terrorist organisations engaging in financing activities in Germany has been rated as medium-high. Here it should be noted that, as a rule, terrorist organisations need most of their financial resources for establishing and maintaining organisational structures (such as for organisational logistics, propaganda and living expenses). In contrast, only small amounts are needed, in many cases, to carry out actual terrorist acts. Fundraising can involve both illegal and legal sources. In some cases, foreign terrorist groups use their diaspora or sympathisers living in Germany to generate donations in order to fund their structures and activities.

Because the German economy is deeply interconnected at the global level, certain cross-border situations are, fundamentally, inherently high-risk. In order to respond to the attendant challenges appropriately, business enterprises must address such risk with regard to ML/TF by using internal control processes as part of their risk management.

Heightened susceptibility, notably for terrorist financing, has been identified for money or value transfer services (primarily in the case of cash transactions with an international dimension and payments outside of an existing business relationship). The high cash intensity of money or value transfer services is considered a notable risk driver. It is prohibited in Germany to operate a money or value transfer service without a licence from BaFin (as takes place, for example, with hawala banking).

A high money laundering risk has been identified in the real estate sector. Effective anonymity can be achieved with the aid of share deals and interlocking sharehold-ings (especially those involving foreign shell companies). Credit institutions, lawyers, auditors, tax advisers and notaries who are involved in or advise on the structuring of such transactions should exercise particular vigilance.

1 On a scale of high, medium-high, medium, medium-low and low.

Abbreviations

ADS	Antidiskriminierungsstelle des Bundes (Federal Anti-Discrimination Agency)
AG	*Aktiengesellschaft* (German public limited company)
AIF	Alternative investment fund
AML	Anti-money laundering
AML/CFT	Anti-money laundering/countering the financing of terrorism
AO	*Abgabenordnung* (German Fiscal Code)
APAS	Abschlussprüferaufsichtsstelle (Auditor Oversight Commission)
AWG	*Außenwirtschaftsgesetz* (Foreign Trade and Payments Act)
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Federal Financial Supervisory Authority)
BAMAD	Bundesamt für den Militärischen Abschirmdienst (Federal Armed Forces Counterintelligence Office)
BAMF	Bundesamt für Migration und Flüchtlinge (Federal Office for Migration and Refugees)
BeurkG	*Beurkundungsgesetz* (Certification Act)
BfV	Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
BGBl.	*Bundesgesetzblatt* (Federal Law Gazette)
BKA	Bundeskriminalamt (Federal Criminal Police Office)
BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend (Federal Ministry of Family Affairs, Senior Citizens, Women and Youth)
BMI	Bundesministerium des Innern, für Bau und Heimat (Federal Ministry of the Interior, Building and Community)
BMJV	Bundesministerium der Justiz und für Verbraucherschutz (Federal Ministry of Justice and Consumer Protection)
BMWi	Bundesministerium für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy)
BND	Bundesnachrichtendienst (Federal Intelligence Service)
BPB	Bundeszentrale für politische Bildung (Federal Agency for Civic Education)
BT	German Bundestag
CFT	Countering the financing of terrorism
DNFBP	Designated non-financial businesses and professions
e. V.	eingetragener Verein (registered association)
EIO	European investigation order
EJN	European Judicial Network
ESA	European Supervisory Authorities
etc.	et cetera
EU	European Union
FamFG	*Familienverfahrensgesetz* (Act on Proceedings in Family Matters)
FATF	Financial Action Task Force
FIU	Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit)
FlugDaG	*Flugdatengesetz* (Passenger Name Record Act)
GbR	*Gesellschaft bürgerlichen Rechts* (civil-law partnership)
GenG	*Genossenschaftsgesetz* (Cooperatives Act)
GenRegV	*Genossenschaftsregisterverordnung* (Ordinance on the Register of Cooperative Societies)
GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum (Joint Centre for Combating Extremism and Terrorism)

GewO	Gewerbeordnung (Trade Regulation Code)
GFG	Gemeinsame Finanzermittlungsgruppen (Joint Financial Investigation Groups)
GmbH	*Gesellschaft mit beschränkter Haftung* (German private limited company)
goAML	Financial Intelligence Unit reporting portal
GTAZ	Gemeinsames Terrorismusabwehrzentrum (Joint Counter-Terrorism Centre)
GVG	*Gerichtsverfassungsgesetz* (Courts Constitution Act)
GwG	Act on the detection of proceeds from serious crimes; here: Money Laundering Act (*Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten – Geldwäschegesetz*)
HGB	Handelsgesetzbuch (Commercial Code)
HRV	Handelsregisterverordnung (Commercial Register Ordinance)
IS	So-called "Islamic State"
IT	Information technology
JIT	Joint Investigation Team
KAGB	*Kapitalanlagegesetzbuch* (Investment Code)
KAPrüfbV	*Kapitalanlage-Prüfungsberichte-Verordnung* (Audit Reports Ordinance Concerning Certain Investment Undertakings)
KrWaffKontrG	*Kriegswaffenkontrollgesetz* (War Weapons Control Act)
KWG	*Kreditwesengesetz* (Banking Act)
LfV	Landesamt für Verfassungsschutz (State Office for the Protection of the Constitution)
LKA	Landeskriminalamt (State Criminal Police Office)
Ltd.	Limited
M&A	Mergers and acquisitions
ML	Money laundering
ML/TF	Money laundering/terrorist financing
No.	Number
NPO	Non-profit organisation
NPP	Nationales Präventionsprogramm gegen islamistischen Extremismus (National Prevention Programme against Islamic Extremism)
NRA	National Risk Assessment
NRW	North Rhine-Westphalia
NSU	So-called "National Socialist Underground"
OC	Organised crime
OECD	Organisation for Economic Co-operation and Development
OLG	Oberlandesgericht (higher regional court)
P.	Page
PartGG	*Partnerschaftsgesellschaftsgesetz* (Partnership Company Act)
PEPs	Politically exposed persons
PIU	Passenger Information Unit
PKS	Polizeiliche Kriminalstatistik (Police Crime Statistics)
PNR	Passenger name record
PrüfbV	*Prüfungsberichtsverordnung* (Audit Report Ordinance)
PrüfV	*Prüfungsberichteverordnung* (Audit Reports Ordinance)
StGB	*Strafgesetzbuch* (Criminal Code)
StPO	*Strafprozessordnung* (Code of Criminal Procedure)
STR	Suspicious transaction report
TF	Terrorist financing

UCC	Union Customs Code
UStG	*Umsatzsteuergesetz* (Value Added Tax Act)
VAG	*Versicherungsaufsichtsgesetz* (Insurance Supervision Act)
VAT	Value added tax
ZAG	*Gesetz über die Beaufsichtigung von Zahlungsdiensten* (Payment Services Supervision Act)
ZahlPrüfbV	*Zahlungsinstituts-Prüfungsberichtsverordnung* (Audit Report Ordinance Concerning Payment Institutions)
ZKA	Zollkriminalamt (Customs Criminological Office)
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister (Central Register of Proceedings conducted by Public Prosecution Offices)

Contents

1 National Risk Assessment structure and processes

1 National Risk Assessment structure and processes

1.1 Legal basis

Under the stipulations of the Financial Action Task Force (FATF) and the Fourth EU Money Laundering Directive, Germany is required to conduct a National Risk Assessment (NRA) on anti-money laundering/countering the financing of terrorism (AML/CFT) at regular intervals. This is a core element of the risk-based approach under the Fourth EU Money Laundering Directive. Its purpose is to direct resources in the best possible manner towards problem areas in AML/CFT and thus effectively mitigate money laundering/terrorist financing (ML/TF) risks. Under section 5 (1) sentence 2 of the Money Laundering Act (*Geldwäschegesetz*), obliged entities under the Money Laundering Act must take the findings of this National Risk Assessment into account when compiling their own risk analysis in the future. The Assessment can thus be expected to have an impact on obliged entities' risk analyses.

1.2 Organisation of the National Risk Assessment process in Germany

The Federal Government's first National Risk Assessment was launched in December 2017 with the Federal Ministry of Finance as lead agency and with the participation of 35 federal and *Länder* agencies (see section 1.3). In regular meetings, four working groups analysed and assessed both money laundering and terrorist financing risks for Germany. The active cooperation of the intelligence services was especially important with regard to terrorist financing. In this connection, the individual terrorist organisations active in Germany were also subjected to individual assessment. This was subsequently combined into an aggregate assessment that is presented in the National Risk Assessment.

The operational work in the working groups took place over a period of 14 months. The supranational risk assessment by the European Commission was taken into account in the course of the National Risk Assessment and used to evaluate the various findings. This National Risk Assessment also incorporates information from numerous pre-existing sector-specific risk assessments. The sector-specific risk assessments are generally highly detailed.

The purpose of the National Risk Assessment is to conduct a realistic strength-weakness analysis in the area of AML/CFT in Germany and to identify, map out and effectively mitigate existing and future risks. The Federal Government will analyse the need for changes in order to make Germany more robust in terms of AML/CFT overall.

The starting point for Germany's National Risk Assessment was a methodology for conducting national risk assessments developed by the World Bank, referred to as the World Bank Tool[2]. The Federal Government adapted and updated this methodology to Germany's specific requirements. It was adapted to conditions in Germany and, among other things, greater use was made of qualitative information sources. The analysis of the threat situation relied particularly heavily on qualitative information from German agencies. Further focal areas included blockchain technology and the use of crypto assets, the analysis of legal persons and legal arrangements and analysis of terrorist financing risk. The methodology used required the

2 World Bank Group, National Risk Assessment Tool.

identification, analysis and assessment of the main ML/TF risks for Germany. The assessment covered both the prevailing threat situation and Germany's vulnerability, as well as the resulting consequences.

Assessment of risk in this Assessment is consistent with the requirements of the risk-based approach under FATF Recommendation 1. ML/TF risk therefore consists in this assessment of the threat potential for and Germany's vulnerability to each of the two forms of risk.

Figure 1: Determination of risk in Germany's National Risk Assessment: Analysis of threat and vulnerability.

A threat is defined as an activity that has a certain potential to cause or possibility of causing harm in connection with relevant forms of crime or the financing of terrorist activities. Vulnerability is understood in this Assessment to mean gaps or unclarities in the prevailing defence mechanism for the prevention and combating of money laundering and terrorist financing. A potential threat or vulnerability can exist both at national and at sectoral level. This National Risk Assessment has analysed the threat and vulnerability situation with regard to money laundering and terrorist financing at both national and sectoral level.

The Federal Government organised the work on this National Risk Assessment in four working groups composed of experts from a total of 35 federal and *Länder* agencies, as follows:

- A: Money Laundering – National Threat Situation/National Vulnerability
- B: Money Laundering in the Financial Sector
- C: Money Laundering in the DNFBP Sector
- D: Terrorist Financing

Alongside knowledge contributed by the competent supervisory authorities, the expertise of the law enforcement agencies involved, of the intelligence services and of the Financial Intelligence Unit were highly important to the outcomes of this National Risk Assessment. The findings of this Assessment are based on discussions among the federal and *Länder* experts involved, on statistical and scientific analyses and on consultation with the private sector and civil society. Gaining an overall picture of the various data in order to generate meaningful results was very important to the success of the National Risk Assessment.

1.3 Agencies involved

The National Risk Assessment on Anti-Money Laundering/Countering the Financing of Terrorism was a cross-departmental task in which the Federal Ministry of Finance was the lead agency. The following federal and *Länder* agencies regularly took part in the four working groups:

Federal Government:

- Bundeskanzleramt (Federal Chancellery)
- Bundesministerium der Finanzen (Federal Ministry of Finance)
- Auswärtiges Amt (Federal Foreign Office)
- Bundesministerium des Innern, für Bau und Heimat (Federal Ministry of the Interior, Building and Community)
- Bundesministerium der Justiz und für Verbraucherschutz (Federal Ministry of Justice and Consumer Protection)
- Bundesministerium für Wirtschaft und Energie (Federal Ministry for Economic Affairs and Energy)

Police authorities:

- Bundeskriminalamt (Federal Criminal Police Office)
- Zollkriminalamt (Customs Criminological Office) (see also Generalzolldirektion below)
- Bayerisches Landeskriminalamt (Bavarian State Criminal Police Office)
- Landeskriminalamt Berlin (Berlin State Criminal Police Office)
- Landeskriminalamt Brandenburg (Brandenburg State Criminal Police Office)
- Landeskriminalamt Nordrhein-Westfalen (North Rhine-Westphalia State Criminal Police Office)
- Landeskriminalamt Rheinland-Pfalz (Rhineland-Palatinate State Criminal Police Office)
- Landeskriminalamt Sachsen (Saxony State Criminal Police Office)
- Landeskriminalamt Thüringen (Thuringia State Criminal Police Office)

The involvement of the Federal Criminal Police Office related both to organised crime and to national security. The Bavaria, Berlin, North Rhine-Westphalia, Rhineland-Palatinate and Saxony State Criminal Police Offices contributed with regard to organised crime and money laundering investigations. The Berlin, Brandenburg and Thuringia State Criminal Police Offices were also involved in the National Risk Assessment with regard to state security.

Judiciary:

- Generalbundesanwalt beim Bundesgerichtshof (Federal Public Prosecutor General at the Federal Court of Justice)
- Generalstaatsanwaltschaft Celle (Celle Prosecutor General's Office)
- Generalstaatsanwaltschaft Frankfurt am Main (Frankfurt am Main Prosecutor General's Office)
- Generalstaatsanwaltschaft Stuttgart (Stuttgart Prosecutor General's Office)

The Federal Public Prosecutor General at the Federal Court of Justice and the Stuttgart Prosecutor General's Office – the current leading representative of the prosecutors general's offices' working group on extremism – were involved in the National Risk Assessment with regard to terrorist financing. The prosecutors general's offices involved with regard to money laundering were the Frankfurt am Main Prosecutor General's Office (primarily the financial sector) and the Celle Prosecutor General's Office (primarily the designated non-financial businesses and professions (DNFBP) sector).

Intelligence services:

- Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution)
- Bundesnachrichtendienst (Federal Intelligence Service)

Generalzolldirektion (Central Customs Authority):

- Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit)
- Zollkriminalamt (Customs Criminological Office)

With regard to specific thematic areas, other directorates of the Central Customs Authority were also involved in the meetings of the relevant working groups according to their competencies.

Supervisory authorities (financial sector):

- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin, Federal Financial Supervisory Authority)

Supervisory authorities (DNFBP sector):

- Staatsministerium des Innern, für Sport und für Integration, Bayern (Ministry of the Interior, Sport and Integration, Bavaria)
- Behörde für Wirtschaft, Verkehr und Innovation, Hamburg (Ministry for Economic Affairs, Transport and Innovation, Hamburg)
- Ministerium des Innern und für Sport, Hessen (Ministry of the Interior and Sports, Hesse)
- Ministerium für Wirtschaft und Energie, Brandenburg (Ministry for Economic Affairs and Energy, Brandenburg
- Senatsverwaltung für Wirtschaft, Energie und Betriebe, Berlin (Senate Department for Economics, Energy and Public Enterprises, Berlin)
- Bezirksregierung Arnsberg (Arnsberg regional government)
- Regierung von Mittelfranken (Middle Franconia regional government)
- Bezirksregierung Münster (Münster regional government)
- Regierung von Niederbayern (Lower Bavaria regional government)
- Regierungspräsidium Darmstadt (Darmstadt district council)
- Regierungspräsidium Freiburg (Freiburg district council)

Central bank:

- Deutsche Bundesbank

In addition to subject-matter expertise, the selection of the *Länder* agencies involved was intended to ensure that the expert groups reflected Germany's diversity. To this end, agencies from city states (Berlin and Hamburg) were involved in the National Risk Assessment as well as agencies from large-area states representing all regions of the country (Baden-Württemberg, Bavaria, Brandenburg, Hesse, Lower Saxony, North Rhine-Westphalia, Rhineland-Palatinate, Saxony and Thuringia). The Federal Ministry of Defence and the Federal Armed Forces Counterintelligence Office were involved with regard to the thematic area of terrorist financing.

With regard to specific thematic areas relating to the DNFBP sector, other supervisory authorities were also involved in the meetings of the relevant working groups according to their work areas. Experts from the Federal Chamber of Civil Law Notaries and from Nuremberg Higher Regional Court were involved in the analysis of anti-money laundering supervision for notaries. Nuremberg Higher Regional Court serves as the coordinating body for the supervision of notaries in North Bavaria, which is performed by the presidents of the respective regional courts, and was therefore selected by way of example. The following bodies were involved as experts in AML supervision for risk assessment with regard to other liberal professions:

Notaries:

- Bundesnotarkammer (Federal Chamber of Civil Law Notaries)
- Oberlandesgericht Nürnberg (Nuremberg Higher Regional Court)

Auditors:

- Auditor Oversight Commission (APAS)
- Wirtschaftsprüferkammer (Chamber of Public Auditors)

Tax advisers:

- Bundessteuerberaterkammer (Federal Chamber of Tax Advisers)
- Steuerberaterkammer Berlin (Berlin Chamber of Tax Advisers)
- Steuerberaterkammer München (Munich Chamber of Tax Advisers)
- Steuerberaterkammer Nürnberg (Nuremberg Chamber of Tax Advisers)
- Steuerberaterkammer Saarland (Saarland Chamber of Tax Advisers)

Lawyers and legal advisers:

- Bundesrechtsanwaltskammer (German Federal Bar)
- Kammergericht Berlin (Berlin Higher Regional Court)
- Rechtsanwaltskammer Berlin (Berlin Bar Association)
- Rechtsanwaltskammer Düsseldorf (Düsseldorf Bar Association)
- Rechtsanwaltskammer Hamburg (Hamburg Bar Association)
- Rechtsanwaltskammer München (Munich Bar Association)

The following agencies were involved in the working group's risk assessment with regard to AML supervision in the gambling sector:

- Ministerium des Innern und für Kommunales, Brandenburg (Ministry of the Interior and Local Affairs, Brandenburg)
- Ministerium für Inneres und Europa, Mecklenburg-Vorpommern (Ministry of the Interior and Europe, Mecklenburg-Western Pomerania)
- Ministerium für Inneres und Sport, Niedersachsen (Ministry of the Interior and Sport, Lower Saxony)
- Regierungspräsidium Darmstadt (Darmstadt district council) (gambling supervision)
- Senatsverwaltung für Inneres und Sport, Berlin (Senate Department for the Interior and Sports, Berlin)
- Staatsministerium des Innern, Sachsen (Ministry of the Interior, Saxony)
- Behörde für Inneres und Sport, Hamburg (Ministry for the Interior and Sport, Hamburg)

Alongside subject-matter expertise, the selection of *Länder* agencies in this thematic area was designed to ensure the broadest possible regional coverage across Germany.

1.4 Private sector consultation

Consultation of the private sector constituted a very important source of information for the National Risk Assessment. Both industry associations and individual entities were selected for this purpose to represent the financial sector (see Annex 1), while the DNFBP sector was represented by the various industry associations for obliged entities (see Annex 2).

For both the financial and the DNFBP sector, products and services and sales channels[3] in each industry were examined in detail and an ML/TF risk assessment was performed with the help of questionnaires. Various entities and industry associations were selected in consultation with the agencies involved in the National Risk Assessment. For the financial sector, this selection was made primarily in consultation with BaFin.

Participants were selected with a view to identifying and presenting risks for the market as a whole. No account was given here to entities' individual risks. With regard to the financial sector, the selection of participants was intended to provide the best possible sample of the German financial landscape. Entities were selected according to the following criteria:

- Overall group having large market share of the sector concerned
- Range of entity sizes
- Range of business models
- Range of sales channels
- Customer structure
- Product structure
- Location.

Involving financial sector industry associations made it possible to gain a more abstract perspective on the entire financial sector and to better contextualise the responses of the individual entities in each group. Involvement of auditors and industry association audit bodies completed the overall picture of the financial sector. The auditors involved carry out audits in the financial sector throughout Germany and consequently have a very good overview of the entire financial sector and its risks.

Also with regard to the financial sector, eight expert consultations were held with representatives of entities and industry associations (with a separate expert consultation held at the Federal Ministry of Finance for each sectoral group). The representatives of public agencies in the Financial Sector working group also took part in these consultations alongside the representatives of the selected entities and industry associations. The consultations were based on the questionnaire evaluated by BaFin. The outcomes of these expert consultations were used to plausibility-check the risk assessments by the Financial Sector NRA working group and to undertake 'deep dives' into specific thematic areas. Each of the consultations provided sufficient time and opportunity for the discussion of various issues. Many of the questions and suggestions put forward by the private sector with regard to the Money Laundering Act in these consultations are to be incorporated in a planned special section on the banking sector in the interpretation and application guidance under section 51 (8) of the Money Laundering Act. The findings from the questionnaires and the subsequent expert consultations were included in the final assessment by the Financial Sector working group at its final meeting and completed its work product. The DNFBP Sector working group likewise used the findings from the questionnaire to plausibility-check its results. Overall, it emerged that the financial sector provided significantly more detailed responses and can be assumed to have greater experience with regard to ML/TF risks than the DNFBP sector.

3 The assessment covers products, services and sales channels. For the sake of simplicity, the word 'products' is exclusively used from now onwards. This includes products, services and sales channels.

1.5 Academic involvement

The Federal Ministry of Finance, as the lead agency, has attached great importance to research findings being incorporated into the National Risk Assessment. This ensures that the National Risk Assessment addresses and analyses new threat scenarios at the leading edge of developments. For this purpose, recent research findings on assessing ML/TF risks were used. With regard to crypto assets, the working group concerned questioned Professor Philipp Sandner of the Frankfurt School of Finance Blockchain Center as an expert on the subject and incorporated his academic input into the risk assessment on this thematic area.

In advance of this National Risk Assessment, the Federal Ministry of Finance commissioned Professor Kai Bussmann of Martin Luther University Halle-Wittenberg with an academic study entitled "Dark figure study on the prevalence of money laundering in Germany and the risks of money laundering in individual economic sectors". The findings of this study, which was published in 2016, were used to assess money laundering risks as part of this National Risk Assessment.

Also as part of the National Risk Assessment, two law-in-action studies on money laundering and terrorist financing were initiated and commissioned by the Federal Ministry of Finance in its capacity as lead agency. Professor Kai Bussmann of Martin Luther University Halle-Wittenberg was commissioned in cooperation with Kienbaum Consultants International GmbH to study the subject matter and development of investigation proceedings on money laundering for the years 2014 to 2016. The study focused on investigation and criminal prosecution proceedings under section 261 of the Criminal Code (*Strafgesetzbuch*). As it was being carried out, however, the study revealed itself to have little information value regarding the current situation in anti-money laundering due to substantial changes to the law that were made after the period examined in the study. In particular, the reform of asset recovery provisions in criminal law and changes in the law with regard to suspicious transaction reporting constitute a paradigm shift in this regard.

Professor Frank Saliger of Ludwig Maximilian University of Munich, in collaboration with KPMG AG Wirtschaftsprüfungsgesellschaft, was commissioned with a parallel study on terrorist financing. This study focuses on the contents and development of investigation proceedings for terrorist financing in Germany between 2015 and 2017. For this purpose, samples of investigation and criminal prosecution proceedings in the area of terrorist financing under section 18 of the Foreign Trade and Payments Act and sections 89a, b and c and 129a and b of the Criminal Code are being analysed.

The goal for these analyses is to provide science-based information in the areas of terrorist financing and money laundering as regards the origins and development of various cases, typologies, structures, underlying criminal activities as well as the sectors that are most affected. For this purpose, the relevant National Risk Assessment working groups identified indicators against which the case files are evaluated. The findings of the two studies are expected to be available to the competent authorities from autumn 2019 in order to aid them in fulfilling their respective legal mandate.

Analysis of mass historical data against specified indicators plays a particularly important role in identifying risk scenarios and potential trends with regard to threats. To improve knowledge in the field of ML/TF in Germany, the Federal Government will therefore continue to make use of academic analyses of historical mass data and incorporate them in its ongoing AML/CFT risk assessment.

2 Legal framework for anti-money laundering/ countering the financing of terrorism in Germany

2 Legal framework for anti-money laundering/countering the financing of terrorism in Germany

2.1 Germany's involvement in international organisations

Germany is actively involved internationally in AML/CFT in a wide variety of ways. Under the framework of the United Nations, in the G7 and the G20, in the Council of Europe and the OECD, Germany is committed to the global prevention of money laundering and terrorist financing. Germany was also actively involved in the establishment of the FATF in 1989 and is thus a founding member. The FATF operates as an international standard setter in anti-money laundering, countering the financing of terrorism and countering proliferation financing. The German delegation is led by the Federal Ministry of Finance and consistently plays a leading role within the FATF. In this context, the Federal Government is committed to continue refining the FATF's standards and methodology in order to further improve AML/CFT.

The Federal Republic of Germany is also a founding member of the European Union (EU). On the basis of the European treaties, Germany transposes the EU money laundering directives into national law. In those directives, the EU implements the FATF recommendations. The Federal Government is consistently actively involved in EU-level negotiations and works in the process to harden the European Single Market against money laundering and terrorist financing. Prior to the First National Risk Assessment, Germany transposed the Fourth EU Money Laundering Directive into national law. The Money Laundering Act amended on that basis entered into force on 26 June 2017. The Directive amending the Fourth Money Laundering Directive was published in the EU Official Journal on 19 June 2018 and entered into force on 9 July 2018. There are various transposition deadlines but the period for transposition of most provisions is 18 months (meaning no later than 10 January 2020). The amending directive specifically addresses issues that have come into the focus of attention following the terrorist attacks in Paris and Brussels and the emergence of the so-called 'Panama Papers'. It is expected that Germany will transpose the amending directive into national law in the course of 2019 (see section 2.2). The EU directive on combating money laundering by criminal law will also be transposed by Germany into national law by 3 December 2020.

2.2 The Money Laundering Act

The prevention of money laundering was placed on a statutory basis in Germany with the enactment of the Money Laundering Act in 1993. The Money Laundering Act requires economic operators in Germany to actively cooperate in the prevention of money laundering and terrorist financing. Persons and entities required to cooperate are termed 'obliged entities' in section 2 of the Money Laundering Act. Under section 50 of the Money Laundering Act, supervision of its enforcement lies with the various competent supervisory authorities.

The stipulations on risk management, on due diligence requirements with regard to customer relationships and on suspicious transaction reporting consequently represent the three main pillars of the Money Laundering Act to ensure a functioning system of money laundering prevention

in Germany. A central role is played here by the risk-based approach, as not all entities need to take the same precautions against risk in order to protect themselves from money laundering and terrorist financing. The statutory requirements are therefore geared to the applicable risks.

Obliged entities must comply with the provisions of the Money Laundering Act without exception. The Money Laundering Act empowers the supervisory authorities to take measures and issue orders to ensure compliance with obligations under the Act. Under section 56 of the Money Laundering Act, fines of up to €100,000 can be imposed in the event of reckless or wilful infringements. In the event of serious, repeated or systematic infringements, the fine can be up to €5 million or up to 10% of annual turnover. There is also a reputation risk because the Money Laundering Act requires the supervisory authorities to publish final and conclusive measures and unappealable administrative fine decisions.

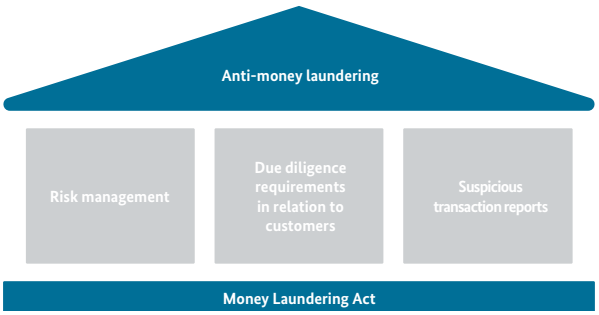

Figure 2: Three pillars of anti-money laundering in Germany.

Under section 51 (8) of the Money Laundering Act, the supervisory authorities regularly provide interpretation and application guidance for obliged entities. BaFin published interpretation and application guidance on the Money Laundering Act for obliged entities under its supervision in December 2018. In its interpretation and application guidance, BaFin presents its administrative practice on issues relating to the Money Laundering Act as amended on 23 June 2017. For compilation of its interpretation and application guidance, BaFin carried out a written and also an oral consultation. The guidance serves the purpose of ensuring that the customer due diligence requirements and internal safeguards are properly implemented and follows a risk-based approach. As part of the implementation guidance, BaFin also explains new features under the law, such as the concept of the notional beneficial owner. It also clarifies, among other things, the identification requirements for a person acting on behalf of a contracting party.

The competent *Länder* supervisory authorities published interpretation and application guidance for organisers and brokers of games of chance in spring 2019. This guidance issued by the *Länder* supreme gambling supervisory authorities under section 51 (8) of the Money Laundering Act is binding for obliged entities listed under section 2 (1) no. 15 of the Money Laundering Act. Publications by industry associations or individual obliged entities listed under section 2 (1) no. 15 of the Money Laundering Act are, where those publications depart from the guidance, immaterial for the purposes of supervisory assessment and are not binding.

The federal professional governing bodies of three liberal professions – lawyers, tax advisers and auditors – have compiled interpretation and application guidance in collaboration with the regional governing bodies and made that guidance available to obliged entities via the websites of the competent supervisory authorities. The federal governing bodies worked together on the substantive development of the interpretation and application guidance in order to ensure consistent interpretation of the law throughout Germany and across the professions.

The remaining supervisory authorities for the DNFBP sector have compiled joint, nationally uniform information sheets, among others for estate agents, traders in goods, insurance brokers, and have made them available to obliged entities. In addition to questions of legal implementation,

the information sheets also provide practical guidance on implementation questions. The uniform national information sheets also take into account the specific requirements of obliged entities in sectors with small-scale structures.

In the course of 2019, the Money Laundering Act will be revised in line with the requirements of the Directive amending the Fourth EU Money Laundering Directive. As already mentioned in section 2.1, the amending directive specifically addresses issues that have come into the focus of attention following the terrorist attacks in Paris and Brussels and the emergence of the so-called 'Panama Papers'. Key changes to German law as a result of the amending directive are as follows:

• Public access to the Transparency Register
Whereas access to the Transparency Register has so far been restricted to those with a "legitimate interest" (such as to journalists), data on beneficial owners will in future be generally accessible to the public ("anyone"). In addition, there are plans to connect up European transparency registers.

• Politically exposed persons (PEPs)
Transactions with PEPs are already subject to heightened due diligence requirements. Member States must now compile lists indicating the specific public functions qualifying a person as a PEP. The European Commission must likewise compile a list of functions at the level of EU institutions and bodies.

• Crypto assets
Providers exchanging crypto assets into and out of legal tender and custodian wallet providers will in future be obliged entities under the Money Laundering Act in Germany.

• High-risk third countries
The due diligence requirements and measures against high-risk third countries are to be harmonised on the basis of the amending directive.

2.3 The Criminal Code

2.3.1 The offence of money laundering

The offence of money laundering was created in 1992 to implement requirements under the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20 December 1988 (Vienna Convention), the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 8 November 1990 (European Council Convention) and Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. Additional impetus came from the FATF Recommendations of 2 July 1990.

Money laundering predicate offences comprise all offences listed in section 261 (1) sentence 2 of the Criminal Code. This is an exhaustive list of predicate offences that has been modified and added to on multiple occasions, notably in order take account of FATF recommendations. It must also be expanded again in order to transpose the EU Directive on combating money laundering by criminal law into national law. The reason for the list is that, when creating the offence of money laundering, the lawmakers made a conscious decision not to stipulate specific, subjective elements of the offence and instead limited themselves to objective, easily demonstrable criteria. In this connection, it was stated in explanatory memoranda that in view of the non-inclusion of subjective elements, extending the offence to all illegal acts would go "too far" ("*zu weit*", BT-Drucksache 12/989, p. 27; BT-Drucksache 13/8651, p. 12; also see in particular BT-Drucksache 12/6853, p. 27: [translation] "In order, on the other hand, to avoid a boundless extension of criminal liability on the basis of the broadly defined objective elements of the offence, it was decided for, the

purpose of balance, to restrict the list of predicate offences to felonies and severe misdemeanours").

Under section 261 (8), an offence committed abroad is also sufficient to qualify as a predicate offence if the offence is punishable where committed and it corresponds to one of the listed predicate offences, although it is not necessary for German criminal law to be applicable to the offence committed abroad. At the recommendation of FATF, the offence of money laundering has also included self-laundering since 2015.

The offence of money laundering covers not only money, but also extends to all property and rights that have value as assets. This includes movable and immovable property, receivables and intellectual property rights. The offence also covers expenditure saved by virtue of tax evasion committed on a commercial or organised basis.

Except as specifically stipulated in subsection (1) sentence 3, the asset must constitute the proceeds of a listed predicate offence. Normally a distinction must be made between the following situations: That which is directly obtained from a predicate offence (the 'original object') always constitutes proceeds of the predicate offence. Hence both that which is obtained from or for a predicate offence (such as the proceeds of or remuneration for a crime) and products resulting from a crime (such as counterfeit money or manufactured narcotic drugs) are classified as objects of the crime. An unaltered original object always satisfies the 'proceeds' criterion. Changing hands has no bearing on the continuation of its inherent incriminated nature. In addition, that which has taken the place of the (unaltered) original object also constitutes proceeds of the predicate offence. This includes surrogate objects, which also covers assets moved in cashless payment transactions. Whether an object that has taken the place of the original object (still) constitutes proceeds of the predicate offence must be determined from an economic perspective. Under case law developed by the Federal Court of Justice, it is sufficient for the portion of the asset that originates from predicate offences to be "not completely insignificant", with no fixed minimum proportion. From an economic perspective, a new object only ceases to be incriminated when its value is substantially attributable to an independent subsequent third-party contribution.

Based on the classification in the above-mentioned international agreements, the offence is divided into three categories of criminal conduct: concealment, obstruction and isolation. Concealment (subsection (1) alternatives 1 and 2) includes hiding an object and concealing its origin. Hiding is any activity that hinders access to the object of the crime by way of keeping it at an unusual location or of conduct calculated to conceal it. Concealing the origin of an object covers all deceptive conduct that aims to make the object of a crime appear to have a different (legal) origin or at least to hide its true origin. Such conduct comprises abstract endangerment offences and it is not necessary for there to be a present endangerment of investigations that are actually in progress.

The obstruction category (subsection 1 alternative 3 onwards) covers conduct that impairs criminal prosecution by either obstructing or specifically endangering the maintenance of a 'paper trail'. Individually specified measures on the part of law enforcement agencies are obstructed if the perpetrator not only delays, but at least in part prevents them. If a measure is specifically under threat of being prevented by the perpetrator, then the alternative criterion of endangerment is satisfied. It is not necessary for the perpetrator themselves to have obtained the asset at a given time. The necessary criterion of specific endangerment is not satisfied if the criminal act merely serves to prepare for a later act of endangerment yet to be separately brought about (such as making available a bank account for an incriminated amount of money

to be used for wire transfers and withdrawals prior to cash wire transfers abroad).

Isolation (subsection (2)) relates to the procurement, keeping or use of incriminated objects. The criterion of procurement is satisfied by procuring control of the incriminated asset by subordinate means. It merely requires the perpetrator to acquire personal, actual control of the incriminated object as the result of an act of transfer in agreement with the predicate offender. Keeping (subsection (2) no. 2) is to be understood as taking the object of the crime into and holding it in possession in order to keep it for a third party or for one's own subsequent use.

The subjective criterion requires at least conditional intent. Recklessness will suffice if the incriminated object originates from a listed offence (subsection (5)). According to a decision of the Federal Constitutional Court, an exception applies in the case of the criteria under subsection (1) alternative 3 onwards and subsection 2 for money laundering by a criminal defence lawyer who must have had sure knowledge of the incriminated origin of the lawyer's fee at the time it was accepted.

Since 2015, it has also been a criminal offence to launder objects that are the proceeds of a predicate offence committed by the perpetrator themselves (self-laundering). To implement the FATF recommendations on the subject, impunity in the case of self-laundering was limited to money laundering conduct by a predicate offender which constitutes typical post-offence conduct (such as hiding the proceeds) or which – viewed in isolation – is socially normal and its unlawfulness only follows from being linked with the predicate offence (BT-Drucksache 18/6389, p. 11). For there to be criminal liability, the perpetrator must bring into circulation an object that constitutes the proceeds of the perpetrator's own predicate offence while obscuring the object's illegal origin.

2.3.2 National security law on countering the financing of terrorism

The Federal Government accords top priority to the fight against international terrorism. All international frameworks on countering the financing of terrorism have been transposed into national law. This includes international conventions, United Nations Security Council resolutions and FATF recommendations. German law on countering the financing of terrorism is part of general criminal law. There is not therefore a separate code of criminal law on terrorism.

The Federal Government attaches the utmost importance to effective law enforcement geared to real dangers and the needs of law enforcement agencies while countering future dangers by upholding human rights and the rule of law and thus removing the basis for radicalising tendencies.

All terrorist financing acts, whether by individuals or groups, are criminal offences in Germany. Severe (prison) sentences are generally imposed, for one thing to adequately match the severity of the crime. Time in prison is generally used for deradicalisation measures. All available criminal prosecution means are used in the investigation of terrorist financing activities. The authorities seek to make use of all relevant information and to exchange information in order to prevent or interrupt activities that it is not possible to prosecute.

The criminal offences under section 89c, 129a and 129b of the Criminal Code and section 18 of the Foreign Trade and Payments Act (*Aussenwirtschaftsgesetz*) cover all three categories of terrorist financing risk identified by the FATF:

1) Collection of assets in Germany and transfer to recipients abroad for terrorist purposes

2) Channelling assets collected abroad for terrorist purposes through the German financial system to a foreign recipient

3) Transfer of assets collected abroad to Germany and use for terrorist purposes in Germany.

It should be emphasised that the fact that acts of terrorist financing are classified as crimes under sections 129a and 129b of the Criminal Code enables the imposition of significantly more severe sentences. Section 129a (1) and (2) of the Criminal Code and section 18 (1) no. 1a alternative 8 and no. 1b of the Foreign Trade and Payments Act also cover attempt.

The offence of terrorist financing (section 89c of the Criminal Code) was created with effect from 20 June 2015 by the Act of 12 June 2015 and replaced the previous provision in section 89a (2) no. 4. Under section 89c of the Criminal Code, the financing of all terrorist offences is a criminal offence. It is thus an offence to collect, receive or make available assets for such a purpose. Assets in this connection primarily comprise money and other items of monetary value. It suffices under section 89c (1) for the perpetrator to have mere knowledge that the funds are meant to be used by a third party, or by the perpetrator (subsection (2)), to commit one of the listed offences. There is therefore no need for an objective connection with the financing of a specific act. Similarly, the perpetrator does not need to know, from a subjective perspective, what specific act the funds are meant to be used for; it suffices for the perpetrator to know or to have the intention that the funds are meant to be used for an (as yet unspecified) act within the meaning of section 89c (1) sentence 1 no. 1 to no. 8. Combining the acts into a single offence, abolishing the materiality threshold for the value of assets and creating a minimum imprisonment penalty has brought German law into line with corresponding FATF stipulations.

The offence under section 89c of the Criminal Code is, in practice, highly important as an initial offence which results in investigations that later frequently lead to charges under section 129a (1) or (2) or section 129a (5). This is because it is frequently easier to obtain the necessary proof of acts leading to the opening of investigation proceedings and hence potential criminal prosecution with reference to section 89c, than with regard to an offence under section 129a (1) or (2) or section 129a (5) of the Criminal Code. Alternatively, prosecution may be brought under section 18 (1) no. 1a alternative 8 or no. 1b of the Foreign Trade and Payments Act, for which the requirements are significantly lower with regard to subjective aspects of the offence. The "provision" or otherwise "making available" of assets in violation of an embargo imposed by a legal act of the European Union can constitute a criminal terrorist financing offence under section 18 (1) no. 1a – previously, until 31 August 2018, section 34 (4) no. 2 – of the Foreign Trade and Payments Act. This notably includes donating money or other economic benefits of any kind to individuals or organisations listed in the EU as suspected terrorists. It is not necessary to make any determination as to the use or intended use of an asset. Merely providing an asset such that the listed individual or organisation has direct access to it satisfies the criteria for the offence. It is necessary – and also sufficient – for the donor to be aware of the circumstances that result in the recipient being subject to economic restrictions.

3 National money laundering and terrorist financing risk situation

3 National money laundering and terrorist financing risk situation

3.1 Money laundering risk situation

3.1.1 National money laundering threat assessment

With a gross domestic product of €3,263.4 billion in 2017, the Federal Republic of Germany is the largest economy in the European Union and the fourth largest in the world. Germany is also an open, highly stable country in the middle of Europe with a very strong, internationally interconnected financial centre and a prospering industrial base. German products are in demand and highly regarded internationally. Germany is highly attractive for investment of all kinds, although this also includes investment of incriminated funds. At the same time, German society has a relatively strong preference for using cash. In light of Germany's high economic attractiveness and the high cash intensity and diversity of the economy, the National Risk Assessment rates the money laundering threat for Germany as medium-high (on a scale of high, medium-high, medium, medium-low and low).

How often money laundering offences are committed in Germany and what sums are involved cannot be gauged with any accuracy because it is impossible to reliably estimate the scale of unreported crime. One estimate puts the annual volume of money laundering in Germany at €100 billion (Professor Bussmann in the dark figure study[4] commissioned by the Federal Ministry of Finance and published in 2016). No separate estimates were made for the National Risk Assessment, as the available police and judicial data do not purport to be representative of the overall situation in Germany. Nor is any other statistical material available on this point. Unquestionably, however, money laundering can cause major economic distortions, disrupt the economy and thus inflict lasting harm on the country.

The National Threat Situation working group in the National Risk Assessment estimated that the majority of money laundering predicate offences (about two-thirds of cases) took place in Germany. This estimate was primarily based on surveys conducted in the jurisdiction of the participating prosecutor general offices and on the experience of participating police and FIU experts. In cases with an international dimension, it was not always possible, despite requests for mutual legal assistance, exchange between FIUs and via Interpol, to determine conclusively where (in Germany or abroad) the predicate offence took place, or where the incriminated funds originated. Precisely because of its powerful economy and general stability, however, Germany is a highly attractive destination for assets incriminated in international organised crime (OC). The National Situation Report 2017 on Organised Crime published by the Federal Criminal Police Office (Bundeskriminalamt) on 1 August 2018 listed a total of 213 OC investigations involving money laundering activities in 2017 (2017: 213/37.2%; 2016: 212/37.7%).[5] In addition, inquiries into money laundering under section 261 of the Criminal Code were conducted in 21.0% of OC investigations (2017: 120; 2016: 130/23.1%). Besides investigations dealing solely with money laundering, most inquiries into money laundering under section 261 of the Criminal Code were conducted in OC investigations concerning drug trafficking/smuggling (36), crime associated with the business world (23) and property

4 See Dark figure study on the prevalence of money laundering in Germany and the risks of money laundering in individual economic sectors, Kai Bussmann, 2016.

5 See Federal Criminal Police Office, Organised Crime, National Situation Report 2017.

crime (15). Moreover, 564 suspicious transaction reports (STRs) under section 43 (1) of the Money Laundering Act were filed in 100 OC investigations (2016: 869 STRs in 108 OC investigations). It should be noted in this connection that AML in Germany can take the form of financial investigations both as part of and independently of prosecution proceedings. According to the Federal Criminal Police Office, the proportion of OC investigations in which financial investigations were conducted averaged about 90% over the past ten years. Financial investigations as part of prosecution proceedings have the purpose of tracking down assets relating to a known predicate offence and identifying the money laundering acts in criminal investigation proceedings. In the case of financial investigations that are independent of prosecution proceedings, suspicious financial transactions are examined in analyses and investigations independently of a specific underlying crime. The aim is to identify the act of which the assets are the proceeds and hence possibly a predicate offence under section 261 of the Criminal Code, as well as to investigate the flows of funds.

The National Risk Assessment concluded that money laundering risk is heightened by the availability of options for conducting transactions anonymously, such as in cash. It should be noted in this connection that cash is highly popular in Germany and the overwhelming majority of Germans regularly pay in cash. According to a Deutsche Bundesbank study on payment behaviour in Germany in 2017[6], cash accounts for 48% of all turnover (about 74% of all transactions). Cash is generally suited to money laundering as its anonymity makes it possible to avoid leaving a trail. At the same time, the aim of money laundering offenders in many cases will be to launder incriminated cash into the cashless payment system while concealing its illegal origin. It has been known for incriminated cash from international organised crime to be frequently smuggled into and out of the country using cash couriers. This deliberately circumvents the restrictions and safeguards of the financial sector. To this end, criminal organisations specifically recruit individuals to transport their incriminated cash on a regular basis across an international border by air, sea, road or rail. The customs administration therefore carries out regular cash checks and will be further intensifying them (see chapter 3.1.5.4). However, it should be noted in this regard that there are few reliable statistics overall, and there are also numerous ways of concealing the trail in cashless payment transactions. This makes it essential to obtain more precise empirical data in this area.

A number of EU Member States have prohibited cash payments above a certain monetary amount and have tightened such rules even further following recent terrorist attacks. There is an assumption that the lack of harmonisation in the EU internal market could lead to a migration of incriminated funds to Member States (such as Germany) that do not have such cash limits. Up to now, there is no empirical data on this point. In a free single European internal market, therefore, the European Commission, for example, should collate better data on the actual scale of the use of cash for money laundering and terrorist financing. It should then be examined whether, in a free single internal market, an effective and simultaneously proportionate means can be found of limiting the misuse of cash and thus better combating money laundering and terrorist financing.

In light of the above, the National Risk Assessment concluded that cash-intensive sectors such as catering, trade in goods and the craft trades may be particularly susceptible to the illegal use of cash. As relevant cases in these sectors frequently involve tax evasion and deliberate complicity in money laundering offences ('active' money laundering), adding to the list of obliged entities under the Money Laundering Act would not appear helpful, especially considering that, in the catering and craft trades sectors in particular, it is not the customers laundering incriminated money. Rather, it is more important to raise awareness

6 Deutsche Bundesbank, Payment behaviour in Germany in 2017, 2018.

among the tax authorities and tax advisers in order to increase the reporting of suspicious transactions in the sectors concerned and also include consideration for anonymity aspects.

It should be noted here that anonymity facilitates money laundering in various situations, and not solely with regard to cash. Certain crypto assets (see section 6) and prepaid credit cards (under a threshold of €100) can also be used for anonymous payment. It can therefore be said in general that adequate counterparty identification by obliged entities under the Money Laundering Act is of special importance in the prevention of money laundering.

3.1.2 Analysis of money laundering predicate offences

Analysis of predicate offences is highly important to effectively combating money laundering. It is not necessary for a predicate offence to be assigned to a specific listed offence. Nevertheless, it must be possible to rule out that money has been obtained lawfully or originates from a non-listed offence that does not constitute a money laundering predicate offence. It should be noted in this connection that Germany as a whole is one of the safest countries in the world. The state nevertheless has a central task of further improving public safety and effectively combating crime. AML is highly effective in this regard, as would-be offenders lose the incentive to commit certain crimes if they cannot use the resulting profits in the legal economy.

The prevalence of predicate offences was analysed on the basis of the Police Crime Statistics, judiciary statistics, recent examples of cases of what is referred to as 'clan crime' as well as the assessment of experts from the agencies involved, including with regard to unreported crime. Predicate offences identified in the European Commission's supranational risk analysis were also included in the analysis.

The experts comprising the National Threat Situation working group ranked fraud, drug-related crime and human trafficking as the predicate offences with the greatest money laundering threat. The money laundering risk for each of these offences was ranked as medium-high (on a scale of high, medium-high, medium, medium-low and low). Table 1 shows related statistical data from the Police Crime Statistics. These three predicate offences are criminal offences which, from experience, are frequently committed in connection with organised crime. OC is defined by the police as the planned commission of criminal offences that are driven by a significant profit or power motive and are individually or collectively of significant scale. It requires the involvement of two or more persons acting in concert with division of responsibilities for a prolonged or indefinite period of time and using commercial or business-like structures, applying force or other means of intimidation or exerting influence on politics, the media, the public administration, the judiciary or the business sector. In essence, therefore, AML can often be equated with combating OC. In many cases, OC offences have an international dimension.

Fraud is a property offence and comes under section 263 of the Criminal Code. The criminal provision has the purpose of protecting property and covers forms of conduct by which somebody deceives somebody else into compromising their own property or that of another for the benefit of the perpetrator or a third party. The judicial and police authorities consider fraud on an organised or commercial basis in particular to constitute a money laundering predicate offence that is frequently followed by money laundering offences. In many cases, groups possess organised structures and manage to obtain very large sums of money. It is probable that the number of unreported cases will normally be small here, as there is typically a victim who is likely to report the crime. In isolated cases, however, a victim of fraud will refrain from reporting the crime due to reputation risk or out of shame.

Drug-related crime also results in money laundering predicate offences on a significant scale. OC structures are generally involved in the large-scale production and distribution of drugs. It can be assumed as a rule that the milieu will possess established money laundering structures. It should be noted in this connection that what constitutes a drug trafficking offence is interpreted very broadly in Germany (extending far into the realm of typical money laundering activities such as the use of cash couriers). The courts very frequenty adjudicate such cases as drug cases rather than as acts of money laundering, even though money laundering is effectively involved. There can also be assumed to be a large number of unreported cases in this area. It is typically an offence that only comes to notice by active investigation (a detected offence as opposed to a reported offence). Illegal drug trafficking plays a central role in the form of OC referred to as 'clan crime'. It should be pointed out here that it is not the case that members of what are called family clans can generally be presumed to be criminal; instead, it is a matter of some parts of such groups committing or having committed criminal offences. This mainly relates to international trafficking in cocaine and cannabis. Members of such OC structures are involved to varying degrees across the entire 'supply chain'. Direct links with South American production locations can be identified as well as diverse involvement in financing, transporting or distributing drugs at central level. Alongside conventional investment in real estate (see section 5.1), businesses typical of the milieu such as shisha bars that form part of a predominately urban event culture offer considerable potential for money laundering activities. Similarly to shisha bars, gambling and betting establishments controlled by such clan structures (see section 5.3) also offer a means of laundering criminally derived money into the legal economy and are thus an integral part of such money laundering activities. They additionally provide a base for preparing, arranging and committing criminal offences.[7]

Human trafficking is a further offence that is frequently characterised by OC structures (as with forced prostitution and temporary employment in the construction sector). Although the number of investigation proceedings is relatively small, they are frequently highly complex, wide-ranging investigations. Witnesses are very frequently from abroad and almost impossible to reach at the time of the main hearing. Human trafficking, too, can be assumed to generate considerable sums in the form of illegal assets. With regard to temporary employment, it can be assumed that there is a large number of unreported cases, despite intensive inspection activity by the Financial Monitoring Unit to Combat Illicit Employment (Finanzkontrolle Schwarzarbeit). Given the good economic situation in Germany, it is expected that 'illegal workers' will continue to be in demand in various sectors. In light of the above, this predicate offence is expected to gain in importance over the long term.

	Number of cases (Police Crime Statistics)			Amounts secured (excluding by judiciary) (€)		
	2014	2015	2016	2014	2015	2016
Fraud	968,866	966,326	899,043	80,960,619	126,034,002	158,031,597
Drug-related crime	276,734	282,604	302,594	21,076,105	21,290,745	24,288,104
Human trafficking	598	568	539	700,130	512,182	2,502,433

Table 1: Predicate offences with medium-high money laundering threat.

7 See Landeskriminalamt NRW, Clan-Kriminalität, Lagebild NRW 2018 (clan crime, NRW Situation Report 2018).

Six predicate offences were rated with a medium money laundering risk: corruption, human smuggling, illegal employment, tax offences, offences under the War Weapons Control Act (*Kriegswaffenkontrollgesetz*) and product piracy. In the area of corruption, it can be assumed that there is a high number of unreported cases, as corruption is not usually reported by those affected. Although corruption plays a fairly minor role in Germany in terms of the frequency of cases, it also tends to entail complex investigations, in some instances involving an international dimension and relatively large monetary amounts. The small number of money laundering investigations and convictions following corruption offences is frequently due to the use of other options for clearing up offences under sections 154 and 154a of the Code of Criminal Procedure (*Strafprozessordnung*).

Human smuggling has gained strongly in importance in recent years. The resulting money laundering threat is consequently rated as a medium risk. Human smuggling structures have become more professional overall in recent years, which can doubtless be explained by increased pressure from state investigation and prosecution activity.[8] There is also expected to be a large number of unreported cases as there is normally no injured party to report them. In light of the general security situation, the attendant refugee flows and the growing professionalism of human smuggling structures, this offence can be expected to continue to gain in importance.

Illegal employment under section 266a of the Criminal Code (non-payment and misuse of wages and salaries) does not currently constitute a money laundering predicate offence. For the forthcoming amendment of section 261 of the Criminal Code to transpose into national law the EU Directive on combating money laundering by criminal law, the National Risk Assessment recommends that consideration should be given to adding section 266a to the list of predicate offences. In light of the strong demand for labour, this offence is expected to continue to gain in importance with regard to money laundering. The resources of the Financial Monitoring Unit to Combat Illicit Employment should therefore be further increased in the years ahead in order to further intensify the fight against illegal employment.

Investigating and prosecuting tax evasion is a major concern for Germany and is vigorously pursued. This is reflected in the criminal tax cases concluded in Germany from 2014 to 2016, with between about 13,800 and 15,300 such cases finally concluded annually. Value added tax (VAT) evasion in particular tends to be an offence committed on an organised and commercial basis. It cannot be ruled out that there may be a large number of unreported cases of VAT evasion and that this number may further rise due to the good economic situation. Tax evasion on a commercial or organised basis and of money laundering significance is included in the list of money laundering predicate offences and section 261 of the Criminal Code therefore also applies for expenditure saved by virtue of tax evasion (subsection (1) sentence 3). Not all tax offences are currently listed as money laundering predicate offences, however, with the result that the predicate offence must in any case be more than 'simple' tax evasion in order to come within the scope of criminal liability for money laundering. From a practical prosecution perspective, extending criminal liability by adding all tax evasion offences to the list of predicate offences would facilitate criminal proof.

Offences under the War Weapons Control Act are frequently OC offences. In many cases there is also an international dimension. Such offences typically involve large sums of incriminated funds (particularly in the form of cash). Increasing use is also made of the dark web with its anonymous online platforms, with payment normally made using cryptocurrencies (see section 6). As part of collaboration between authorities in Germany,

8 See Bundeskriminalamt und Bundespolizei, Schleusungskriminalität, Gemeinsames Bundeslagebild 2017 (human smuggling, Joint National Situation Report 2017).

Austria and France, wide-ranging executive measures were taken in November 2017 in a complex of investigations against an arms dealing ring operating throughout Europe. This was preceded by two years of investigations in the three countries. As a result of the executive measures, six suspects were arrested in France, three in Austria and two in Germany. Searches in Germany resulted in the seizure in total of eleven firearms, large quantities of ammunition and around €100,000 in cash. In Austria, a total of 47 short firearms, 106 long firearms, several hundred kilograms of ammunition and about €35,000 in cash were seized.[9]

	Number of cases (Police Crime Statistics)			Amounts secured (excluding by judiciary) (€)		
	2014	2015	2016	2014	2015	2016
Corruption	6,571	4,790	4,292	30,485,673	8,055,763	32,963,004
Human smuggling offences	3,612	5,140	3,666	0	0	0
Illegal employment	86,557	88,466	88,468	748,437	242,819	2,893,748
Tax offences[11]	15,193	15,269	13,801	11,208,542	22,602,629	27,768,149
War Weapons Control Act offences	542	502	617	279,643	99,017	3,350
Product piracy[12]	45,738	23,338	21,229	137,700,000	132,300,000	180,040,000

Table 2: Predicate offences with medium money laundering threat.

Product piracy is likewise a typical OC crime. OC-aided structures are generally used both in production and in distribution. According to a recent OECD study, trade in counterfeit and pirated goods accounted for about 3.3% of total world trade in 2016.[10] Counterfeit and pirated goods amount to some €450 billion a year, thus presenting major potential for money laundering. The money laundering threat from this crime area is expected to continue growing in Germany over the long term.

The money laundering threat with regard to the predicate offences of theft, forgery, counterfeiting money, blackmail and robbery is rated medium-low. Theft is a mass crime in Germany. In the majority of cases, however, the amounts involved are relatively small. Money laundering therefore plays a fairly minor role in such cases. Where such offences are committed on an organised basis, however, money laundering is of major importance as with other OC offences. The number of unreported cases will tend to be relatively small because the victim of a theft can generally be expected to report it. Thefts of low-value items of lesser money laundering significance, on the other hand, often go unreported because of the effort involved in doing so. The assessment for robbery is similar. Robbery in connection with OC (as part of clan crime, for example) is particularly significant as a money laundering predicate offence.

Professional document forgery and counterfeiting of money frequently involve established structures as there are relatively high barriers to the production of good forgeries. Germany experiences relatively few cases in this area overall. There is frequently an overlap with fraud cases. The number of unreported cases of professional document forgery is likely to be relatively large. Money counterfeiting offences

9 See Bundeskriminalamt, Waffenkriminalität, Bundeslagebild 2017 (gun crime, National Situation Report 2017).

10 See OECD/EUIPO, Illicit Trade – Trends in Trade in Counterfeit and Pirated Goods, 2019.

11 Criminal tax proceedings concluded by public prosecution offices and courts in each year. Amounts seized excluding tax authorities.

12 See Generalzolldirektion, Zolljahresstatistik 2016 (Annual Customs Statistics 2016), p. 12. Product piracy is not covered by the Police Crime Statistics.

can be a source of income, for example via the dark web. Such cases often involve large sums that are distributed on an organised basis. The bulk of cases probably relate to very small amounts, however, that are not laundered. There is presumed to be a particularly large number of unreported cases in connection with dark web crime.

With regard to blackmail, it should be noted that this has a certain significance as a money laundering predicate offence when committed in connection with OC, for example in the area of protection racketeering. Payments here are very frequently made in cash. The number of unreported cases is estimated to be very large as many victims of protection rackets are unlikely to report the offence for fear of reprisals. However, the great majority of prosecuted cases in Germany are for blackmail involving the use or threat of force, which tends to have less money laundering significance.

The money laundering threat is rated as low for the predicate offences embezzlement, unlawful appropriation and offences under the Weapons Act (*Waffengesetz*). Handling stolen goods is also a mass offence with relatively small item values that only acquires a higher threat potential in connection with OC. Handling stolen goods is therefore likewise rated as a low threat. Other offences can of course also be connected with money laundering according to the circumstances of the individual case.

The experts estimated that the majority of money laundering predicate offences in Germany took place domestically (see section 3.1.1). Predicate offences frequently also have links to multiple countries. In many other money laundering cases, it is not possible to determine conclusively whether the predicate offences took place in Germany or abroad. It is undisputed, however, that Germany is a highly attractive target for internationally operating money launderers, notably due to the strength of its economy and very high degree of political stability.

3.1.3 International interconnectedness of the German economy

Germany's economy is highly interconnected internationally. Germany is also a member of the European Single Market and has been a world-leading exporter for many years. Both the German financial sector and the designated non-financial businesses and professions (DNFBP) sector are very closely integrated into the global economy. The National Risk Assessment consequently attached great importance to the cross-border money laundering threat and assessed it between Germany and 33 other countries (or territories). Those countries were selected on the basis of various criteria. They included, in particular:

- All neighbouring states of Germany
- Countries where a relatively large number of Germans live
- Countries whose nationals live in Germany in relatively large numbers
- Countries of particular economic importance to Germany
- Countries that are frequently mentioned internationally in connection with ML/TF.

The ML threat for Germany was assessed as high risk with regard to the following eleven regions/states: Eastern Europe (in particular Russia), Turkey, China, Cyprus, Malta, British Virgin Islands, Cayman Islands, Bermuda, Guernsey, Jersey and Isle of Man. There is great variation among these countries regarding the specific ML risks for Germany.

Russian and Russian-speaking OC groups pose a substantial and sustained ML threat to German (and European) security interests. Western Europe is thus a focus of Russian OC money laundering activities. ML risk is additionally amplified by close ties between Russian OC and

intelligence structures in the region. According to intelligence gathered by German security agencies, incriminated funds from Russia are also known to have been laundered through the Frankfurt am Main financial centre (for example with the aid of correspondent banking relationships with German banks). There is intelligence in this context that incriminated funds are sent from Russia to London, Switzerland, overseas islands, Malta, Cyprus and Frankfurt am Main and then invested in Germany.

Germany and Turkey have strong economic links and there are extensive financial ties as well as very strong personal relationships due to the fact that large numbers of people of Turkish extraction live in Germany. The country continually comes into the focus of financial intermediaries specialising in money laundering as a pivot between East and West. Istanbul is thus considered a hub for OC as regards drug trafficking and illegal migration to Europe. There are also points of contact here with terrorist financing in the direction of the Middle East by way of hawala banking (see Chapter 3.2.2). At the same time, the Germany-Turkey corridor is very significant with regard to money or value transfer services (such as for remittances). Large quantities of cash in transit are discovered very frequently on flights to Turkey. It remains to be seen what effect the depreciation of the lira has on the flow of incriminated funds between Germany and Turkey.

Regarding China, cash infractions have frequently been detected on past flights from Germany to China. Large quantities of pirated products from China are also known to have been distributed in Europe by way of OC structures. The resulting incriminated profits were both laundered in Germany (for example through the purchase of luxury products and real estate) and transferred back to China (frequently by cash couriers).

Concerning Malta, the specific ML risk is inherent in the structure of the financial centre, which could abet opacity and concealment. Malta is also a gambling hub. It is a base for online gambling (in the form of online casinos), which is prohibited in Germany. This generates illegal profits in Germany. For some years, Malta has also implemented a so-called Golden Visa programme under which investors can obtain Maltese citizenship for a specific fee. Malta enables foreign nationals to become Maltese citizens in return for investment, provided that certain criteria are met. As with Malta, the design of the Cypriot financial centre and the Golden Visa programme there also create the possibility of specific ML risks for Germany, thus potentially abetting opacity and concealment.

Golden Visa programmes

In addition to Malta and Cyprus, the countries analysed also include other EU Member States with Golden Visa programmes. They require an investment of between €800,000 and €2 million in order to obtain citizenship. For criminals, this offers an attractive opportunity to invest incriminated funds with the added benefit of acquiring citizenship of the country concerned. Such citizenship arrangements for investors thus entail a variety of risks for the Member States in question, and also for the EU as a whole – in particular, security risks and also risks related to money laundering, corruption and tax evasion. These risks are heightened by the cross-border rights that go with Union citizenship. Under the Fourth EU Money Laundering Directive, financial institutions and other entities ('obliged entities') in the EU are required to conduct customer due diligence checks to satisfy their due diligence obligations. The Directive amending the Fourth EU Money Laundering

Directive, which entered into force on 9 July 2018, introduced the requirement to carry out more due diligence checks when a third-country national "applies for residence rights or citizenship in the Member State in exchange of [sic] capital transfers, purchase of real estate or government bonds, or investment in corporate entities in that Member State". Germany will transpose this requirement into national law at the latest by 10 January 2020. Member States must also ensure that citizenship arrangements for investors do not circumvent the application of EU anti-money laundering rules. They must therefore ensure that funds paid by applicants for citizenship and residence rights go through institutions that are obliged entities within the meaning of the Money Laundering Directive.

With regard to the British Virgin Islands, the Cayman Islands, Bermuda, Guernsey, Jersey and the Isle of Man, the specific money laundering risk for Germany lies in the structure of the financial centre, which in each case permits opacity and concealment. In these destinations, incriminated funds, including funds from Germany, can be easily invested in a variety of vehicles (such as shell companies).

The ML threat for Germany was assessed as a medium-high risk for the six states Lebanon, Panama, Latvia, Switzerland, Italy and the United Kingdom. Lebanon in particular plays a major role here with regard to the laundering of 'clan crime' funds. This form of OC is active in certain parts of Germany (notably Berlin, the greater Bremen region and the Ruhr region) and is presumed to be involved in numerous (international) OC offences. Funds acquired in Germany are frequently transferred to Lebanon and then laundered.

There are extensive economic and strong personal ties with Italy due to the large numbers of people of Italian extraction in Germany. The participating security agencies have indications of Italian OC attempting to launder incriminated funds, which are generated both domestically and internationally, in Germany (for example through the acquisition of properties in Germany). Italian OC is also known to have been active in protection racketeering in Germany. The resulting incriminated funds were laundered both in Germany and in Italy.

In conclusion, a high or medium-high money laundering threat for Germany has been identified with regard to the 17 states and regions mentioned. A further 17 countries were analysed that pose only a medium, medium-low or low ML threat for Germany. Further information is provided in Annex 4.

3.1.4 Legal arrangements and legal persons

As a global financial centre and internationally highly interconnected economy, Germany is particularly susceptible to money laundering risks associated with certain international company types. A total of 3,481,860 business enterprises operated in Germany in 2017. Despite the fact that the Germany economy is deeply interconnected at the global level, most of these were enterprises with fewer than ten employees subject to social insurance. According to the Company Register (*Unternehmensregister*), such enterprises account for 89% of enterprises in Germany.[13]

The supranational risk assessment by the European Commission has shown that criminals often try to hide their identities through shell companies, trusts or complicated corporate structures. In such cases, the beneficial owners cannot be clearly identified. To the knowledge of the law enforcement agencies, in larger-scale ML/TF cases (in the case of TF mainly involving non-profit organisations), repeated use has been made of opaque structures in order to

13 See Unternehmensregister, 2017.

conceal beneficial owners (in ML cases primarily by using foreign company types). Germany has consequently launched numerous measures in recent years for greater transparency with regard to such legal arrangements. This included the establishment of the Transparency Register in 2017 (see section 3.1.5.1). In this regard, it can generally be said that German legal entities tend to be poorly suited as vehicles for money laundering due to the requirement as to veracity of the register. The main entry point here is likely to be foreign companies as shareholders. However, this is primarily a susceptibility of the foreign company type and hence essentially a foreign risk that materialises or could have an adverse impact in Germany (meaning Germany is affected only indirectly).

In the course of this National Risk Assessment, the most common company types operating in Germany were analysed and assessed for their money laundering threat. With regard to OC, it can generally be said that when deciding what company type to use in a specific case, OC groups weigh up various factors including the economic strength of their organisation, their field of activity and how they plan the money laundering to take place in order to minimise the risk of detection and maximise their financial profit from the offences committed. Foreign company types are often selected due to the lack of requirements as to veracity of the register. Many foreign companies are not subject to such veracity requirements, and this poses considerable risks. The Transparency Register aims to counter these risks. This is predominantly unnecessary for German companies, however, as the information concerned is already in the Commercial Register (*Handelsregister*) and cross-referenced in the Transparency Register.

Among German company types, most cases in the area of general economic crime relate to companies incorporated as a GmbH (*Gesellschaft mit beschränkter Haftung*) – a German private limited company. This is ascribed to the fact that the GmbH is a popular and widespread company type. Money laundering offences mainly involve small and medium-sized enterprises that in most cases are not specifically established for the purpose of money laundering. Instead, the acts relating to money laundering take place using existing corporate vehicles. Overall, it can be concluded that the GmbH is a proven company type that is of great importance for small and medium-sized enterprises, in particular due to the liability regime (with liability to creditors for the company's debts limited to its capital).

Among GmbHs, a subtype that is very frequently encountered in connection with money laundering activities is the *Unternehmergesellschaft* (*haftungsbeschränkt*), this being a type of limited liability company that can be established relatively easily without a significant minimum capital requirement. A comparable foreign company type would be the limited company (as in the United Kingdom). Limited companies are similarly well suited for money laundering. It can be stated in general that any corporate structure whose ultimate beneficial owner is not a natural person but an anonymous or anonymised company type (Ltd. or trust – either a common-law trust or in Germany a *Treuhänder*), is susceptible to money laundering (and also terrorist financing) and significantly impedes investigations for criminal prosecution purposes.

A further company type frequently encountered in certain business areas is the AG (*Aktiengesellschaft*), which is a German public limited company. These are very frequently large business enterprises whose susceptibility to money laundering does not necessarily follow from being incorporated as an AG but from their specific business activities. It is relatively rare for an AG to be established specifically for the purpose of engaging in and concealing money laundering.

Among partnerships, susceptibility to money laundering is seen in the GbR (*Gesellschaft bürgerlichen Rechts*) – the German civil-law partnership. Supervision of such businesses is structurally more difficult due to the diverse and flexible forms of arrangement. All company types that are easy to launch with little red tape are suited in principle to money laundering. Such companies can be made available at short notice to set up a money laundering scheme. With a GbR, however, ML risk is crucially mitigated by the partnership necessarily being linked to the identities of the partners. Partnerships therefore do not provide the concealment that is so important to money launderers.

Non-profit organisations (NPOs) are also encountered in connection with terrorist financing activities. In Germany, NPOs very frequently take the form of an e. V. (*eingetragener Verein*) – a German registered association. In light of the specific features of the non-profit sector and the prominence of NPOs, including in international financial transactions, seen in countering the financing of terrorism, the Federal Government is currently working on a separate sectoral risk assessment with a focus on this thematic area. Registered associations (in particular) are also encountered in connection with what is referred to as 'rocker crime' and politically motivated crime by foreign nationals.

Foreign companies can be used by criminals as corporate vehicles to launder their incriminated funds. Such companies are used to invest the incriminated funds worldwide (including, for example, in the German real estate sector). In connection with the use of foreign corporate networks, the Federal Criminal Police Office is currently conducting extensive investigations into the so-called 'Panama Papers'.[14] The example of the Panama Papers illustrates the large scale of investigations in OC cases in this field. The Federal Criminal Police Office has the entire dataset.

14 See Federal Criminal Police Office, Organised Crime, National Situation Report 2017.

This consists of data from Panamanian offshore service provider Mossack Fonseca. The Panama Papers dataset obtained and structured by the Federal Criminal Police Office has a data volume of 2.78 terabytes comprising some 41,500,000 objects, including emails, documents from the client portfolio, information on discussions with clients, account transactions and incorporation documents. Mossack Fonseca supported some 14,000 clients in the incorporation of 270,000 shell companies in 21 offshore regions. It can be said in this connection that the use of foreign company types significantly complicates ownership structures and is therefore particularly well suited to the concealment of incriminated assets. Opening up German company law to foreign company types has thus created a commensurate degree of risk (notably in connection with offshore companies).

3.1.5 National defence mechanisms and responsibilities in anti-money laundering

Germany has set up national AML/CFT defence mechanisms. The aim is for money laundering to be effectively prevented and combated by the competent authorities both at Federal and at *Länder* level.

3.1.5.1 Transparency and openness: role of the Transparency Register and of the Commercial Register, Cooperative Societies Register and Partnerships Register

The Transparency Register, which has been available on a tiered access basis since 27 December 2017, is conceived as a form of backstop. Companies and other legal persons must provide

information on their beneficial owner in the Transparency Register if that information is not already available from entries and documents in certain other public registers. Accordingly, the Transparency Register provides access to other relevant registers from which beneficial ownership can be ascertained in addition to entries recorded in the Transparency Register itself.

Legal representatives of legal persons under private law and of partnerships with legal capacity (section 20 (1) of the Money Laundering Act) as well as trustees and Treuhänder (section 21 (1) and (2) of the Money Laundering Act) must give notification of their beneficial owners for entry in the Transparency Register without delay unless the beneficial owners are already ascertainable from other public sources (such as the Commercial Register). Listed companies are exempted from separate notification for the Transparency Register if the exercise of control is already evident from voting rights notifications.

The following information on the beneficial owner must be included in the notification: first name and surname, date of birth, place of residence, type of beneficial owner (notional or actual) and the nature and extent of the beneficial interest (see section 19 (1) of the Money Laundering Act). Notification is also required if there are subsequent changes to the information on the beneficial owner or the situation changes or reverts so that the beneficial owner can henceforth be ascertained from other registers.

Access to search the Transparency Register is currently tiered according to the function of the inspecting party. Certain public agencies thus have full access to the data in the Transparency Register in the course of their duties. Obliged entities, on the other hand, can only access it on a case-by-case basis and to meet due diligence requirements. In addition, anyone can be given access to specific entries provided that they demonstrate a legitimate interest in the case in question.

Transposition into national law of the Directive amending the Fourth EU Money Laundering Directive (Directive (EU) 2018/843) is expected to result in changes to the Transparency Register from 1 January 2020 as follows:

In accordance with the requirements of the Directive, the Transparency Register will be accessible in future to the "general public". As before, inspecting parties must register online with the Transparency Register providing proof of identity and must pay an inspection fee. Neither the place of residence nor the precise address of beneficial owners will be viewable for the general public. As is already the case, restrictions can be applied for in the case of danger to life or limb of the beneficial owner.

In future, obliged entities under the Money Laundering Act and competent authorities will be required after inspection to report to the registrar entity any discrepancies in the Transparency Register that may come to their attention. This is to ensure the accuracy and high quality of entries.

In addition, obliged entities under the Money Laundering Act will be required in future to obtain proof of registration or an extract from the Register when they begin a new business relationship with associations or legal entities that are registered in the Transparency Register. This is to ensure that the associations or legal entities concerned have complied with the notification requirement for entry in the Transparency Register.

The introduction of the Transparency Register created a useful tool for enhancing transparency. The quality of data recorded in the Transparency Register will be further improved. The search features for the Register are also subject to ongoing improvement. An additional aim is to further enhance the utility of the Transparency Register in all areas of AML/CFT. From the perspective of the law enforcement agencies and the FIU,

consideration should therefore be given to providing them with the ability to search the Transparency Register for beneficial owners by name.

The purpose of the Commercial Register (*Handelsregister*) is to disclose facts and legal relationships, relating to merchants and commercial enterprises, that are essential in legal dealings. As a public register of key company data and legal facts, it is above all a means of increasing corporate disclosure in order to better safeguard legal relations in general. The Commercial Register consequently aims to provide a presentation of the facts required to be entered that is as clear, reliable, complete and current as possible. In a similar way, the Cooperative Societies Register (*Genossenschaftsregister*) provides information on the legal relationships of registered cooperatives, and the Partnerships Register (*Partnerschaftsregister*) on partnerships.

What specifically must or may be entered in the Commercial Register is determined by requirements for each type of company. This information typically consists of the company name, registered office, headquarters and subsidiaries or branches, company objects, authorised representatives, company type, share capital and name of the proprietor. The information contained in the Cooperative Societies Register comprises the name of the cooperative, registered office and objects, any obligation for members to make additional contributions to capital, the management board, representation rules, holders of Prokura (statutory general power of attorney), the opening, rescission or termination of insolvency proceedings, dissolution and deregistration of the cooperative; the information contained in the Partnerships Register comprises the personal details and profession exercised by each partner, the name of the partnership and the place where it has its registered office, general rules governing the representation of the partners and any specific rules relating to individual partners, and further information comprising any change of name of the partnership, change between partnership and professional partnership with limited professional liability, relocation of the registered office, entry of a new partner, departure of a partner, change in power of representation, change in the objects of the partnership, dissolution of the partnership or deregistration of the partnership. The entries in the Commercial Register, Cooperative Societies Register and Partnerships Register are therefore directed in particular at disclosing ownership structures, including authorised representation. The accuracy of the facts recorded is primarily ensured on a preventive basis by the involvement of civil law notaries in registration filings and by judicial examination of filings. Responsibility for public authentication lies with the notary. The notary must not only verify and record the identity of each individual whose signature is to be authenticated (section 40 (4) read in conjunction with section 10 of the Certification Act (*Beurkundungsgesetz*)), but must also check whether there are grounds for refusing to perform the notary's official function, for example because the content of a document violates a statutory prohibition (section 40 (2) of the Certification Act), and – in the case of entries in the Commercial Register – check that the filing is capable of entry (section 378 (3) sentence 1 of the Act on Proceedings in Family Matters and in Matters of Non-contentious Jurisdiction (*Familienverfahrensgesetz*)). Additional checks by a notary are unnecessary for filings in the Cooperative Societies Register as these generally require an advance assessment by the audit body (section 11a of the Cooperatives Act (*Genossenschaftsgesetz*)).

The Commercial Register, Cooperatives Societies Register and Partnerships Register and the documents filed with them may be inspected by anyone for information purposes, meaning without proof of legitimate interest (section 385 of the Act on Proceedings in Family Matters and in Matters of Non-contentious Jurisdiction read in conjunction with section 9 (1) sentence

1 of the Commercial Code; section 156 (1) of the Cooperatives Act; section 5 (2) of the Partnership Companies Act (*Partnerschaftsgesellschaftsgesetz*). Inspection usually takes place by automated data retrieval (section 9 (1) of the Commercial Code; section 52 of the Commercial Register Ordinance (*Handelsregisterverordnung*); section 156 (1) sentence 1 of the Cooperatives Act; section 1 of the Ordinance on the Register of Cooperative Societies (*Genossenschaftsregisterverordnung*); section 5 (2) of the Partnership Companies Act). German public agencies and foreign public agencies within the scope of the EU Services Directive are exempt from paying the fees usually charged for inspection.

3.1.5.2 Prevention and supervision

Germany attaches the utmost importance to ML/TF prevention. The supreme guiding principle of the German supervisory authorities comprises early detection of risks and implementation of robust defence mechanisms.

The supervisory authority for obliged entities in the financial sector is the Federal Financial Supervisory Authority (BaFin). To this end, BaFin has established a Department for the Prevention of Money Laundering. BaFin performs the ongoing supervision of banks, insurers, asset management companies and agents in the money or value transfer service business. In the course of its ongoing supervision activities, BaFin analyses the audit reports of obliged entities and holds regular discussions with entities' management. It also conducts audits of its own, both routinely on the basis of the BaFin risk assessment of obliged entities and on an ad-hoc basis. BaFin continuously improves risk-based money laundering supervision taking into account the specific risk situation of each obliged entity (see section 4). It plans in this context to intensify dialogue with obliged entities. BaFin will vigilantly monitor technological change in the financial sector and counter the resulting ML/TF phenomena. The Federal Government will ensure in this context that BaFin continues to have the necessary resources at its disposal on an appropriate scale so that it can continue to discharge its growing responsibilities.

In the DNFBP sector, supervision is essentially the responsibility of the *Länder* supervisory authorities and of professional governing bodies in the case of certain liberal professions. The structure of the various industries in the DNFBP sector (see section 5) means that supervision of the obliged entities in some cases involves specific challenges. In certain industries, for example, there is no exhaustive list of all obliged entities; examples include traders in goods and service providers for companies, Treuhand assets and Treuhänder (civil-law trusts and trustees). More resources are also to be made available with regard to the DNFBP sector in order to adequately address the sector's special features. The coordinating function of the Financial Intelligence Unit (FIU) is also to be further strengthened in order to further improve the risk-based approach.

Ad-hoc exchange between agencies takes place as needed. A key finding of the National Risk Assessment in this connection is that information exchange both between agencies and with the private sector should be further increased overall and in part institutionalised in order to be able to respond even better to ML/TF risks. Together with the FIU, supervisory authorities have a major part to play in the organisation of such dialogue. The main state agencies to be involved alongside the supervisory authorities are police forces, the FIU and the intelligence services.

3.1.5.3 Financial Intelligence Unit

The Financial Intelligence Unit (FIU) – in German, Zentralstelle für Finanztransaktionsuntersuchungen – is the central national unit for the receipt, collection and analysis of suspicious transaction reports (STRs) that may be related to ML or TF. As of 26 June 2017, the FIU was transferred from the Federal Criminal Police Office to the Central Customs Authority and reorganised as an administrative authority. The reorganisation of the FIU was implemented on the basis of the Act on the Implementation of the Fourth EU Anti-Money Laundering Directive, the EU Funds Transfer Regulation and on the Reorganisation of the Financial Intelligence Unit (*Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen*).

Money laundering and terrorist financing are international phenomena that can only be effectively prevented and countered at international level in an integrated approach. Intensifying and optimising international cooperation is therefore a constant priority in the various bodies and in bilateral and multilateral consultations between the FIU and its international partners. The FIU is a member of the Egmont Group, a network of currently 164 FIUs worldwide, and of the EU FIU Platform, a grouping of European FIUs initiated by the European Commission.

The FIU is a functionally independent agency that is organisationally embedded within the Central Customs Authority and within its functional area is independent in discharging its responsibilities and powers. Criminal investigations in the field of money laundering are conducted exclusively by the competent federal and *Länder* prosecution services and police authorities and where applicable by customs and tax investigation services. The FIU has the purpose of centrally receiving, analysing and assessing STRs. In 2018, a total of 77,252 (2017: 59,845) STRs were reported to the FIU under sections 11 and 14 of the former Money Laundering Act and sections 43 and 44 of the revised Money Laundering Act.[15] In accordance with its mandate and acting on the basis of findings and analysis results, the FIU 'filters out' only those cases that are worth pursuing. These are then passed on to the competent (law enforcement) authorities. If the Financial Intelligence Unit concludes in its analysis that an asset referred to in a report is connected to money laundering, terrorist financing or other criminal conduct, it is required to provide the competent law enforcement agency with all relevant information, including the report with its findings. Such a connection with money laundering, terrorist financing or another criminal offence is deemed to exist when, based on an appraisal of the individual case and all information drawn upon in the analysis, there may be sufficient factual indications of a crime having been committed. The FIU's analysis and assessment embodies a 'systemic' decision-making prerogative resulting from the fact that an STR is not a criminal complaint within the meaning of the Code of Criminal Procedure (*Strafprozessordnung*) but a reporting obligation under trade law. Accordingly, the new FIU has been established as an administrative authority to correlate with the administrative nature of the money laundering reporting system.

If the FIU has indications that a transaction is related to money laundering or terrorist financing, it may temporarily halt the transaction under section 40 of the Money Laundering Act in order to properly complete its analysis. The FIU will continuously improve the quality and targeting of analytical reports. Processing time per case is to be further reduced while maintaining the targeted quality level. STRs not involving complex money laundering and terrorist financing structures (such as those involving money mules

15 See FIU-Jahresbericht 2018 (FIU Annual Report 2018).

and fraud cases) are to be passed on in future to the law enforcement agencies without delay.

The FIU has a recognised human resources requirement (as of November 2018) of 475 staff, of which 400 are involved in discharging the FIU's policy area responsibilities. In the coming months, the FIU will gradually fill vacant budgeted staff positions with qualified staff in order to further accelerate STR processing.

On revision of the Money Laundering Act, the FIU's task description was expanded with a strengthening of its analysis work and closer cooperation with obliged entities and public agencies nationally and internationally in the field of AML/CFT. The FIU has a coordinating function with regard to the supervisory authorities, which also includes specific provision for information exchange. The FIU will further expand and strategically develop this competency in order to strengthen supervision overall and further improve interchange with obliged entities. The FIU's coordinating function is also intended to provide additional support for supervision in the DNFBP sector to enhance the effectiveness of AML/CFT in that sector.

Based on routine integration and application of basic parameters such as EU sanctions lists and the current FATF list of high-risk and other monitored jurisdictions, the FIU has identified priority risk areas categorised under the separate headings of money laundering and terrorist financing.[16] The FIU will use these to prioritise incoming STRs and their processing in operational analysis to adequately reflect the shared understanding of risk/crime concentrations and thus ensure that the risk-based approach is applied. Strategic analysis by the FIU additionally triggers supporting analyses to specifically address prioritised risk areas. This is notably aided by the compilation of specific typology papers, by the organisation of related events, by increased information interchange with partner authorities and obliged entities and by the corresponding involvement of national and international partners.

Under section 31 (5) of the Money Laundering Act, the FIU has broad powers to access tax data. The FIU is also ensured access to criminal prosecution data by way of section 31 (4) of the Money Laundering Act. For this purpose, to the extent necessary to discharge its responsibilities under section 28 (1) sentence 2 no. 2 of the Money Laundering Act, it has access to the INPOL Bund police forces joint database system.

The area of financial intelligence is to be further strengthened. The data to which the FIU has access and its powers are to be gradually extended for this purpose. The Federal Government therefore plans in future for the FIU to be additionally notified of police automated data-matching hits with regard to special category data. The FIU is also to have access to criminally relevant information in the Central Register of Proceedings Conducted by Public Prosecution Offices (ZStV). This will further enhance its ability to discharge its responsibilities as the central national unit for the receipt, collection and analysis of STRs, further improve reporting quality and progressively accelerate processing.

3.1.5.4 Anti-money laundering activities of the judiciary and security agencies

AML activities are conducted in Germany on the basis of a division of responsibilities between security and law enforcement agencies both at federal and at *Länder* level. Criminal prosecution, in particular, in relation to money laundering is largely a *Länder* responsibility in Germany and is handled by the competent prosecution services acting as lead agency with the support of police authorities and the customs investigation service.

16 See FIU key issues paper: Priority risk areas in FIU operations to combat money laundering and terrorist financing, 2019.

Money laundering investigations where ML is the primary offence are frequently conducted at the level of the Joint Financial Investigation Groups (Gemeinsame Finanzermittlungsgruppen/GFG). A GFG generally consists of the state criminal police office of the relevant *Land* and the competent customs investigation office. There is also a federal-level GFG under the Federal Criminal Police Office composed of equal numbers of officers from the Federal Criminal Police Office and the Customs Criminological Office. The GFG frequently leads investigations in large and complex cross-border cases. In other cases, the Federal Criminal Police Office conducts such investigations when requested by a prosecution service or where it has primary responsibility. Financial investigations are conducted on a standardised basis in OC investigation proceedings (including in investigations of money laundering predicate offences). According to the Federal Criminal Police Office, the proportion of OC investigations in which financial investigations were conducted averaged about 90% over the past ten years (see section 3.1.1). German prosecution services and police authorities are in constant communication with partner countries with regard to AML. With regard to the judiciary, Germany also takes part in Eurojust; with regard to the police, Germany takes part in both Europol and Interpol.

The law enforcement agencies generally have the entire scope of the Code of Criminal Procedure at their disposal in criminal investigations involving money laundering, with investigations frequently being taken up under section 152 (2) of the Code of Criminal Procedure on the basis of an initial suspicion – meaning where there are sufficient factual indications – of a crime under section 261 of the Criminal Code. STRs result in the tracing of account data and account movements and the analysis of money flows. In the course of STR clearing, the investigation then mostly focuses on the predicate offence, as section 261 of the Criminal Code is conceived as a follow-on offence based on (previous) unlawful conduct of which the asset must be the proceeds. Possible investigation measures under sections of the Code of Criminal Procedure, in addition to search and seizure, include telecommunications surveillance under section 100a, acoustic surveillance under section 100f, obtaining telecommunications traffic data under section 100g and mobile device location under section 100i and, in especially serious cases, online intercepts under section 100b and acoustic surveillance of private premises under section 100c. Cross-border investigations are frequently necessary and can be conducted effectively and rapidly by virtue of international mutual legal assistance, which in the EU especially is highly formalised and streamlined. The European investigation order (EIO) and the possibility of establishing joint investigation teams (JITs) are very helpful in this regard and frequent use is made of them. This primarily aids the coordination of criminal prosecution measures and international financial investigations.

The customs administration conducts frequent checks (such as cash checks at frontiers, airports and seaports) to prevent the smuggling of incriminated assets. This involves mobile control units as well as stationary controls. With regard to cash, the customs administration regularly trains control officials at all locations in the conduct of cash checks and consequently has qualified control staff in this area. In addition to technical aids (such as X-ray equipment), officials also make targeted use of cash sniffer dogs in their controls. Customs checks are subject as a matter of principle to the risk-based approach. This follows from the Union Customs Code (UCC) (Regulation (EU) No 952/2013). Article 46 (2) of the UCC thus stipulates that customs controls must primarily be based on risk analysis on the basis of criteria developed at national, Union and, where available, international level. For cross-border cash movements, this general approach under the UCC is supplemented by the stipulations of Regulation (EC) No 1889/2005 on controls of cash entering

or leaving the Community (the Cash Controls Regulation). These controls, too, are primarily based on a risk analysis in order to identify and assess the risks and develop necessary countermeasures. The provisions of Union law are supplemented and further elaborated by the Customs Administration Act (*Zollverwaltungsgesetz*) and in particular by various manuals. The risk-based control approach is consistently followed through here and further refined with local risk management. In this way, adequate account is taken of regional specificities while ensuring that identifiable trends are made known and acted upon across all regions. Regular exchange takes place at local level on a basis of trusting partnership between the relevant agencies, such as with the Bundespolizei (Federal Police).

The Act on the Processing of Passenger Name Record (PNR) Data to Implement Directive (EU) 2016/681 (Passenger Name Record Act – *Flugdatengesetz*) requires a passenger information unit (PIU) to be established at the Federal Criminal Police Office. The PIU processes passenger name record (PNR) data – sent by airlines – in a passenger data information system in order to prevent and counter terrorism offences and serious crime. To this end, the PIU matches the data against databases on persons and objects sought or under alert and against patterns. The purpose of this matching is to identify persons for whom there are factual indications that they have committed or will in the foreseeable future commit any of the offences – including terrorist financing and money laundering – listed in section 4 (1) of the Passenger Name Record Act. Subject to restrictions under the Passenger Name Record Act, the PIU may transfer information and intelligence to the following authorities for further examination or for suitable measures to be taken: the Federal Criminal Police Office, the state criminal police offices in the *Länder*, the Customs Administration, the Bundespolizei, the Federal Office for the Protection of the Constitution and its counterparts in the *Länder*, the Federal Armed Forces Counterintelligence Office and the Federal Intelligence Service. Data processing within the PIU is geared to a major extent to preventing future criminal offences and thus follows and supports the risk-based approach, including in the areas of anti-money laundering, preventing terrorism and countering terrorist financing.

The Federal Intelligence Service (Bundesnachrichtendienst) investigates and analyses foreign matters related to money laundering as part of its statutory mandate. Its ML-related activities are equally directed at gaining strategic and structural intelligence on specific large-scale money laundering networks. The Federal Intelligence Service also regularly analyses the enabling conditions for money laundering and identifies new money laundering methods, typologies and developments in international financial centres and offshore regions. The objective is to obtain intelligence on the present foreign threat situation with direct relevance to Germany.

Germany has capable and specialised agencies for the combat of money laundering, at both federal and *Länder* level. The Federal Government will continue to step up this work and to continuously improve the conditions to effectively combat money laundering. The resources needed are therefore to be increased on an ongoing basis (above and beyond staff positions already approved), in particular in the judiciary and security agencies. The Federal Government aims to further improve statistics in the areas of the judiciary, police authorities and customs for adequate assessment of the national risk situation. Greater use is to be made in future of the systematic evaluation and analysis of historical data for the detection of patterns and threat scenarios.

3.1.5.5 Confiscation of incriminated assets

Confiscation of incriminated assets is an extremely effective method of combating organised crime. Crime is often driven by the profit motive. Confiscating the proceeds of crime hits criminals where it hurts. There are several phases to the asset recovery process: investigation of assets, temporary freezing, final confiscation, disposal following final judgment and in some cases compensation of the victim or victims. Germany has sufficient scope to impose effective confiscation measures. A distinction is made between preventive confiscation and confiscation under criminal law.

A reform of criminal law asset recovery that entered into force on 1 July 2017 brought substantial amendments to the Criminal Code and the Code of Criminal Procedure. The amendments comprised a major overhaul of criminal law asset recovery. The law has notably been made more effective with regard to 'extended' and 'independent' confiscation. Freezing of assets is now mostly mandatory in investigation proceedings, whereas it was previously at the discretion of the prosecution service. 'Extended' confiscation under section 73 of the Criminal Code means that assets can still be confiscated even if they cannot be traced to a specific proven criminal offence. All that is required is another proven offence. Under the new law, this can be any offence (and not a specific predicate offence, as was the case previously).

Criminal law asset recovery is in principle possible for any criminal offence leading to the acquisition of proceeds. If property is secured because of suspicion of an offence listed in section 76a (4) sentence 3 of the Criminal Code (which includes money laundering), a court can order the property to be confiscated without proof of a specific criminal offence, provided that the court is convinced, in light of the overall circumstances, that the object constitutes the proceeds of an unlawful act (see section 76a (4) sentence 1 of the Criminal Code). That conviction is based on factors such as the party's personal and economic circumstances and any gross discrepancy between the value of the object and the party's legitimate income (section 437 of the Code of Criminal Procedure).

Property can also be temporarily secured for the purposes of averting dangers to the public. The legal basis for this is the federal and *Länder* police acts, section 12a (7) of the Customs Administration Act (*Zollverwaltungsgesetz*) and section 32b of the Customs Investigation Service Act.

Germany thus has a significantly improved legal framework overall. There are initial indications that the new provisions will in practice result in the increased use of temporary securing measures. Experience in the courts also shows that the instrument of asset recovery has become considerably more effective.

3.2 Terrorist financing risk situation

3.2.1 Terrorism threat

The terrorist threat has materialised in Germany in recent years as a result perpetrated acts of terrorism. It is currently still rated as a high abstract threat. The greatest terrorist threat potential is posed by Islamic terrorism, although right-wing and left-wing extremists also pose a terrorist threat for Germany. There were five Islamic terrorist attacks in Germany in 2016 alone, of which the most serious was the December 2016 attack in Berlin, which left 12 dead and over 50 injured; there was a further Islamic terrorist attack in 2017. The "Islamic State" (IS) terrorist organisation claimed responsibility for the attacks. In at least two cases, there were verifiable contacts between the attackers and

members of IS prior to the attacks. Additionally, there was a series of similar planned attacks that security agencies were able to frustrate ahead of time. There were no Islamic terrorist attacks in Germany in 2018. Plans for attacks uncovered at various stages of preparation nevertheless show that there is no reason to sound the all-clear.

The terrorist threat situation in Germany today is driven by Salafist ideologies and globally oriented jihadist groups. This primarily relates to further plans for Islamic terrorist attacks – both by simple means and of a more complex nature – mostly by individual actors not tied to an organisation, inspired by Jihadist ideology, frequently self-radicalised and acting alone or in very small groups ('individual jihad'), but also by 'hit teams' acting on behalf of globally operating Islamic terrorist groups such as IS and Al-Qaida.

Developments in states bordering on Europe are particularly important in this regard, notably in terms of those returning from crisis regions in Syria and Iraq and the possibility of members and proxies of terrorist organisations entering Germany under cover of migration.

Foreign terrorist fighters and women who have travelled out in the past are a particular focus. Individual, mostly very young Islamists, considering themselves called to become 'fighters', engage in both legal and criminal activities – going as far as preparing and carrying out attacks and travelling to the conflict zone – in order to finance their objectives. Fighters for crisis regions and (potential) terrorist attackers are recruited from the ranks of various Salafist groups, both larger and smaller, that operate in Germany. This mainly involves individuals from the sphere of Salafi mosque associations. Such groups also generate funds to support terrorist organisations by way, for example, of financial contributions for foreign terrorist fighters. While the so-called IS is almost defeated in military terms, Germany security agencies expect that international terrorist groups will continue to try and carry out attacks in Germany and across Europe. These organisations, and most of all the so-called IS, also operate continuously online to recruit potential individual attackers for terrorist attacks.

3.2.2 Terrorist financing risk assessment

Countering the financing of terrorism (CFT) involves far more than merely preventing terrorist attacks at home. International terrorist organisations also use Germany to recruit members and generate support or funds. While not all such organisations have active terrorism operations in Germany or structures of their own in the country, German authorities nevertheless take decisive action to combat them. The Federal Government considers CFT to be an integral part of combating international terrorism even though, in contrast to the situation with most other criminals, generating and moving funds is not the main motive for the crime.

On the basis of the methodology underlying this NRA, the threat of terrorist organisations engaging in financing activities in Germany has been rated as medium-high ('threat' meaning a certain potential to cause harm or a possibility of harm, in line with the FATF methodology). There are currently organisations active in Germany that have organisational structures of their own in the country as well as others that have an impact on the security situation without such structures. In this connection, it should be noted that terrorist organisations as a rule need most of their financial resources for establishing and maintaining their organisational structures (such as to establish organisational logistics and for propaganda and living expenses). In contrast, only small amounts are needed in many cases to carry out actual attacks.

There are currently no indications of systematic financing of left-wing extremist terrorism in Germany. The groups can essentially be categorised as follows:

- Jihadist groups without organisational structures of their own in Germany
- Foreign terrorist groups oriented towards their countries of origin with significant support circles in Germany
- Salafist groups in Germany
- Right-wing extremist or terrorist groups in Germany.

Regarding 'lone wolves' inspired, for example, by globally operating Islamic terrorist networks, it should be noted that individuals in this category are known in some cases to have been able to prepare and carry out terrorist acts with minimal funding. No significant financial resources are needed to carry out such attacks and there are no terrorist organisational structures to finance. Such attacks can nevertheless cause severe harm. With this form of terrorism, the severity of the potential harm resulting from attacks is significantly out of proportion with the possibility of detection from money flows. Likewise in present-day threat situations with regard to right-wing extremism, the potential attacker profile is generally considered a lone wolf or member of a very small group. No such terrorist organisations of major significance – comparable to the "National Socialist Underground" (NSU) – have been identified in recent years. Thus in the area of right-wing terrorism, too, there is not always a need for relatively large sums of money for terrorists to achieve their objectives.

Fundraising can involve both illegal and legal sources. Personal funding (such as earned income, benefits and savings) is frequently a very substantial legal source of financing for acts of terrorism. Investment in real estate and businesses (such as in catering) would also appear a potential way of ensuring sustained flows of money in order to consolidate structures for the long term. Sources of funding observed in the past have been family support (in connection, for example, with individuals travelling to foreign conflict zones and joining terrorist organisations there) and borrowing.

In some cases, foreign terrorist groups use their diaspora or sympathisers living in Germany to generate donations in order to fund their structures and activities. As well as the covert collection of donations for manifest terrorists, individual organisations based in Germany – mostly registered associations – have collected donations for purportedly humanitarian purposes where the donations have then indirectly benefited terrorist groups. In light of this, the Federal Government is currently carrying out a separate sectoral risk assessment on the non-profit sector. Donations in kind can also play an important role. Activities observed have notably included the collection of clothing, medical drugs and military equipment, and also of vehicles. Another possibility is the funding of terrorist ambitions by other countries, at least for the establishment of structures that promote the radicalisation of individuals.

Detected sources of illegal funds for terrorist financing have included theft, burglary, robbery, handling stolen goods, drug trafficking and offences relating to benefit, insurance, internet and tax fraud. There is at least a theoretical possibility of funds being generated by trading on the stock exchange (using derivatives, for example) to speculate on price movements connected to specific attacks by the organisation concerned.

3.2.3 Cross-border channels

Fund raising for terrorist purposes often takes place at a distant geographic remove from where the organisations concerned actually operate. While it is

frequently impossible to avoid using the established banking system for donations, terrorists often seek channels, when it comes to forwarding the sums collected, that leave as few traces as possible and provide security agencies with few clues as to where the money ends up. Frequently, different methods are combined into hybrid forms of global money transfer. Another known method is the smuggling and subsequent sale of tangible assets.

Islamic terrorism continues to make substantial use of informal money and value transfer systems such as hawala. All money or value transfer services (MVTSs) harbour risks with regard to terrorist financing. Hawala and other informal money and value transfer systems pose a particular threat, however. Informal money and value transfer systems are services that typically operate outside of the traditional financial sector and provide money or value transfer over long distances. Such transfer arrangements are usually based on an established relationship of trust (such as on the basis of ethnicity) or develop in regions where the banking system is rudimentary. The best-known form of informal transfer arrangement is hawala. While it is often used for legitimate purposes, this system can also provide a way for terrorist organisations to transfer funds with practically no means of tracing them. The money to be transferred is accepted by a hawala broker, or *hawaladar*, for a fee (usually about 0.5-5%). The customer is given a password that they communicate to the recipient at the destination, where another *hawaladar* pays the money to the recipient in return for being told the password. Brokers settle up using couriers, settlement accounts or payment in goods (such as vehicle exports). Hawala often involves a fairly large network of people whose transfers are hard to trace as there is little documentation or other evidence. The security agencies involved in the National Risk Assessment estimate that about US$200 billion are transferred by such systems worldwide every year. The great bulk of these funds, however, can be assumed not to be destined for terrorist financing. In Germany, the operation of MVTSs requires a licence. Unlawful operation is prohibited by BaFin and is also a criminal offence.

Cross-border cash transport by couriers is another way for terrorists to launder funds past the surveillance mechanisms built into the conventional financial system. Increased use is made in this context of organised crime (notably in Eastern Europe) with its established networks for cash transfer. It should be borne in mind that the term ‘courier’ covers several situations. On the one hand, there are professional couriers who carefully prepare their assignments and are paid for their services. Use is also made, however of casual couriers who, for example, bring money over when travelling on business. This is a tactic that is known to have been deployed by PKK sympathisers. Occasional use is made of ‘jihadi volunteers’ who visit a terror camp and have to pay several thousand dollars for admission. There are also cash couriers who are unaware that they are supporting a terrorist group. These are frequently people with regular employment abroad who visit their families in the target country. They mostly travel with money from foundations or private donors that, on arrival, is channelled to the terrorist organisation concerned.

The legal financial system is also known to have been misused for terrorist financing. Larger sums in particular are frequently transferred through the conventional financial system. Security agencies have observed in this connection how sums of money have been transferred abroad for terrorist purposes using money or value transfer services (see section 4.4). The security agencies share the concern that, given the large number of agents in the DNFBP sector in Germany, a number of individuals could have applied for employment with large undertakings in order, by suitable manipulation, to transfer money – ostensibly legally – for recipients from the terrorist scene.

The deliberate use of putative non-profit organisations (NPOs) under the control of terrorist organisations and the misuse of legitimate NPOs are another means of internationally transferring funds (see note with regard to sectoral risk assessment in section 3.1.4). Over or under-invoicing by businesses is a further potential method of terrorist financing.

3.2.4 National defence mechanisms and responsibilities in terrorist financing

Combating terrorism is a top priority for Germany. A key part of this is preventing, halting and sanctioning financing activities.

3.2.4.1 Terrorist financing prevention

In the Money Laundering Act, the German lawmakers have created an extremely effective legal framework for the prevention of terrorist financing (see section 2.2). Compliance with its requirements is ensured for the financial sector by BaFin and for the DNFBP sector by other supervisory authorities (see section 3.1.5.2).

The supervisory authority for the financial sector under the Money Laundering Act is BaFin. Its powers under the Money Laundering Act are supplemented with regard to the regulation of credit institutions by section 6a of the Banking Act (*Kreditwesengesetz*). Under the Banking Act, BaFin can, among other things, order deposits to be frozen if there are sufficient grounds for suspicion that they serve – or would serve if a financial transaction were to be carried out – the purpose of terrorist financing under section 89 of the Criminal Code or of the financing of a terrorist organisation under section 129a, including when read in conjunction with section 129b of the Criminal Code. Section 27 (2) of the Payment Services Supervision Act and section 6 of the Investment Code extend these powers to entities regulated under that legislation.

Movements of cash and cash equivalents across borders – whether third country or EU borders – are supervised by the customs administration under section 1 (4) of the Customs Administration Act read in conjunction with Regulation (EC) No 1889/2005 (see section 3.1.5.4). Where there is reason to believe that cash or cash equivalents are being moved across borders for terrorist financing purposes, customs administration control units can seize them and place them in customs custody through to the end of the fifth business day following their discovery in order to ascertain their origin or intended use. When there are indications of terrorist financing, the clearing process to ascertain origin and intended use is carried out by the customs investigation service. The temporary seizure period may be extended once for up to three months by decision of the competent court at the application of the customs investigation service.

It should be noted that a special feature of cash controls in connection with terrorist financing is that in many cases, transported cash proves to be not incriminated, meaning not associated with a criminal offence. In such cases, therefore, the legal origin (such as earned income or savings) is capable of being traced. Also, the amount carried is frequently (in some cases significantly) less than €10,000 and so does not normally have to be declared on entering or leaving Germany. These facts mean that as a rule, in addition to the amount itself (such as sum total, denominations and alleged origin), controls also have to consider other indications that money is being carried for the purposes of terrorist financing.

Such indications include:

- Unusual itinerary
- Luggage not matching destination/ duration of travel
- Items carried (such as outdoor equipment or large quantities of medical drugs)
- Prior knowledge about the individual.

The Federal Government is also committed to the prevention of extremism and early deradicalisation of individuals who could potentially be later drawn into terrorism. It has supported programmes and measures for the prevention of extremism since as early as 1992. This work also deprives terrorist organisations of their support base and makes it far harder to generate funds. Numerous initiatives, associations and highly committed individuals throughout Germany work every day for diverse, peaceful and democratic coexistence. They are supported in this work by the federal "Demokratie leben!" ("Live Democracy!") programme under the Federal Ministry of Family Affairs, Senior Citizens, Women and Youth (BMFSFJ). This programme operates at various levels. It funds projects for the prevention of radicalisation and promotion of democracy with local, regional and supraregional focus and supports associations, projects and initiatives that are dedicated to promoting democracy and diversity and work to counter right-wing extremism, racism, antisemitism, Islamic extremism, left-wing militancy, other forms of antidemocracy and inhumanity, violence, hatred and radicalisation.

The programme was launched in January 2015. The funding for 2019 totals €115.5 million. From 2020, the programme's objectives are to be readjusted and given clearer focus, primarily with a view to current social challenges and on the basis of experience to date. It thus remains a central pillar of and continues to pursue the objectives of the Federal Government Strategy to Prevent Extremism and Promote Democracy presented in 2016. Promoting democracy, shaping diversity and preventing extremism are to be guiding principles as the new core objectives of "Demokratie leben!".

Under the Federal Government Strategy to Prevent Extremism and Promote Democracy and in coordination with the Federal Government Commissioner for the New *Länder*, the Federal Ministry of the Interior, Building and the Community (BMI) supports prevention and democracy work in Germany via the federal programme "Zusammenhalt durch Teilhabe" ("Cohesion through Participation"). A prevention network has become established throughout Germany in close cooperation with the Federal Agency for Civic Education, the Federal Anti-Discrimination Agency, *Länder* democracy centres, local authorities and civil society actors.

Along similar lines to the Strategy to Prevent Extremism and Promote Democracy, but in a separate programme, additional funding has been made available since 2018, primarily through BMFSFJ and BMI, under the National Prevention Programme (NPP) against Islamic Extremism. The funding amounts to €100 million a year in 2018 and 2019. It is used to fund field and research projects that further develop existing approaches or develop new or additional provision.

Structures central to deradicalisation work include those resulting from the Deradicalisation working group established in 2009 under the Joint Counter-Terrorism Centre (GTAZ). The main player at federal level is the Radicalisation counselling centre, which was based on a proposal from the Deradicalisation working group and established by order of BMI in 2011 under the Federal Office for Migration and Refugees (BAMF). Since 2012, the counselling centre has provided a hotline for initial counselling of people close to (presumed) radicalised individuals. Any further need for

counselling is provided in partner counselling centres all over Germany. Local provision structures and authorities (mostly the *Länder*) also work with (presumed) radicalised individuals themselves to support a deradicalisation process.

BAMF provides platforms for regular interaction between the partner counselling centres. The BAMF counselling centre also serves as a point of contact and coordinating body for public (security) agencies at federal, *Länder* and local authority level, civil society providers and other interested stakeholders in Germany and abroad. The work of the counselling centre was placed on a permanent basis in 2017. Since 2018, the BAMF Research Centre has undertaken ongoing academic evaluation to further optimise the work and provide quality assurance. In 2019, leadership of the Deradicalisation working group, which provides forums for the relevant federal and *Länder* agencies, was transferred from the Federal Office for the Protection of the Constitution to BAMF. BAMF is consequently the central liaison body in this thematic area and work area, in close consultation with BMI.

3.2.4.2 Financial sanctions

Listing organisations and individuals in an international counter-terrorism sanctions regime is a preventive measure against terrorist activities. Financial sanctions are governed by directly applicable Union law. Deutsche Bundesbank is the national competent authority for implementation of EU financial sanctions, including Council Regulations (EC) No 2580/2001 (combating terrorism) and (EC) No 881/2002 (measures against ISIL/Da'esh and Al-Qaida). The Bundesbank is listed as competent authority in the annexes to the EU financial sanctions regulations.

In national law, a mandate to monitor compliance with acts of the Council or the European Commission in the field of foreign trade and payments legislation is contained in section 23 of the Foreign Trade and Payments Act. Under section 23 (2) of that Act, the Bundesbank conducts examinations on the premises of financial undertakings, credit institutions, financial services companies, asset management companies and insurers to monitor compliance with financial sanctions and foreign trade and payments reporting provisions. Responsibility for this lies with the Bundesbank's four Service Centres (SCs) for External Sector Audits. About 100 examinations are conducted each year. Any suspected violation of sanction provisions is immediately notified to the competent prosecution service or main customs office.

In cases where financial sanctions involve licensing or reporting obligations, the responsibilities assigned to the Bundesbank are discharged by the SC for External Sector Audits in Munich. This SC is also the contact point for businesses and private individuals concerning questions about the application and interpretation of EU financial sanctions. In fundamental issues, the SC liaises with the Federal Government through Bundesbank Central Office. Coordination with other competent departments within the Federal Government is the responsibility of the Federal Ministry for Economic Affairs and Energy (BMWi). Statistical reports and notifications are also passed on to BMWi in accordance with the respective financial sanction regimes.

In the implementation of financial sanctions against terrorism, the Financial Sanctions SC mostly acts in connection with notification procedures. If monies or economic resources (such as benefits following release from prison) have to be provided to persons sanctioned by the UN for participation in or support of terrorist activities, the Financial Sanctions SC prepares the notification and, if necessary, the obtaining of approval from the competent UN committee. The notes are submitted by the Permanent Mission of the Federal

Republic of Germany to the United Nations. When exemptions are authorised from counter-terrorism financial sanctions imposed autonomously by the EU, a notification procedure may be required in order to notify the other Member States and the European Commission. The Bundesbank informs credit institutions based in Germany about new developments concerning financial sanctions (such as measures against persons or organisations connected with terrorism) in a circular in which it also requires them to report frozen funds.

The National Risk Assessment has revealed a lack of clarity and awareness as to responsibilities for enforcing prohibitions on the disposal of frozen movable assets (primarily cash, precious stones and precious metals) and immovable assets (mostly real estate). In addition, the procedures for collecting and collating information about frozen economic resources (real estate or movable assets of value not intended for personal use) and frozen cash are not specified in sufficient detail. As an initial step, the Federal Government will therefore raise awareness among the authorities concerned with regard to the possibilities in this problem area and monitor the results. If awareness raising proves not to be enough, other measures are to be explored having due regard to effectiveness considerations. These could include, for example, establishing a central body with nationwide responsibility for identifying and tracking down the property of listed persons.

3.2.4.3 Suspicious transaction reporting with regard to terrorist financing

The FIU is the central national unit for the receipt, collection and analysis of suspicious transaction reports (STRs) that may be related to ML or TF (see also section 3.1.5.3). Like all incoming STRs, terrorism-related STRs undergo automated basic screening as soon as they are received by the FIU. All terrorism-related STRs are also passed up for information purposes, immediately after receipt, to the Federal Office for the Protection of the Constitution. On the basis of its professional judgement, the latter passes the STRs on to any potentially affected *Länder* offices for the protection of the constitution. If matters are submitted that are of relevance to national security, the FIU sends the operational analysis and all relevant information to the competent law enforcement agency (state security division in the case of the state criminal police office of one of the *Länder*, or prosecution service). The same information is also sent to the Federal Intelligence Service (BND). If the FIU orders a terrorism-related STR to be sent on to the Federal Office for the Protection of the Constitution, the FIU also provides the latter with the findings of the operational analysis and all relevant information.

Close and ongoing information exchange between authorities is imperative in day-to-day national security work and is an integral and core element of the national security architecture. The FIU maintains intensive contact with the German police authorities and intelligence services. Relevant intelligence on specific persons or matters is exchanged in connection with mutual requests between the investigating authorities and intelligence services. The FIU cooperates constructively and intensively, both on a case-by-case basis and independently of specific cases, with the state criminal police offices in the *Länder* and other relevant security agencies.

Business entities often find it challenging in practice to identify suspicious transactions in relation to terrorist financing. This has been confirmed in the many discussions with representatives of the private sector. To detect incriminated transactions, credit institutions, for example, use ‘red flags’ (such as names of senders and recipients) in their monitoring systems and match transactions against

sanction lists. Terrorist financing often transpires in practice to involve very small monetary amounts that easily fall through the gaps as evidence. In light of this, in collaboration between all competent authorities, regularly updated terrorist financing typologies should be compiled to further improve the information at the disposal of obliged entities.

3.2.4.4 Counter-terrorism financing activities of German security agencies

In Germany's federal system, prosecution services and police authorities at both federal and *Länder* level are involved in combating terrorism. Criminal prosecution for terrorism offences and hence also for terrorist financing is effectively dealt with in collaboration between federal and *Länder* prosecution services. The Federal Public Prosecutor General at the Federal Court of Justice is the specialist federal prosecution service for the prosecution of terrorism offences under criminal prosecution powers assigned by law (section 142a read in conjunction with section 120 of the Courts Constitution Act (*Gerichtsverfassungsgesetz*)). It has primary responsibility for criminal prosecution in the case of crimes related to terrorist financing where the terrorist financing constitutes a criminal offence under section 129a or 129b of the Criminal Code. In accordance with section 142a (2) of the Courts Constitution Act, it may refer initiated investigation proceedings to *Länder* prosecution services in cases of lesser importance (section 142a (2) no. 2 of the Courts Constitution Act). Conversely, the Federal Public Prosecutor General may take over investigation proceedings into offences under section 89c of the Criminal Code or section 18 of the Foreign Trade and Payments Act, for which criminal prosecution is normally the responsibility of *Länder* prosecution services, if the Federal Public Prosecutor General deems them to be of special importance (section 142a (1) of the Courts Constitution Act).

With regard to police authorities, the Federal Criminal Police Office is the national central office of the German police within Germany's federal system. The Federal Criminal Police Office is also responsible for international cooperation and in certain cases discharges police responsibilities in criminal prosecution. The State Security Division of the Federal Criminal Police Office, which is responsible among other things for combating international terrorism, is paralleled by virtually identical organisational structures in the state criminal police office of each of the *Länder*. The latter in turn preside over police units around the country, which are likewise responsible for various measures against terrorist activities. The state criminal police offices and the Federal Criminal Police Office exchange police information on a regular and standardised basis as part of the criminal police reporting service. This is also used to exchange information on all investigation proceedings relevant to national security and to give notice of any financial investigations being carried out. There are also various shared databases in which both the Federal Criminal Police Office and all competent *Länder* police authorities store and provide mutual access to relevant national security intelligence.

In the investigation of international terrorism, the Federal Intelligence Service, the Federal Office for the Protection of the Constitution, the *Länder* intelligence services and the *Länder* offices for the protection of the constitution also generate important intelligence on aspects of terrorist financing and so help combat it. The information generated in this way is made available as reports and oral briefings to the various public agencies and ministries within their respective remit (at federal level the Federal Chancellery, the Federal Ministry of Finance, the Federal Ministry of the Interior, Building and the Community, the Federal Ministry of Justice and Consumer Protection and the Federal Ministry for Economic Affairs and Energy and the Federal Foreign Office, and at

Länder level the competent *Länder* ministries of and senate administrations for internal affairs). The Federal Criminal Police Office, the Federal Office for the Protection of the Constitution and the Federal Intelligence Service also regularly compile a joint situation report on terrorist financing.

To ensure comprehensive information exchange between the *Länder* and the Federal Government, the Joint Counter-Terrorism Centre (GTAZ) has been set up in Berlin (for Islamist-motivated terrorism) and the Joint Centre for Combating Extremism and Terrorism (GETZ) in Cologne (for other extremist and terrorist phenomena). The participating agencies are – besides the Federal Criminal Police Office – all 16 *Länder* offices for the protection of the constitution, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the Federal Armed Forces Counterintelligence Office, the Federal Office for Migration and Refugees (BAMF), the Bundespolizei (Federal Police), the Federal Public Prosecutor General at the Federal Court of Justice and the Customs Criminological Office. Representatives of all these agencies exchange current intelligence here on a day-to-day basis within the scope of prevailing law. Focal areas comprise optimising information flows, intensifying inter-agency cooperation, pooling knowledge on terrorist phenomena, strengthening analytical capabilities, early detection of potential threats and discussing and implementing operational measures. Intelligence from foreign services is also fed in via the German intelligence services. As the Customs Criminological Office is likewise represented in the Joint Counter-Terrorism Centre, it is possible for particularly significant suspected cases to be brought up with the FIU and an FIU representative to be included in a case meeting.

The established division of responsibilities between the Federal Public Prosecutor General at the Federal Court of Justice and *Länder* prosecution services ensures full and efficient criminal prosecution with regard to terrorist financing. Since 2017, all *Länder* have established 'state security centres' at the level of prosecutor general offices to centrally conduct, coordinate or support investigation proceedings into suspected terrorism offences and in particular alleged offences under section 89c of the Criminal Code. This pooling of competencies ensures that cases relating to terrorist financing are detected, investigated and where necessary submitted for review with a view to being taken over by the Federal Public Prosecutor General at the Federal Court of Justice.

Law enforcement agencies also cooperate closely and intensively at international level. In view of transnational links between terrorist offenders, cooperation at European level has been continuously intensified, with a pivotal role played by the Eurojust judicial cooperation unit established in 2002. Eurojust's mission is to stimulate and improve coordination and cooperation between national judicial authorities in the investigation and prosecution of severe cross-border crime in the European Union. On several occasions, joint investigation teams (JITs) have been set up between Eurojust and other EU Member States. The resulting possibility of exchanging intelligence without formal requests for mutual legal assistance and of more easily coordinating the course of investigations proves to be a major advantage in such cross-border cases.

The Federal Public Prosecutor General at the Federal Court of Justice also maintains a dedicated contact point in the European Judicial Network (EJN). Established in 1998, the EJN is a network of contact points in each of the EU Member States that aims to facilitate judicial cooperation in criminal matters and notably the better processing of mutual legal assistance requests. There is also diverse bilateral cooperation, primarily with EU Member States.

Organisational units specialised in financial investigations in relation to politically motivated crime are implemented in the organisational structures serving national security, both at the Federal Criminal Police Office and at the criminal police offices of the *Länder*. The financial investigations are divided between clearing up STRs and (frequently resultant) investigation proceedings. With regard to money laundering, it is ensured in accordance with the Fourth EU Money Laundering Directive that all STRs received by the FIU are matched against police data. STRs rated relevant by the FIU are passed on to and further processed by the competent law enforcement agencies in the individual *Länder*.

On transposition of the fourth EU Money Laundering Directive into national law, the Federal Office for the Protection of the Constitution and the Federal Intelligence Service were also provided with the capability of obtaining more comprehensive information from STRs. The new Money Laundering Act thus stipulates that STRs are to be transmitted without delay to the Federal Office for the Protection of the Constitution where there are factual indications that transmission of the information is necessary for that agency to perform its functions. Further to each transmitted STR, the Federal Office for the Protection of the Constitution must also be sent the findings of the corresponding operational analysis together with all relevant information. The same applies for transmission to the Federal Intelligence Service where there are factual indications that the transmission of the information is necessary for that agency to perform its functions. Section 32 (3) of the new Money Laundering Act also created the legal basis for the Federal Office for the Protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counterintelligence Office (BAMAD) themselves – in addition to the law enforcement agencies – to make intelligence requests to the FIU subject to requirements detailed in that section of the Act. Under section 34 of the Money Laundering Act, the FIU additionally has the possibility of making international information requests to other FIUs for the performance of its responsibilities.

An increasing focus of investigations comprises potential crossover points between terrorism and organised crime. This increases the demands with regard to inter-agency information exchange. It also calls for greater inner-agency coordination. The Federal Government will provide ongoing support for such forms of cooperation to continue in order, for example, to effectively prevent organised clan crime from operating in concert with foreign terrorist organisations.

Both the Federal Government and the *Länder* have created large numbers of new staffing positions in response to continually rising case numbers in the fight against terrorist offences and the resulting increased involvement of *Länder* authorities. They plan to continue in the same direction. In addition, the Federal Government will also further improve statistics on terrorist financing in the areas of the judiciary, police authorities and customs. The statistics are also to be adapted to the needs of effectively countering the financing of terrorism.

4 Financial sector

4 Financial sector

The National Risk Assessment addresses the financial sector and the designated non-financial businesses and professions (DNFBP) sector as subsectors of the German economy. For this purpose, the financial sector comprises banking, insurance, securities and financial and payment services. The analysis focused on the threat situation and the vulnerability of products in each subsector.[17] A dedicated presentation of the risk rating was also produced for the banking and insurance sector. Detailed information on the national threat situation is provided in section 3. Inherent ML/TF risk in financial sector institutions was initially assessed and rated against general and specific risk factors. General risk factors are risks resulting from the customer base, products and services, sales channels or corporate structure. An institution's inherent risk is also affected by its geographic location. Specific individual factors can additionally be distinguished that capture certain attributes of a general risk factor in more specific terms, such as the number of politically exposed persons or high-risk customers in the customer base. The individual assessments were subsequently matched against the self-assessments of the institutions themselves following private-sector consultation, and aggregated into an overall rating.

4.1 Banking sector

4.1.1 Overview of the German banking sector

Knowledge of the special features of the German banking sector from an international perspective is of great importance to understanding the present assessment.

The German banking system is divided into specialised and universal banks. Specialist credit institutions typically limit their activities to selected areas of banking business as listed in section 1 (1) of the Banking Act (*Kreditwesengesetz*) and in many cases are affiliated with a universal bank. Specialised banks include mortgage banks, building and loan associations, institutions with special functions and other institutions with specialised services. Where activities are restricted to specific areas, the risk of being misused for ML/TF purposes is commensurately smaller. Conversely, universal banks are credit institutions that operate in many of the areas of the banking business listed in section 1 (1) of the Banking Act, with conventional deposit-financed lending as the core business. These banks are often better able than highly specialised banks to offset multiple kinds of risks in specific business areas. The German banking sector is dominated by universal banks. Germany's system of universal banks thus differs from the system of ring-fenced/specialised banks in English-speaking countries where a traditional distinction is upheld between investment banking and commercial banking.

Another major difference from other international banking systems is Germany's high bank density. While this has continuously decreased in recent years, the German banking sector still has a very large number of legally independent banks compared with other countries. According to Deutsche Bundesbank banking statistics, a total of 1,823[18] banks were in operation in Germany at the end of 2017. This means over two banks per 100,000 population, compared with less than

17 The assessment covers products, services and sales channels. For the sake of simplicity, the word 'products' is exclusively used from now onwards. This includes products, services and sales channels.

18 See Deutsche Bundesbank, Banking Statistics July 2019, p. 104.

one in France. It should be noted, however, that in contrast to most European countries, almost three-quarters of German banks are decentralised regional savings banks (390 institutions) and credit cooperatives (918).[19] These are mostly local universal banks with limited regional market focus and size. Because of their regional focus, these affiliated credit institutions have particularly extensive knowledge of the risk situation in their market and client environment.

German banks also vary considerably in size. Alongside the major banks, which usually operate internationally,there are a large number of small to medium sized banks. Savings banks and cooperative banks account for only a quarter of the aggregated balance sheet totals of all banks. In contrast, the five biggest banks account for more than a third of the entire banking sector in terms of balance sheet total.[20]

For statistical reporting purposes, the Deutsche Bundesbank statistics divide the German banking sector into categories of banks with a summary distinction between private-sector, public-sector and cooperative credit institutions. These three pillars of the German banking sector differ with regard to their objectives, liability arrangements and numbers of legally independent institutions. Whereas private-sector commercial banks are primarily profit-driven, the focus in the other two pillars is on fulfilling specific (assistance) tasks.

In accordance with section 2 (1) no. 1 of the Money Laundering Act, the subject of analysis in the following consists of credit institutions as defined in section 1 (1) of the Banking Act, with the exception of the entities specified in section 2 (1) nos. 3 to 8 of the Banking Act, and German branches (*Zweigstellen*) and branch offices (*Zweigniederlassungen*) of credit institutions domiciled abroad. The analysis is essentially based on the bank categories used in the Deutsche Bundesbank banking statistics.

19 See Deutsche Bundesbank, Banking Statistics July 2019, p. 104.
20 See Deutsche Bundesbank, Banking Statistics July 2019, p. 106.

4.1.2 Risk situation of the banking sector as a whole

As financial intermediaries, German banks are highly important to the German economy overall due to their transformation functions for business and their international interconnectedness. Large turnover volumes and the sector's natural focus on asset management and transfer mean that the banking sector as a whole continues to be exposed to high risk of money laundering offences. The threat of the banking sector as a whole being misused for terrorist financing is rated as medium-high. No rising or falling trend is seen in this connection. It should be noted here, however, that large, internationally active banks in particular have high inherent risk due to their diverse product range, large business volumes and international interconnectedness.

The analysis has shown that money laundering and terrorist financing frequently continue to depend on cash. Cash transactions are consequently a regular subject of STRs and investigations in the banking sector as elsewhere. Another key factor here is the money or value transfer service (MVTS) business that is also conducted by banks and involves high risks, particularly in the case of cash transactions with an international dimension and payments outside of an existing business relationship. With money or value transfers to high-risk jurisdictions, there is also always the possibility of payments being used in connection with terrorist financing.[21] BaFin has recently placed a focus on monitoring compliance with AML/CFT obligations by MVTS providers in the banking sector.

The analysis differentiated between the national and the international threat. The home threat is rated medium-high and the foreign threat is rated high. International financial flows pose a prominent risk due to the global interconnectedness of the German economy. In foreign transfers, Germany

21 See section 4.4 for further detail.

is notably exposed to an international threat due to correspondent banking business. The risk depends among other things on the jurisdiction in which a bank is domiciled. Correspondent banks are frequently used as a channel to disguise payments to offshore jurisdictions. In light of the high inherent risk, correspondent banking relationships are to be subjected to enhanced due diligence requirements. It should be noted here that correspondent banking business in Germany is generally only conducted by big, globally operating banks and by banks with foreign interests. The bulk of smaller and medium-sized regionally focused banks do not have correspondent banking relationships. Correspondent banking services are also important in domestic transfers. In the savings banks and cooperative banks category, transfers are usually first cleared within the sector through correspondent bank accounts with the respective central institution. A number of other banks also participate indirectly in wire transfer systems via large institutions as part of correspondent banking in order to reap price advantages from economies of scale. As a result, international transfers frequently involve multiple intermediate steps. This sometimes leads to situations in which the payer and payee are not known to the correspondent banks as customers; in such cases the correspondent banks have to rely on prior input from the downstream banks for any identity verification. Correspondent banking relationships also enable banks to offer financial services for countries where they have no banking licences or branches of their own. Banks in developing countries in particular frequently depend on correspondent banking relationships in order to carry out international transfers and obtain access to major financial markets such as the US dollar and euro foreign exchange markets.

The total number of German banks' correspondent banking relationships is estimated to have declined by over one third since 2014. This is mainly due to de-risking measures by many major banks in recent years, such as terminating correspondent banking relationships with high-risk jurisdictions, and to cost-efficiency considerations. While this trend has led, on the one hand, to lower risk in correspondent banking, it has, on the other hand, caused a partial migration to MVTS, including unlicensed money transfer in the form of hawala banking. This makes it harder to trace incriminated funds.

BaFin focuses primarily on the general requirements for correspondent banking relationships and does not normally monitor individual transactions. In this connection, the fact that the law with regard to money laundering is not fully harmonised in relation to correspondent banking poses a challenge for supervisory authorities in Europe. The fact that, in some cases, implementation and supervision diverge significantly among EU Member States opens the door in principle to supervisory arbitrage with regard to cross-border correspondent banking. A further difficulty is that the major money laundering scandals in recent years have involved cross-border transactions or business relationships, and combined with the fact that supervisory authorities and law enforcement agencies especially only have a national remit, this has frequently resulted in failure to detect and investigate problem cases in a timely manner. Further harmonisation of AML requirements may be useful here. BaFin is nevertheless in ongoing exchange on such matters with the competent German law enforcement agencies, the FIU and various foreign supervisory authorities. A focus of BaFin's supervisory activities in 2019 will be on reviewing the AML requirements for correspondent banking among internationally active banks. Likewise, the FIU will in future place special focus on STRs relating to correspondent banking transactions.

The National Risk Assessment has also shown that increased inbound foreign investment, notably in corporate shareholdings and real estate, constitutes a large threat in relation to ML and TF. In certain

risk sectors such as real estate[22], which generally involves high ML risk, there are geographical regions where the risk is particularly high. The general risk situation of banks in relation to the real estate sector is thus normally higher in the urban than in the rural context. Banks in border regions also tend to show heightened ML/TF risk.

The analysis has also confirmed the general trend towards a cultural change in banking. Digitalisation and acceleration of bank processes and workflows confront banks with new challenges, including with regard to ML/TF prevention. Shorter processing times and faster payment processing, and especially instant payment, together with certain online transaction forms and new payment methods pose a threat to adequate prevention measures. There are also new risks in this context as a result of innovative business models and new technologies from fintech companies. Banks are also entering into collaborations with fintechs, some of which do not require a licence from BaFin.[23] Services, products and assets that favour anonymity, particularly in connection with crypto assets, also create new opportunities for ML and TF.[24] BaFin has established a competence centre on fintechs in the banking sector and monitors compliance with AML requirements, for example with on-site inspections. Inter-agency information sharing on emerging developments helps ensure effective supervision.

However, the private-sector consultation in particular also showed that innovative technologies can also provide opportunities with regard to ML/TF risk management. Potential application areas in this regard could include monitoring and STR processing. An algorithm could be used to generate smaller numbers of false positives, enable rapid, real-time processing and thus ensure more effective monitoring and suspicious transaction reporting. According to the banks, however, no market-ready solutions are yet available. The supervisory authorities likewise regard this trend as an opportunity and will develop a corresponding framework.

The private-sector consultation also clearly showed that all bank categories have difficulties in applying CFT due diligence requirements. For most banks, it is not entirely clear how specific cases of terrorist financing can be identified in ex-ante assessment. A key measure is that of screening customer lists against published sanction lists. Due to the poor quality of the sanction lists, however, the useful output from such screening is not proportionate to the effort involved. The banks therefore report a need for more specific information and typologies from the competent authorities in order, in particular, to be able to identify TF organisational structures and generate corresponding STRs. In the course of work on the National Risk Assessment, the competent authorities advocated the compilation of a typology paper for this purpose.

Due to exercise of intervention powers by BaFin and the law enforcement agencies, the total number of STRs in the banking sector is large. With 65,132 STRs, credit institutions continue to generate over 80% of the total. The total number of SARs has grown elevenfold since 2008.[25] Continuous, mutual information exchange is a key precondition for a successful suspicious transaction reporting system. A further part of this is the fact that the FIU, in accordance with section 41 (2) of the Money Laundering Act, provides feedback on relevance, content and quality of incoming STRs within a reasonable time. In light of this, the FIU has developed a framework under which it provides obliged entities with feedback in aggregated form on the content and quality of generated STRs (feedback reports). Obliged entities are provided with comprehensive guidance on the FIU website to support them in the registration and reporting process so that they can comply with their statutory duty to submit STRs. By means of the guidance on the use of goAML, the FIU informs obliged entities

22 See section 5.1 for further detail.
23 See section 4.6 for further detail.
24 See section 6 for further detail.
25 See FIU, Jahresbericht 2018 (Annual Report 2018), p. 14.

about its form and content requirements for proper electronic submission of STRs. The FIU will continue to refine and improve this feedback system.

Information exchange has been increased in recent years, both between public agencies and with the private sector. This exchange is to be further intensified on the basis of the positive feedback in the course of the work on the National Risk Assessment. Exchange on innovative technologies and new methods of money laundering and terrorist financing is particularly important in this connection.

Product vulnerability for the banking sector as a whole is rated as medium-high. It should be noted that this rating is primarily accounted for by large, internationally active banks and banks with foreign interests. For small and medium-sized banks, primarily in affiliated credit institutions and other credit institutions categories, product vulnerability is rated as medium. Sector-specific features are presented in the sections that follow.

With regard to the banking sector as a whole, the quality and effectiveness of general ML controls can be said to be adequate. In the Money Laundering Act and the Banking Act, Germany has a comprehensive and adequate legal and regulatory framework of preventive and supervisory measures for the prevention of ML/TF in the banking sector. The obligations on obliged entities under the Money Laundering Act are to be added to in the Banking Act in order to take account of the special features of the credit institutions subject to supervision.

Overall, the legislation is implemented effectively using the risk-based approach and on the basis of adequate powers and sufficient resources. The quality and effectiveness of supervisory procedures and practices have been continually improved in recent years. Banks are required to submit the audit reports on the audits of their annual financial statements to the Supervisory Authority. These reports provide the basis for supervisory activities applying the risk-based approach. Evaluation of the reports enables the Supervisory Authority to address deficits at individual entities on a targeted basis and require the entities concerned to remedy the findings. Evaluation of the reports also provides a basis for the risk classification of supervised institutions, in which the inherent risks are matched against the quality of preventive measures taken by the institutions themselves.

To further operationalise the risk-based approach, BaFin restructured its Prevention of Money Laundering Directorate as of 1 January 2017 with the establishment of two new divisions focused on the conduct of inspections by in-house personnel and on the supervision of institutions that are subject to intensified supervision. This new structural concentration and enhanced focus on inspection brought together expertise in ML/TF prevention and also generated synergies. BaFin itself carries out narrow-scope inspections for in-depth examination of specific focal areas according to the institution's specific risk situation. Inspection planning in this connection is a core element of the risk-based supervisory approach. BaFin conducted 31 on-site inspections in 2017 and 90 in 2018. Initial experience from the on-site inspections conducted by BaFin itself presents a positive picture. The BaFin inspectors were able to gain their own impressions on site, and the staff of the institutions took the opportunity to obtain first-hand information from the inspectors about supervisory requirements. BaFin will step up on-site inspections in future under the risk-based approach with a further shortening of inspection intervals for each institution.

In the event of findings concerning identified deficits in ML/TF prevention, the Supervisory Authority may under section 51 (2) of the Money Laundering Act take the appropriate and necessary

measures and issue orders to ensure compliance with the requirements stipulated under the Money Laundering Act and the Banking Act. This is supplemented by the general provisions in the Banking Act. BaFin may, for example, appoint a special representative at the institution itself or stipulate specific focal points for the audit of the annual financial statements. The informal measures effected in the majority of cases, such as letters of objection or discussions with the Supervisory Authority, are the softer response in accordance with the proportionality principle and have so far proved sufficient as a rule to induce institutions to comply with their statutory obligations. In 2018, BaFin effected 297 measures in this connection due to identified non-compliance with an obligation and conducted 2,672 other inspection measures. Informal measures are, as a rule, a more effective supervisory tool, as they tend to be implemented more quickly by institutions. It should also be noted that the bulk of supervisory activities do not cross the publicity threshold. This is partly due to the confidentiality requirements under section 9 of the Banking Act and section 54 of the Money Laundering Act. Under section 51 (9) of the Money Laundering Act, data on measures taken or caused to be taken is recorded in the form of statistics. The scope and effectiveness of supervisory measures can therefore be rated in the aggregate as adequate.

On the basis, in particular, of audit reports and on-site inspections by BaFin itself, the integrity and knowledge of bank staff with regard to ML/TF prevention are rated as high for the banking sector as a whole. There are strict supervisory requirements and stipulations with corresponding consequences and it has been standard practice for banks to provide their staff with training for many years. It is in the vital interest of banks themselves to employ well-trained bank staff in order to minimise ML/TF and thus keep the institution from harm. As well as potential reputational harm, money laundering and terrorist financing can in principle also involve operational risks. The sector is very aware of the possibilities for ML and TF. Compliance with anti-money laundering requirements is subject as a rule to internal audit, to external audit by auditors and by industry association audit bodies and to supervision.

Under section 7 (1) of the Money Laundering Act, obliged entities must appoint a money laundering reporting officer at senior management level and a deputy. The money laundering reporting officer serves executive management and as such must be organisationally and functionally subordinate to executive management or to a member of executive management. BaFin's findings show that money laundering reporting officers have sufficient powers and resources as a rule and are provided with the means needed to properly discharge their function. The effectiveness of organisational provision for anti-money laundering is therefore rated, in the aggregate, as high. It was also noted, however, that in individual instances, among small banks in particular, the organisational provision for AML could be assigned more time and human resources. This is mainly because the appointed officer in some cases also has other functions in the bank concerned and faces ever-increasing demands due to steadily rising statutory requirements and new findings from supervisory practice. Deficits with regard to the organisational structure and to the resources available to the money laundering reporting officer are also known to have been found at major banks. Findings of this kind are addressed by further intensifying supervisions and conducting increased numbers of on-site inspections. Banks that are subject to intensified supervision are to continue to be closely supervised by BaFin.

Under section 10 (1) no. 5 of the Money Laundering Act, obliged entities must continuously monitor business relationships, including transactions carried out under them. This is to ensure that transactions tally with applicable knowledge of the customer profile and where necessary the origin of

the assets. In this connection, under section 25h (2) of the Banking Act, credit institutions must generally operate and update IT systems that enable them to identify business relationships and individual transactions in payment operations that, in the light of knowledge of methods of money laundering, terrorist financing and other criminal actions, appear to be particularly complex or large or take place in an unusual manner or without an obvious economic or legitimate purpose. Enhanced due diligence requirements must also be fulfilled under section 15 of the Money Laundering Act if there could be a heightened ML/TF risk. In particular, section 15 (3) no. 1 (a) of the Money Laundering Act stipulates that it must be ascertained whether the contracting party is a PEP. Under section 43 of the Money Laundering Act, in the event of suspicious business relationships or transactions, obliged entities must report the matter to the FIU. The effectiveness of suspicious transaction monitoring and reporting, in particular on the basis of audit reports and on-site inspections by BaFin, is rated, in the aggregate, as high. As a rule, banks have effective and adequate systems for documenting, monitoring and reporting suspicious transactions. There are strict supervisory requirements and stipulations, compliance with which is ensured in various ways including internal audit, external audit by auditors and by industry association audit bodies, and supervision. On the basis of sampling, findings were made in all five banking sectors. Most of these related to deficits in documentation. Findings with significant (*gewichtig*) and severe (*schwergewichtig*) impacts[26] on the effectiveness of prevention measures were primarily found at large, globally operating banks and in some cases in the private banking sector. Violations are sanctioned accordingly by the Supervisory Authority.

Due to the detailed statutory requirements, German banks have a strong focus on initial customer identification. Identification in bank branches – face-to-face identification – continues to be the most frequently used identification method. Online account opening has become increasingly widespread in recent times, however. Non-face-to-face banking usually relies on video identification[27], the Postident identification procedure or identification using the online functionality of a personal identity card.

Careful initial identification must be followed up with regular ongoing identity verification with comprehensive monitoring of the business relationship and transactions. Adequate documentation and monitoring are especially important in dealings with customers without a business relationship (casual customers). Particularly when there are large numbers of casual customers and cash transactions, as with MVTS, adequate and effective monitoring is essential in order to be able to operate effective suspicious transaction reporting. BaFin already recognises the issue of casual customers and specifically targets it in on-site inspections.

Brexit, if it comes about, is not expected in principle to have significant impacts on ML prevention by banks in Germany. The United Kingdom is not classed as a high-risk jurisdiction and has comparable anti-money laundering standards. It should be noted, however, that the Money Laundering Act provides for a number of exemptions and special rules for EU countries that banks would no longer be able to apply in relation to the United Kingdom. Against the backdrop of the transposition into national law of the EU Money Laundering Directives, some provisions of the Money Laundering Act place banks under different obligations depending on whether a third country or an EU Member State is involved. In certain situations, therefore, Brexit would increase costs for banks.

Germany was one of the first countries in the world to set up an automated account information access

26 See the classification of audit findings in Annex 5 to section 27 of the Audit Report Ordinance (Prüfungsberichtsverordnung).

27 See BaFin Circular 3/2017 (GW).

procedure in 2003. This enables law enforcement agencies in particular to obtain relevant account master data on account holders, persons with powers of disposal and beneficial owners. BaFin also supervises credit institutions with regard to their obligation in relation to the automated account information access procedure and in this way ensures that up-to-date databases are always available for this purpose. On the basis of the automated account information access procedure, law enforcement agencies are provided in about 140,000 individual cases per year with information for the prosecution of crimes such as money laundering, terrorist financing, fraud and theft and for the seizure of assets relating to such offences. Following a technical modernisation in 2018, law enforcement agencies have been able to transmit requests electronically. This technical improvement is currently being rolled out and has already resulted in a significant acceleration of the process.

A special section on the banking sector in the interpretation and application guidance under section 51 (8) of the Money Laundering Act is being compiled in 2019 in order to take full account of the banking sector's requirements.

4.1.3 Individual banking sectors

For the purposes of the National Risk Assessment, credit institutions that engage in banking business within the meaning of section 1 (1) of the Banking Act were divided into five banking sectors in order to be able to adequately analyse risk potential and vulnerability potential, as follows:

1. Major banks and cooperative and public-sector central institutions
2. Branches and branch offices of foreign banks in accordance with section 53 and 53b of the Banking Act.
3. Regional banks and other commercial banks
4. Affiliated banks (cooperative banks and savings banks)
5. Other credit institutions.

The classification is essentially based on the Deutsche Bundesbank banking statistics. In addition, various types of banking products were classified and subjected to risk assessment for each of the above banking sectors. For the purposes of the National Risk Assessment, the term 'products' is used as a collective term for (financial) products such as payment accounts, (financial) services such as asset management and (sales) channels such as electronic banking. A total of 13 products were classified for the National Risk Assessment.[28] Each product was assessed on the basis of product-specific factors. In particular, the following attributes and criteria were included in the analysis:

- Customer base profile
- Availability over time
- The product's suitability for the transfer of assets
- The product's fungibility
- Frequent use of cash
- Potential anonymous use
- Characteristics of possible sales channels
- Scope of diligence measures.

The individual characteristics of the selected banking sectors and their specific risk situation are presented in the following. The sectoral risk assessment heavily depends on the applicable product segment and sales channel.

4.1.3.1 Major banks

The analysis in this sector covers major banks and cooperative and public-sector central institutions. These represent more than a third of the entire banking sector in terms of balance sheet total.[29] Due to their business model and the fact that they are deeply interconnected internationally, the

28 See sections 4.1.3.1 to 4.1.3.5 for further detail.
29 See Deutsche Bundesbank, Banking Statistics July 2019, p. 106.

banks analysed in this sector offer the broadest range of banking products when compared with the remaining banking sectors. This goes with corresponding inherent risks. The major banks have a nationwide branch network and in addition to traditional corporate and retail banking are increasingly active in securities and in investment banking. They have a strong international market focus in their banking activities and financing.

Cooperative and public-sector central institutions operate at supraregional level in the affiliated banks sector. They handle clearing for affiliated banks and provide banking that the regional affiliated banks are unable to offer due to their small size and regional focus. The central institutions enable affiliated banks to tap into the international money and capital markets as needed. They tend to focus their activities on wholesale banking and capital market transactions and compete here with major private-sector commercial banks.

Overall, the potential threat to the banking sector under analysis of being misused for money laundering and terrorist financing, due to its global interconnectedness, diverse product range and large business volume, is rated the highest when compared with the remaining banking sectors. While no rising or falling trend is seen in this regard, there has been a rise in the public perception due to recent money laundering scandals involving major banks. The banks in this sector are highly important to the German economy due to their size and the fact that they are deeply interconnected internationally. There is also market pressure on the major banks sector to comply with the anti-money laundering standards of foreign bodies. This results in the obliged entities complying with additional foreign anti-money laundering requirements. This pressure is intense and in part affects commercially important business, but also has to be seen in perspective relative to the sum total of all banking business, hence the overall market pressure is still to be rated as high.

Due to the wide-ranging business activities with a corresponding range of products together with the global interconnectedness, the vulnerability of the banking products of major banks to be misused for money laundering is rated highest when compared with the remaining banking sectors. Product vulnerability consequently rates as high.

In order to assess the ML/TF risks of specific banking products in this sector, it is important to have at least a general understanding of the product sizes and volumes. The table below shows the sizes and transaction volumes for products of major banks on a five-point scale from ‘low’ to ‘high’. The total size of a given product corresponds here to its significance within the sector relative to other products provided in the sector. The ratings were plausibility-checked and verified in the private-sector consultation. Assessments by the institutions themselves, the German banking sector and auditing firms were included in the rating.

Bank products: Number: 13	**Total size/value of product**	**Average transaction size**
Current accounts	medium-high	medium
Term and savings deposits	medium	medium
Money or value transfer services	medium-low	low
Foreign currency dealing and sale of precious metals	low	medium-low
Safe deposit boxes	low	low
Credit cards (including prepaid)	medium-low	medium-low
Retail lending	medium-high	medium-high
Corporate lending	medium-high	high
Securities, investment in financial derivatives and other investments	high	high
Foundations, trusts and offshore vehicles	medium-low	medium-high
M&A	medium-low	medium-high
Correspondent banking business	medium-high	medium
Trade finance	medium-high	medium-high

Table 3: Total size/value of products and average transaction size among major banks

Due to the international focus of their business, the banks under analysis are seen to have the largest range of products when compared with the remaining banking sectors, with corresponding inherent risks. Their international connectedness results in large foreign interests, including in some cases in high-risk jurisdictions. The observed phenomenon of increased inbound foreign investment, notably in corporate shareholdings and real estate, is handled by major banks as a rule. Correspondent banking plays a major part here. Trade finance, which has an important role due to Germany's exporting strength, is a highly important product in this sector. The total size of a given product provides an indication as to the potential risk of being misused for money laundering and terrorist financing. As the size and volume of a given product increase, it becomes easier in principle for criminals to disguise incriminated funds and transactions, and harder to prevent money laundering and terrorist financing. Products used to process complex transactions are also exposed to heightened threat of being misused for money laundering and terrorist financing.

The table below shows, as an outcome of the National Risk Assessment, the sector's bank products and bank services in order of risk of being misused for money laundering and terrorist financing, commencing with (1) for the highest-risk product:

Bank products: Number: 13	**Money laundering**	**Terrorist financing**
Current accounts	1	1
Correspondent banking business	2	2
Foundations, trusts and offshore vehicles	3	9
Securities, investment in financial derivatives and other investments	4	11
M&A	5	5
Trade finance	6	6
Foreign currency dealing and sale of precious metals	7	7
Money or value transfer services	8	3
Corporate lending	9	8
Credit cards (including prepaid)	10	10
Retail lending	11	4
Safe deposit boxes	12	13
Term and savings deposits	13	12

Table 4: Ranking of the products of major banks by risk

This rating was based on product-specific factors, taking into account case studies and certain product characteristics. Current accounts are the basis of a business relationship here and serve as the reference account for other bank products. They are subject to heightened risk as funds on current accounts can be highly fungible and liquid. Transactions can be made at short notice and at any time. Cash can also be deposited and withdrawn at any time, including using ATMs. There are wide-ranging sales channels, including online banking without direct customer contact. In online retailing, new payment methods are seen in which the payer and the payee can be separated across multiple levels. This can make it difficult to identify the actual end consumer or the beneficiary of the payment account. Instant payment allows amounts to be transferred in real time. Current accounts can also be used for terrorist financing purposes, especially in the case of low-volume transactions, as smaller amounts are harder to identify and trace than larger-volume transactions.

Correspondent banking involves high inherent risk due to the in some cases complex international interconnections. Correspondent banks are frequently used as a channel to disguise payments to offshore jurisdictions. In all, the four major banks have by far the largest number of correspondent banking relationships. One challenge in correspondent banking is that of knowing who the true customers are in a correspondent banking relationship. An effective monitoring system is indispensable here. Correspondent banking relationships have declined by 43% overall since 2014 due to de-risking measures (at the ten biggest German banks in terms of balance sheet total).

MVTS is rated in a heightened risk category with regard to terrorist financing, primarily due to the use of cash and the fact that there is usually an international dimension. However, the relative size of MVTS business among major banks in this sector is smaller than among other banks.

The securities, investment in financial derivatives and other investments product is a grouped category. General securities investment, especially in the case of small volumes in the retail segment, in principle presents a smaller risk than with institutional investors or investment in derivatives and exotic financial products.

Substitute currencies in forms such as prepaid credit cards or precious metals likewise constitute a risk. Trade finance, foundations, trusts and offshore vehicles are also connected with heightened risk because of their structures are usually complex structures, because they favour anonymity, and because they have an international dimension.

Trade-based money laundering is particularly significant for Germany because of the trade volumes it generates as an industrial powerhouse. In 2017, Germany, as the world's third-largest exporter and importer, exported goods with a total value of €1,273 billion and imported goods with a total value of €1,006 billion.[30] Typical ML/TF methods are over-invoicing and under-invoicing goods and services, multiple billing of goods and services, fictitious trades and the use of shell companies. In trade finance, banks have a large amount of information on business relationships. In contrast to pure-play lending business or correspondent banking business, this information can be used in monitoring with the effect of reducing risk. For this purpose, it is important for the bank – in addition to the documents required in any case – to have sufficient knowledge of the underlying trade transaction and the trading partners. Only then is a bank able to detect indications of trade-based money laundering and accordingly submit an STR to the FIU. The banking sector plays a very important role here in the identification of anomalous transactions.

Foreign currency dealing and the sale of precious metals are provided on a small scale. This product relates to a large extent to providing bank customers with foreign currency in usual, relatively small quantities for planned travel. In some cases, purchases and sales of gold are carried out on behalf of customers on a substantial scale. In addition to in-branch service, banks sometimes offer online ordering of foreign currency and precious metals up to a specific limit per order and per day together with home delivery. This requires a current account with the bank and online banking access. Deliveries can be made to a freely specified delivery address anywhere in Germany, provided the account holder or authorised representative is named as the addressee. As a rule, this service is only available for customers with an existing customer and account relationship. However, there is evidence of it also being offered to non-customers. The proper application of internal safeguards and customer care obligations together with adequate documentation are particularly important in this connection.

In contrast, loan products generally have lower ML risk. Mortgages in particular require extensive proof of income, assets and future cash flows, if only to verify creditworthiness. Corporate lending is more susceptible in principle to money laundering than retail lending because it tends to involve more complex structures and larger transaction volumes. Conversely, consumer loans are more relevant in connection with terrorist financing because of lesser stipulations as to the use of the funds. Money laundering risk is generally rated higher in corporate banking than in retail banking because ownership structures and transaction profiles tend to be more complex. On the other hand, retail banking products and services, especially with regard to payment services, tend to be more susceptible to terrorist financing than other corporate and institutional banking products. Terrorist financing often involves the illicit use of legally acquired funds. Such a "suspicious use of funds" is far harder for a bank to pick out than a anomalous or suspicious origin in connection with money laundering.

Use of a credit card generally requires a reference account, which means that the transaction history

30 See Federal Ministry for Economic Affairs and Energy for Economic Affairs and Energy, "Facts about German foreign trade", October 2018.

can be traced from accounts in the same bank. It is harder to trace, however, if the reference account is with another bank. It is not normally possible to load a credit card with cash. Prepaid credit cards are an exception here. Cash withdrawals are possible, and break the paper trail. Because of this, credit card business, or prepaid credit card business, harbours a high terrorist financing risk as well as a money laundering risk. Terrorists can use credit cards for any purpose at any time, including abroad. Terrorists have highly diversified financing mechanisms and new anonymous methods are emerging for obtaining and transferring funds. Although there have so far been few points of contact in practice, banks stated in the private-sector consultation that they perceive an overall increase in extremism and active radicalism, including on the part of self-radicalised individuals.

BaFin will continue to closely supervise and carry out targeted on-site inspections at banks that are subject to intensified supervision.

4.1.3.2 Branches and branch offices of foreign banks

This sector includes, under section 53 of the Banking Act, all branches of undertakings domiciled outside Germany and, under section 53b of the Banking Act, branch offices of credit institutions domiciled in another member state of the European Economic Area. These belong to the – predominantly private-sector – commercial banks pillar of the German banking system and, like all German credit institutions, are subject to the Banking Act and the Money Laundering Act. The presence of branches of foreign banks in Germany has grown with increasing globalisation.[31] In this connection, foreign customers tend to demand and make use of a presence in Germany.

It should be noted that branch offices under section 53b of the Banking Act are not required by law to have compliance with AML requirements verified by the auditor of the annual financial statements. BaFin has consequently intensified supervision of branch offices coming under section 53b of the Banking Act. To remedy the information deficit, data and information are gathered from such banks by means of questionnaires and targeted on-site inspections are carried out under a risk-based supervisory approach. Branches under section 53 of the Banking Act, on the other hand, are subject to statutory reporting requirements.

Banks in this sector mostly have a similar business model to major, internationally active banks in the first sector, with corresponding inherent risks. Their business activities are therefore geared to the needs of internationally operating customers and differ from those of regionally operating affiliated banks with a considerably larger volume of international business. The threat of this sector being misused for money laundering and terrorist financing is therefore rated by the public agencies involved as high. No rising or falling trend is seen in this connection.

The overall vulnerability of products provided by branches and branch offices to be misused for money laundering is rated medium-high. This assessment is based among other things on these banks' extensive business activities, with a corresponding range of banking products and international interests. Product vulnerability in this sector is higher in principle than in the affiliated banks and other credit institutions category. It should be noted that, despite measures taken by the Supervisory Authority, there is an information deficit relative to other banks due to the lack of reporting obligations on branch offices coming under section 53b of the Banking Act.

The table below shows, in a similar way to the previous sector, the size/value and average transaction size for each product provided by branches and branch offices. As before, the ratings were plausibility-checked and verified in the private-sector consultation.

31 See Deutsche Bundesbank, Banking Statistics July 2019, p. 106.

Bank products: Number: 13	**Total size/value of product**	**Average transaction size**
Current accounts	medium-high	medium
Term and savings deposits	Medium	medium
Money or value transfer services	medium-low	low
Foreign currency dealing and sale of precious metals	Low	low
Safe deposit boxes	Low	low
Credit cards (including prepaid)	Low	medium-low
Retail lending	Medium	medium
Corporate lending	medium-high	high
Securities, investment in financial derivatives and other investments	Medium	medium-high
Foundations, trusts and offshore vehicles	medium-low	medium-high
M&A	medium-low	medium-high
Correspondent banking business	Medium	medium-low
Trade finance	Medium	medium-high

Table 5: Total size/value of products and average transaction size among branches and branch offices.

Branches and branch offices are seen in general to have similar activities and a comparable product range to the major banks in the first sector. The volumes are frequently smaller, however. To avoid repetition, reference is made to the discussion on the first banking sector and only specific features are highlighted in the following.

Due to their international dimension, branches and branch offices naturally play an important part in foreign trade finance for trade in goods, export finance and foreign corporate finance. These banks support foreign companies, among other things with documentary foreign trade in Germany. They handle much inbound foreign investment, for example by institutional customers. In this connection, foreign customers tend to demand and make use of a presence in Germany. Current accounts are therefore used to process payments for foreign customers. Retail customers in particular, including embassy staff, often do their banking through a branch or branch office connected with their home country. Their retail banking activities also include securities transactions. MVTS is of major importance and cash transfers abroad are possible in principle. Branches are also involved in payments with third countries and in some cases high-risk jurisdictions.

The table below shows, as an outcome of the National Risk Assessment, the sector's bank products and bank services in order of risk of being misused for money laundering and terrorist financing, commencing with (1) for the highest-risk product:

Bank products: Number: 13	**Money laundering**	**Terrorist financing**
Correspondent banking business	1	2
Current accounts	2	1
Foundations, trusts and offshore vehicles	3	9
Money or value transfer services	4	3
Securities, investment in financial derivatives and other investments	5	11
M&A	6	5
Trade finance	7	6
Foreign currency dealing and sale of precious metals	8	7
Corporate lending	9	8
Credit cards (including prepaid)	10	10
Retail lending	11	4
Safe deposit boxes	12	13
Term and savings deposits	13	12

Table 6: Ranking of the products of branches and branch offices by risk.

4.1.3.3 Regional banks and other commercial banks

This sector comprises all banks in the regional banks and other commercial banks category in the Deutsche Bundesbank statistics. The banks in this sector belong to the predominately private-sector commercial banks pillar of the banking system and compete with each other within the category. They consequently differ from cooperative and public-sector banks. As the term indicates, regional banks originally comprised banks whose activities were limited to a specific regional territory. Today, this sector contains a highly diverse cross-section. While many operate as conventional universal banks, some are also highly specialised. The analysis thus extends to corporate and automotive banks, private bankers and other credit institutions that continue to be regional banks. Many banks in the continuously growing direct banking segment are also commercial banks. Direct banks differ among other things due to web-based or telephone-based banking. This is important with regard to identification and ongoing monitoring of customer relationships. Direct banks offer customers a high degree of flexibility, in many cases combined with low transaction fees. In contrast to the major banks, however, most banks in the regional banks and other commercial banks category still tend to be smaller and have a branch network that is restricted to a specific region. In a similar way to the business model operated by savings banks and cooperative banks, the focus of their activities is on primarily deposit-financed lending to businesses and private households. They compete in this regard with the savings banks and cooperative banks. Regional banks and other commercial banks account for a combined balance sheet total of €1,056,715 million as of 31 December 2017 and

in terms of balance sheet total are thus comparable as a category to the cooperative banks.[32]

The threat of the regional banks and other commercial banks sector being misused for money laundering and terrorist financing is rated by the public agencies involved as high overall. At the same time, the overall threat potential tends to be lower than among the large globally active banks in the first sector. No rising or falling trend is seen in this connection.

The vulnerability of this banking sector's products to being misused for money laundering is rated overall as medium-high. This vulnerability is nevertheless lower relative to the major banks in the first sector but higher than among the affiliated banks and other credit institutions category. For a large proportion of the small and medium-sized regional banks with regional activities, however, the vulnerability of their products is similar to that for affiliated banks.

The table below shows, in a similar way to the previous sectors, the size/value and average transaction size for each product provided by regional banks and other commercial banks. As before, the ratings were plausibility-checked and verified in the private-sector consultation.

Bank products: Number: 13	**Total size/value of product**	**Average transaction size**
Current accounts	medium-high	medium-low
Term and savings deposits	medium-high	medium-high
Money or value transfer services	medium-low	medium-low
Foreign currency dealing and sale of precious metals	low	low
Safe deposit boxes	low	low
Credit cards (including prepaid)	medium	medium
Retail lending	medium-high	medium
Corporate lending	medium	high
Securities, investment in financial derivatives and other investments	medium-high	medium-high
Foundations, trusts and offshore vehicles	medium-low	medium-high
M&A	medium	medium-high
Correspondent banking business	medium-low	low
Trade finance	medium-low	medium

Table 7: Total size/value of products and average transaction size among regional banks and other commercial banks

32 See Deutsche Bundesbank, Banking Statistics July 2019, p. 106

It should be noted here that the above averages do not apply to all banks in the sector. This is because, as mentioned above, this category combines what in some respects is a very disparate range of banks. A substantial proportion of these banks conduct business on a similar scale and volume as banks in the affiliated banks category. Business is concentrated among other things on payments, corporate and retail lending and securities. On average, however, there is a comprehensive product range. Due to the wealth of different business models, all customer groups tend to use the products on offer. In some cases, therefore, there is also demand from high-risk customers.

A number of banks in this sector increasingly handle investment from abroad, notably in German real estate. The sector features an international branch and branch office network, especially in the case of subsidiaries of foreign banks.

As a rule, banks in the sector offer both face-to-face and remote banking. The recent past has seen growing demand for online banking. Use is also made here of video identification and the Postident identification procedure. Account opening is usually done at a branch, however.

In addition, banks reported in the private-sector consultation that vulnerability with regard to ML/TF has risen due to the increasing digitalisation of payment processes.

MVTS business generally has high importance among banks whose core business has an international dimension. This product is used both for national and for international transactions. Workers' remittances play a role in the latter. On the other hand, many banks rule out such business altogether to avoid sources of error. Cash transfers by casual customers carry particularly high risk in this connection. This is especially the case if, for example, not all customer due diligence requirements are met and there is no effective monitoring. Under section 10 (3) sentence 1 no. 2a of the Money Laundering Act, banks that offer MVTS outside of a business relationship must identify casual customers in the case of transfers upwards of €1,000. The rule in practice, however, is for every casual customer to be identified. Prevention measures in this connection vary considerably in quality.

The private-sector consultation showed that so-called basic payment accounts are subject to greater monitoring with regard to payments. This is because of the lower identification requirements. However, the problem of a person being potentially identified on the basis of false information in identification documents poses itself prior to the banks' customer acceptance process. Although there are relatively few suspicious cases in practice, banks see at least a perceived inherent risk in this connection.

As in other banking sectors, foreign currency dealing and the sale of precious metals are provided on a small scale. To avoid sources of error, however, many banks rule out such business altogether or only offer it below the statutory thresholds.[33]

Securities transactions and fiduciary and asset management services are provided, in some cases on a large scale. Average transaction volumes tend to be higher here because there tends to be a large number of wealthy customers. The products do not generally have the same complexity and scope as with the large, globally operating banks.

Operating credit card business involves heightened risk with regard to terrorist financing. The private-sector consultation showed among other things that prepaid credit cards and the cross-border card-to-card transactions associated with credit cards are vulnerable to terrorist financing abuse. Terrorists can use credit cards to make payments for any purpose at any time both in Germany and abroad.

33 See section 4.1.3.1.

Banks in this sector increasingly provide retail loan products. Consumer loans are therefore significant in connection with terrorist financing because of lesser stipulations as to use of the funds.

While safe deposit boxes are a side-product atypical of banking, they can in principle be used for the safekeeping of incriminated funds, including in connection with terrorist financing. As a result of the revision of the Money Laundering Act, section 24c (1) sentence 1 no. 1 of the Banking Act provides transparency with regard to the existence of a safe deposit box as part of customer master data. Beginning in 2019, related infringements result in an objection from the Supervisory Authority.

The table below shows, as an outcome of the National Risk Assessment, the sector's bank products and bank services in order of risk of being misused for money laundering and terrorist financing, commencing with (1) for the highest-risk product:

Bank products: Number: 13	**Money laundering**	**Terrorist financing**
Money or value transfer services	1	1
Current accounts	2	2
Correspondent banking business	3	5
Securities, investment in financial derivatives and other investments	4	8
Foreign currency dealing and sale of precious metals	5	6
Corporate lending	6	7
Foundations, trusts and offshore vehicles	7	9
Trade finance	8	11
Retail lending	9	4
Credit cards (including prepaid)	10	3
Term and savings deposits	11	12
M&A	12	13
Safe deposit boxes	13	10

Table 8: Ranking of the products of regional banks and other commercial banks by risk.

4.1.3.4 Banks in the affiliated banks category

This sector comprises all banks placed in the savings banks and cooperative banks category in the Deutsche Bundesbank statistics. These are mostly local universal banks with limited regional market focus and size. Their business mainly focuses on taking savings deposits and medium to long-term lending such as mortgage loans and capital expenditure loans for small and medium-sized businesses and for local authorities. This sector consequently comprises a very homogeneous group of banks. Although, being universal banks, they can in principle carry out all types of banking business, their proximity to local markets and customers and slightly limited product range give them a good ability to assess and counter ML/TF risks. The regional principle is notably reflected in the branch network and means in many cases that customers are personally known, and that anomalies are noticed directly by bank staff. It is only through their affiliation that individual affiliated banks are able to provide a broad range of banking and financial services. For example, payments are cleared via central institutions that, among other things, have the correspondent banking relationships needed for the purpose.

The threat of the affiliated banks sector being misused for money laundering and terrorist financing is rated by the public agencies involved as medium-high overall. The threat potential thus tends to be lower than for banks in the first three banking sectors, although higher than for the other credit institutions category. No rising or falling trend is seen in this connection.

The vulnerability of the affiliated banks category's products to being misused for money laundering is rated overall as medium. This vulnerability is lower relative to the banks in the first sectors but higher than among the other credit institutions category.

The table below shows, in a similar way to the previous sectors, the size/value and average transaction size for each product provided by affiliated banks. As before, the ratings were plausibility-checked and verified in the private-sector consultation. In addition to the assessments made by the affiliated banks themselves, the analysis also incorporated the experience of the industry associations and selected association audit bodies.

Bank products: Number: 13	**Total size/value of product**	**Average transaction size**
Current accounts	high	medium-low
Term and savings deposits	medium-high	medium
Money or value transfer services	medium-low	medium-low
Foreign currency dealing and sale of precious metals	low	low
Safe deposit boxes	low	low
Credit cards (including prepaid)	medium-low	medium
Retail lending	high	medium-high
Corporate lending	medium	high
Securities, investment in financial derivatives and other investments	medium	medium
Foundations, trusts and offshore vehicles	medium-low	medium-high
M&A	low	medium-high
Correspondent banking business	low	medium-low
Trade finance	low	medium

Table 9: Total size/value of products and average transaction size among the affiliated banks category.

A major business focus in the affiliated banks category is medium and long-term lending. Retail lending business is particularly important here. In this connection, consumer loans are in principle highly vulnerable to being misused for terrorist financing purposes because of lesser stipulations as to the use of funds.

A further focus is the deposit business, primarily in the form of current accounts. This essentially addresses all customer groups. It is primarily conducted with regional customers, however. In some cases, high-risk customers are precluded. Any international dimension is generally only on a small scale and in particular only tends to be involved where an affiliated bank operates in a border region. IT monitoring systems established across all affiliated banks ensure full monitoring of business relationship and transactions.

Some use is made in the affiliated banks category of MVTS. In this connection, affiliated banks offer what may be termed back-to-back cash transactions. This is where a cash amount is paid in with instructions for the amount to be paid back out in cash at a recipient bank. On the other hand, many banks rule out such business altogether to avoid sources of error. Where offered, MVTS is generally strictly limited, for example by means of thresholds. Checks are also made as to the source of funds. Business with casual customers is generally ruled out entirely.

The volume of business in foreign currency dealing and the sale of precious metals has declined in recent years. Many smaller banks rule out such business under the risk-based approach altogether, or only offer it below the statutory thresholds. This business continues to be provided by larger affiliated banks, primarily in conurbations with diverse population structure. Foreign currency dealing is primarily provided on a small scale on a retail basis, such as for foreign travel by customers. The risks associated with such transactions are seen to be closely monitored. Foreign currency dealing and the sale of precious metals are only available as a rule for customers with an existing account relationship.

Affiliated banks do not generally have products involving trusts and offshore vehicles, but they do generally handle business with primarily regional foundations. There is in principle a money laundering risk here due to the sometimes complex structures involved.

Securities transactions are mostly not part of affiliated banks' core business and are therefore offered on a smaller scale than in other banking sectors. Securities transactions are primarily conducted on a retail basis and increasingly in larger affiliated banks.

The table below shows, as an outcome of the National Risk Assessment, the sector's bank products and bank services in order of risk of being misused for money laundering and terrorist financing, commencing with (1) for the highest-risk product:

Bank products: Number: 13	**Money laundering**	**Terrorist financing**
Current accounts	1	1
Money or value transfer services	2	2
Corporate lending	3	7
Foreign currency dealing and sale of precious metals	4	5
Retail lending	5	3
Credit cards (including prepaid)	6	4
Safe deposit boxes	7	6
Correspondent banking business	8	8
Securities, investment in financial derivatives and other investments	9	11
Foundations, trusts and offshore vehicles	10	10
Term and savings deposits	11	9
Trade finance	12	12
M&A	13	13

Table 10: Ranking of the products of affiliated banks by risk.

4.1.3.5 Other credit institutions

For the purposes of the National Risk Assessment, all banks were placed in the other credit institutions category that are subsumed in the Deutsche Bundesbank statistics under the following collective terms: mortgage banks, banks with special, development and other central support tasks, building and loan associations and guarantee banks. Specialised credit institutions typically limit their activities to selected areas of banking business and in many cases are affiliated with a universal bank. Mortgage banks, for example, provide long-term loans to finance the construction of properties and public infrastructure. For this purpose, mortgage bonds (Pfandbriefe) are issued that can be acquired by other customers and institutions. Where activities are restricted to specific areas, the risk of being misused for ML/TF purposes is commensurately smaller.

The threat of the other credit institutions sector being misused for money laundering and terrorist financing is rated by the public agencies involved as medium overall. The overall threat potential is thus the lowest when compared with the remaining banking sectors. No rising or falling trend is seen in this connection.

The vulnerability of the other credit institutions category's products to being misused for money laundering and terrorist financing is rated overall as medium. This sector has the lowest vulnerability when compared with the remaining bank categories.

The table below shows, in a similar way to the previous sectors, the size/value and average transaction size for each product provided by banks in the other credit institutions category. The banks in the other credit institutions category are seen to have the smallest range of products when compared with the remaining banking sectors, with correspondingly smaller inherent risks. As before, the ratings were plausibility-checked and verified in the private-sector consultation.

Bank products: Number: 13	**Total size/value of product**	**Average transaction size**
Current accounts	low	medium-low
Term and savings deposits	high	medium-low
Money or value transfer services	–	–
Foreign currency dealing and sale of precious metals	–	–
Safe deposit boxes	–	–
Credit cards (including prepaid)	low	medium-low
Retail lending	medium-high	medium-high
Corporate lending	medium-high	high
Securities, investment in financial derivatives and other investments	medium	medium-low
Foundations, trusts and offshore vehicles	–	–
M&A	–	–
Correspondent banking business	–	–
Trade finance	–	–

Table 11: Total size/value of products and average transaction size among banks in the other credit institutions category.

Only a few of these banks offer current accounts and credit cards and then only on a small scale. If provided, current accounts are offered in combination with other products such as credit cards. Where they are on offer, such products in principle have high vulnerability with regard to ML/TF. As a rule, however, current accounts are only available to a limited range of customers, such as retail customers, young people's accounts or for bank staff. With regard to credit cards, prepaid credit cards are also offered in individual cases (including on an online basis), but once again, as a rule, solely for a limited range of users, such as under-eighteens.

Term and savings deposits constitute a large overall share of the total business volume. The total product value is particularly large among building and loan associations (*Bausparkassen*), which account for a large proportion of the sector in terms of balance sheet total. However, the average transaction volume tends to be small. These are mostly smaller transactions in the form of deposits such as regular payments into a home purchase savings plan (*Bausparvertrag*). Outgoing payments are naturally larger.

Lending is also an important part of the business of banks in the other credit institutions category. Large-volume loans can be misused here for money laundering purposes, for example by incriminated funds being included in the repayment instalments.

The other credit institutions category has low vulnerability overall with regard to terrorist financing because products having high terrorist financing vulnerability are either not offered at all or are only provided on a small scale.

The table below shows, as an outcome of the National Risk Assessment, the sector's bank products and bank services in order of risk of being misused for money laundering and terrorist financing, commencing with (1) for the highest-risk product:

Bank products: Number: 13	**Money laundering**	**Terrorist financing**
Current accounts	1	1
Credit cards (including prepaid)	2	2
Corporate lending	3	5
Securities, investment in financial derivatives and other investments	4	4
Retail lending	5	3
Foreign currency dealing and sale of precious metals	–	–
Foundations, trusts and offshore vehicles	–	–
Trade finance	–	–
Money or value transfer services	–	–
Term and savings deposits	–	–
Correspondent banking business	–	–
M&A	–	–
Safe deposit boxes	–	–

Table 12: Ranking of the products of other credit institutions by risk.

4.2 Insurance sector

4.2.1 Overview

In accordance with Germany's federal system, insurance supervision is divided between the Federal Government and the *Länder*. At the federal level, BaFin supervises the private-sector insurance undertakings operating in Germany that are of material financial and economic importance as well as public-sector insurance undertakings engaging in open competition that operate beyond the borders of any one of the *Länder*. The *Länder* supervisory authorities primarily supervise public-sector insurance undertakings whose activities are restricted to one of the *Länder* and those private-sector insurance undertakings that are of minor economic and financial importance. All insurance undertakings in Germany must also adhere to the principle of business segregation under section 8 (4) of the Insurance Supervision Act (*Versicherungsaufsichtsgesetz*). This stipulates that life insurance business, health insurance business and property and accident insurance business must be carried out by independent undertakings. As a result of these stipulations, there are a large number of insurance undertakings that belong to larger insurance groups. With 84 undertakings and over €909 billion – almost 60% of the aggregate investment portfolio of all German primary insurance undertakings under federal supervision – the life insurance business is of major relevance in the overall market.[34]

All insurance products were included in the analysis work for the National Risk Assessment. The public agencies involved do not currently have any indication of insurance undertakings that are not as yet obliged entities under the Money Laundering Act being misused for money laundering. The information on the insurance sector contained

34 See BaFin, Annual Report 2017, p. 110 and 183.

in the following therefore relates to the over 200 insurance undertakings under money laundering supervision by BaFin. Under the Money Laundering Act, these include insurance undertakings that provide life insurance, provide accident insurance with premium refund or grant money loans.

The German insurance sector has a primarily national focus. With the exception of globally operating groups, the majority of German insurance undertakings are regionally or nationally focused. Public-sector insurance undertakings in particular operate according to the regional principle. As a result of digitalisation, however, especially in sales, regional borders are becoming increasingly blurred and many undertakings market their insurance products throughout Germany.

The threat of the sector being misused for money laundering is rated by the public agencies involved as medium-low overall. There is assumed to be a trend towards an increase in this risk because the persistent low interest rate environment is causing companies to launch more flexible life insurance products and increasingly to offer bank-like products. Such products could make the sector more attractive for money launderers.

The vulnerability of the insurance sector's products to being misused for money laundering is rated overall as between medium-low and low. BaFin itself conducts on-site inspections of insurance undertakings that are obliged entities. In conjunction with internal audit reports on ML/TF prevention quality, the Supervisory Authority gains a comprehensive picture of prevention in each undertaking. On the basis of this knowledge, staff integrity and knowledge of money laundering prevention are rated as high. The effectiveness of money laundering reporting officers is likewise rated as high across the entire sector, although smaller and medium-sized insurance undertakings frequently do not assign the necessary human resources to the function of the money laundering reporting officer. This usually manifests itself in the person concerned having to discharge other responsibilities or line responsibilities within the insurance undertaking in addition to their role as money laundering reporting officer.

Under the 'know your customer' principle, insurance undertakings are required to ascertain their customers' financial background. When establishing a business relationship, insurance undertakings should collect relevant information (such as occupation) in order to assess the customer's risk level. Many insurers do not yet ask customers to state their occupation in every instance, however, because this information is frequently only elicited in connection with the risk that is to be insured (as with occupational disability insurance), rather than for money laundering prevention purposes.

On the positive side, most insurance undertakings do not accept cash as a matter of policy. There are isolated exceptions, but these are limited to a small number of individual cases and are specially monitored by the money laundering reporting officer. Most insurance undertakings now only keep cash on hand for the purpose of small cash advances. The great majority of undertakings therefore no longer accept or pay out cash. This is largely an outcome of intensive prevention work by BaFin, including in connection with on-site inspections.

The FIU and law enforcement agencies in particular take a critical view of the number of STRs from the insurance sector. They account for less than 1% of all STRs. It became clear in the expert consultation that money laundering reporting officers invest considerable resources in verifying satisfaction of the requirements under section 43 (1) of the Money Laundering Act. It should be expressly emphasised in this connection that in order for there to be a reportable matter, it is necessary, but also sufficient, for there to be facts that indicate the

presence of the circumstances under section 43 (1) of the Money Laundering Act.[35] Comprehensive fact-finding and assessment in many cases helps the FIU in the filtering process as well as helping law enforcement agencies in their investigations, but in certain circumstances can also result in relevant cases not being reported. In case of doubt, therefore, an STR must always be submitted.

4.2.2 Insurance products

4.2.2.1 Endowment life insurance and deferred annuity insurance

With endowment life insurance and deferred annuity insurance products, a basic distinction has to be made between regular premium and single premium policies. A further distinction has to be made with regard to sales channels, which are divided into sales made by tied agents and banks versus online sales and sales made by independent brokers. The ML risks can generally be assumed to be lower in sales by tied agents and banks.

The vulnerability of regular premium policies to being misused for money laundering is rated as medium-low. The vulnerability of single premium policies to being misused for money laundering is rated as medium-low. There is no appreciable difference in the rating given for products sold by tied agents and banks. This is mainly because of the high inherent money laundering threat arising from the single premium.

The total volume of endowment life insurance and regular premium deferred annuity insurance is high at just under 60% of new business in the life insurance sector. The total volume of single premium policies, at just over 13%, is rated medium-low. The proportion of this accounted for by public insurers is small.[36]

Relevant typologies for these products include:

- Contrary to what is agreed in the policy, a policyholder announces that they will make large advance payments against the insurance premiums.

- An insurance policy is terminated early and paid out by cheque, with the policyholder taking a loss. In such cases, the policyholder will frequently have had an unusual interest – prior to taking out the insurance – in early termination and the payout options.

- A policyholder presents fictitious documentary evidence for the source of funds; for example, it is stated that a property has been sold abroad and the documents submitted are not the originals.

Payment of single premiums and large regular premiums is primarily significant with a view to misuse of the product for money laundering. When payments exceed the relevant thresholds set by insurers in their risk analysis, the source of the funds must be ascertained or the transaction passed on to the money laundering reporting officer for further examination. The policyholder's financial circumstances must be plausible relative to the size of the premium paid.

The low interest rate environment is causing insurance undertakings to offer new forms of products in order to generate new business. The trend is towards 'flexible' products that, unlike conventional endowment products in insurance, allow flexible premiums and payouts over the term of the policy. This includes the policyholder being free to choose both the timing and size of payments. These products are therefore equivalent to money market account and savings account

35 See decision of Frankfurt Higher Regional Court (Oberlandesgericht Frankfurt) of 10 April 2018; 2 Ss-OWi 1059/17.

36 BaFin, internal survey, as of 31 December 2017.

products provided by banks. Unlike banks, insurance undertakings do not have to provide IT-based monitoring by law. A lack of IT-based monitoring can give rise to transaction risks as the new forms of products can be misused for money laundering and it is near-impossible to monitor transactions closely on a manual basis. The fact that insurance undertakings – unlike a customer's principal bank – do not provide current accounts means that they do not have full visibility over customers' cash flows. This can hinder suspicious transaction reporting even where there is an effective system in place.

4.2.2.2 Term life insurance

The market share of term life insurance and corresponding disability products in new life insurance business is rated medium at just over 25%.

The vulnerability of term life insurance to being misused for money laundering is rated medium-low. However, the product lends itself more to terrorist financing than to money laundering. A young customer taking out funeral expenses insurance or life insurance can be an indication of a planned journey to a terrorist region as a fighter. To prevent terrorist financing, therefore, insurers should exclude death or disability due to involvement in acts of war in their general terms and conditions of insurance.

4.2.2.3 Accident insurance with premium refund

Of a total of 201 insurance undertakings in the property and casualty insurance segment, only 22 have an accident insurance with premium refund product in their portfolio.[37] In addition, only 13 undertakings still actively generate new business.[38] It should be emphasised that this product generally involves smaller insured amounts and the total value of the product is therefore rated as minor.

37 BaFin, internal survey, as of 31 December 2017.
38 BaFin, internal survey, as of 31 December 2017.

The product's vulnerability with regard to potential money laundering is therefore rated as low. The product can, in principle, be misused for money laundering purposes during the accumulation phase, but it is not very attractive to money launderers because of the smaller insured amounts.

4.2.2.4 Bank-like products

The term 'bank-like' products here covers capital redemption business and lending business. Capital redemption business primarily consists of money market and savings products. It currently accounts for just under 4% of new business in life insurance. Lending business primarily refers to mortgages and loans. Primary insurance undertakings (under BaFin supervision) currently have about 4% of their total investments in loans secured by mortgage (residential and commercial). Loans to business enterprises (excluding banks) account for about 1% of investments.[39]

Vulnerability with a view to potential money laundering is currently rated as medium-low. These not being core insurance products, there is a risk of individuals deliberately aiming to place incriminated funds with the insurance sector by means of capital redemption products. There is latent risk here due to insurers in some cases lacking awareness of the obligation to identify the counterparty and to ascertain the beneficial owner. In on-site inspections, BaFin has found isolated instances of money laundering reporting officers not including these products in ML prevention measures to the same extent as core insurance products.

In principle, all typologies are also relevant to the insurance sector with regard to bank-like products as have been defined for the banking sector. An example of a typology for the lending business is where illicit funds are laundered to an insurer by means of large extra payments on

39 BaFin, internal survey, as of 31 December 2017.

principal. This can also be done by early repayment of the loan. The money launderers also accept that this will incur prepayment penalties.

The Supervisory Authority will closely watch how bank-like products develop in terms of market share in order to be able to respond to changes in the market accordingly. In particular insurance undertakings which increasingly offer bank-like products should consider deploying an IT-based transaction monitoring system.

The table below shows the size and use of intermediaries in relation to each insurance product. These factors were among those taken into account in rating vulnerability.

Insurance products:	Total size/value of product	Average transaction size
Endowment life insurance and deferred annuity insurance (sold via independent brokers and online) with regular premium	high	medium
Endowment life insurance and deferred annuity insurance (sold via independent brokers and online) with single premium	medium-low	medium
Endowment life insurance and deferred annuity insurance (sold via tied agents and banks) with regular premium	low	low
Endowment life insurance and deferred annuity insurance (sold via tied agents and banks) with single premium	low	low
Term life insurance	medium	medium
Accident insurance with premium refund	low	medium
Bank-like products – capital redemption business	low	medium
Bank-like products – lending business	low	medium

Table 13: Total size/value of each product and use of intermediaries in insurance.

The table below shows insurance products in order of risk of being misused for money laundering and terrorist financing, commencing with (1) for the highest-risk product:

Insurance products:	Money laundering	Terrorist financing
Endowment life insurance and deferred annuity insurance (sold via independent brokers and online) with flexible premiums and payouts	1	5
Endowment life insurance and deferred annuity insurance (sold via tied agents and banks) with flexible premiums and payouts	2	6
Endowment life insurance and deferred annuity insurance (sold via independent brokers and online) with single premium	3	7
Endowment life insurance and deferred annuity insurance (sold via tied agents and banks) with single premium	4	8
Term life insurance	5	9
Bank-like products – lending business	6	9
Endowment life insurance and deferred annuity insurance (sold via independent brokers and online) with regular premium	7	3
Endowment life insurance and deferred annuity insurance (sold via tied agents and banks) with regular premium	8	4
Accident insurance with premium refund	9	2
Bank-like products – capital redemption business	10	1

Table 14: Ranking of insurance products by risk.

The ranking is based on abstract risk and disregards the total size of each product. Due to their increasing market significance, endowment life insurance policies and deferred annuity insurance policies with flexible premiums and payouts were subjected to separate assessment.

4.2.2.5 Assessment across all products

Where insurance undertakings offer lending business, capital redemption business or products with flexible premium and payout options, they should, with a view to the risk-based approach, apply a particularly critical appraisal to whether adequate ML/TF prevention requires an IT-based monitoring system. The outcome of this appraisal should in future be incorporated in their own risk analysis. The FIU and law enforcement agencies

voiced concerns that the low incidence of STRs from the insurance sector could be connected to the lack of IT-based monitoring systems. The FIU also raised concern about the fact that very few STRs related to premiums being paid by a party other than the policyholder. This typology also lends itself to IT-based monitoring. International insurance groups generally have IT-based monitoring systems and a number of other undertakings have already decided to deploy them. The Supervisory Authority is currently surveying the use of such systems in the insurance sector under its supervision and in case of doubt will raise the need for them with insurance undertakings on a case-by-case basis.

Risk profiles of insurance undertakings are compiled on the basis of reports by inter-nal audit functions in accordance with section 53 (2) of the Insurance Supervision Act and on the basis of on-site inspections. Insurers consequently have a special status in money laundering supervision and, while there are historical reasons for this, it also has specific implications for supervision by BaFin. BaFin is unable to stipulate requirements as to reporting by internal audit functions. Evaluating the submitted reports ties up considerable resources, as such evaluatoins cannot be systematised. To date, a relatively large number of on-site inspections by BaFin have been required in order to ensure examination by 'insurer-neutral' bodies.

In the course of work for the National Risk Assessment, a revision of the reporting obligations under the Audit Reports Ordinance (*Prüfungsberichteverordnung*)[40] was therefore advocated for reporting by credit and financial services institutions.[41] Cross-sectoral standardisation of reporting obligations towards the Supervisory Authority would further improve supervisory standards and further intensify the application of the risk-based supervisory approach.

40 Ordinance concerning the contents of auditors' reports on the annual financial statements and on the solvability of insurance undertakings (Prüfungsberichteverordnung/PrüfV).
41 See annex 5 to section 27 of the Audit Report Ordinance.

4.3 Securities sector

The subject matter of analysis in the securities sector comprises the 136 authorised and 314 registered asset management companies.[42] Securities business engaged in by banks is part of section 4.1.

As of the year-end 2017, asset management companies managed a total of 6,449 investment funds with assets of €2,062 billion. Of these, 2,417 were retail funds with assets totalling €498 billion and 4,032 were special AIFs with assets of €1,564 billion. Aggregate (net) cash inflows into retail and special funds amounted to €94.9 billion. (Gross) cash inflows amounted to some €332 billion, of which €115 billion was attributable to retail investment funds and €217 billion to special AIFs. This was set against cash outflows totalling some €237 billion.[43]

The threat of the sector being misused for money laundering is rated by the public agencies involved as medium overall. No rising or falling trend is seen in this regard. These assessments are based among other things on the fact that transactions in this sector tend to be complex and, particularly in the special funds segment, involve high volumes. Due to the generally high money laundering threat in the real estate sector[44], real estate funds are rated as particularly vulnerable. Recent industry figures clearly confirm the general trend towards investment in real estate. Open-ended real estate special funds in particular have recorded growing inflows of cash for years. Due to small numbers of investors and individual structuring of special funds, these are rated as being particularly vulnerable overall.

In 2017, the number of asset management companies authorised to manage open-ended real estate funds remained constant at 58. While 21 asset management companies also established open-ended real estate funds for retail investors, 37 limited their activities to the management of

42 BaFin, Annual Report 2017, p. 154.
43 See BaFin, Annual Report 2017, p. 155.
44 See section 5.1 for further detail.

open-ended real estate special funds. The fund volume of this market segment amounted to €92.33 billion as at the end of 2017. (Gross) cash inflows into open-ended real estate funds for retail investors amounted to €7.9 billion, the same as in the previous year. (Gross) cash inflows into open-ended real estate special funds increased for the seventh year in succession, to €16.2 billion (previous year: €14.9 billion). The fund assets of open-ended real estate special funds amounted to €88.2 billion at the end of 2017 (previous year: €75.6 billion).[45]

With regard to ML prevention, asset management companies that manage real estate funds in particular should question the source of funds, above all with larger transactions, and examine suitable documentary evidence as needed. Real estate sales carry high ML risk because of the sums involved are sometimes large.

The vulnerability of the securities sector's products to being misused for money laundering is rated medium-high. For consumer protection purposes, the Investment Code (*Kapitalanlagegesetzbuch*) distinguishes between asset management companies requiring authorisation and those which must only register before commencing operations. Retail investors within the meaning of the Investment Code cannot usually invest in investment funds issued by registered asset management companies. For this reason, registered asset management companies only have to meet some of the (verification) obligations that authorised asset management companies face under the Investment Code.

All asset management companies have identical obligations under the Money Laundering Act but their business models differ considerably. Closed-ended funds in particular are subject to great variety in terms of specialisation, asset competencies, product lines, corporate structures and service relationships. Determinations as to the sectoral ML threat therefore do not permit any direct inferences about the threat situation of any specific asset management company.

A key factor for assessment of an asset management company's threat situation is knowledge about the financial circumstances of its individual customers. Such information can be obtained if a customer's identity is known. However, as retail investment funds are not required to keep a register, many asset management companies do not know the identity of their individual customers. The situation is different where the custodian bank and asset management company belong to the same corporate group. In such cases, information from ongoing business relationships can be matched up and anomalous transactions more easily detected. Because of the heterogeneous nature of the sector, it is currently unclear whether all asset management companies are sufficiently aware of their individual money laundering risk. Two measures have been developed to raise risk consciousness throughout the sector:

1. In future, the money laundering part of the audit report on an authorised asset management company, in addition to the narrative presentation already required under section 13 of the Audit Reports Ordinance Concerning Certain Investment Undertakings[46], is to include a questionnaire with findings.[47]

2. A corresponding reporting obligation towards the Supervisory Authority should also be inserted for registered asset management companies with regard to ML/TF prevention quality. Various implementation options are currently being examined.

45 See BaFin, Annual Report 2017, p. 155-156.

46 Ordinance concerning the subject matter of the audit and the content of audit reports for external asset management companies, investment stock corporations, investment limited partnerships and funds (*Kapitalanlage-Prüfungsberichte-Verordnung*/KaPrüfbV).

47 See, for example, annex 5 to section 27 of the Audit Report Ordinance.

The fact that the number of STRs submitted by asset management companies to the FIU is in the low double digits confirms the necessity of these measures.[48] It should be noted, however, that in connection with purchases and sales of funds, depositaries (usually banks), where use of a depositary is mandatory, frequently submit an STR, as they match up their customer's financial circumstances against the transaction, which allows them to detect anomalies. Asset management companies, however, are obliged entities in their own right and are consequently required to submit STRs themselves.

A special section on the banking sector in the interpretation and application guidance under section 51 (8) of the Money Laundering Act is to be compiled in 2020.

4.4 Payment service providers

4.4.1 Money or value transfer services

Money or value transfer services (MVTS) or money remittance business within the meaning of section 1 (1) sentence 2 no. 6 of the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz) are services where funds are received from the payer, without a payment account being created in the name of a payer or a payee, for the sole purpose of transferring a corresponding amount to the payee or to another payment service provider acting on behalf of the payee, or where the amount is received on behalf of and made available to the payee. Before the Payment Services Supervision Act was introduced in 2009, money or value transfer services were regulated as a financial service under section 1 (1a) sentence 2 no. 6 of the former version of the Banking Act. ML/TF prevention was precisely the reason why this service was added to the Banking Act, and made subject to licensing, on entry into force of the sixth major revision of the Banking Act as of 1 January 1998. In 2009, on transposition into national law of the First Payment Services Directive, such services – among other types of business – were removed from the list of what constitutes banking business and brought under the 2009 Payment Services Supervision Act as a payment service. On transposition into national law of the Second Payment Services Directive of 2015 (Directive (EU) 2015/2366), the definition of money remittance given in that Directive was incorporated in section 1 (1) sentence 2 no. 6 of the 2018 Payment Services Supervision Act.

In Germany, the MVTS business is dominated by a small number of relatively large foreign payment institutions. These are generally represented on the German market by their distributors ('agents'). Electronic money institutions and payment institutions can operate money transfer by using agents. A distributor in the form of an agent within the meaning of section 1 (9) of the Payment Services Supervision Act is any legal or natural person acting as an independent businessperson providing payment services on behalf of a payment institution or an e-money institution. Who is an 'agent' is published in the payment institutes register of the payment institute's home member state. The various national registers are linked to form a Europe-wide register at the European Banking Authority.

The use of agents is common for institutions which operate into Germany as well as those which operate out of Germany. Agents serve as drop-in points for cash acceptance for the purpose of global remittances. The involvement of agents in the MVTS business significantly affects the ML/TF risks because it segments the business and thus makes risk management more demanding.

48 Over the period from establishment of the new FIU on 26 June 2017 to 29 May 2018.

In addition, a total of eight of the 35 payment institutions[49] in Germany provide MVTS. Their market share is small, however, at less than 5% of the total volume. Alongside these specialised providers, there are a number of banks – mostly branches or branch offices of foreign banks – that provide money transfer for casual customers in the form of what are called home remittances. Here, too, cash is accepted outside of an existing business relationship.

The threat of the sector being misused for money laundering and terrorist financing is rated by the public agencies involved as high overall, as the payments are generally made in cash and in many cases outside of an existing business relationship. The high cash intensity of MVTS is considered a notable risk driver in this connection. The large number of agents of international payment service providers means that there is always the possibility of the transferred amounts being used to support terrorist activities in crisis regions. No rising or falling trend is currently seen in this regard. The qualitative importance of MVTS for the economy as a whole is rated as low. The entire sector's business volume is in the single-digit billion range. The experts involved believe that a large proportion of the business goes unreported. This mostly relates to the provision of money transfer without a licence from BaFin. The unlicensed side of the business is often referred to as hawala banking. This is prohibited in Germany. Using its investigative powers, BaFin tracks down unlicensed operators, prohibits their unauthorised operations and, if necessary, winds up the unauthorised business activities. BaFin has a range of powers to investigate a case: It can issue requests for information and presentation of documents; measures can be directed at the hawaladar as well as at a person involved in the unauthorised operation. In addition, BaFin can inspect the premises and, if there is a court warrant, carry out searches. If unauthorised business activities are ascertained, BaFin can intervene. It can prohibit the unauthorised business activities and order that they be wound up. BaFin can also commission an outside party with the winding up. BaFin's measures can also be directed at persons involved in the *hawaladar*'s unauthorised business activities; for example, where funds are transferred using a bank, the bank can be ordered not to make any further dispositions without BaFin's consent. Measures imposed by BaFin must be enforced immediately. BaFin may publish the measures it imposes. BaFin has made the pursuit of unlicensed money transfer a focus of its supervisory activities in 2019. The Federal Government will continue to increase the resources for BaFin's enforcement activities. Detailed information on hawala banking is provided in section 3.

A relevant typology is the use of forged identity papers to transfer cash abroad. Agents occasionally act in collusion with customers in this regard. Transfers are also anomalous where there is no apparent family or business-related explanation for the frequency and size of the transactions.

A further typology is where payment institutions are misused by customers to conduct unlicensed money transfer. For example, a customer transfers funds, which have been accepted previously, in their own name. There are various indications (including STRs from operators) that acting in the capacity of agent is, in itself, occasionally misused as a 'cover' for unlicensed money transfer. It is not permitted for agents themselves to accept payment orders, even if they execute the orders using the institution, or to act on behalf of an unlicensed undertaking. An agent who accepts payment orders under which the payer's identity is concealed is not only in breach of obligations under the Money Laundering Act. The agent is also acting as an unlicensed undertaking by accepting the transaction amount other than on behalf of the institution.

Another phenomenon is the recruitment of individuals which are referred to as money mules

49 BaFin, internal survey, as of 30 June 2018.

(*Finanzagent*). A criminal recruits an unsuspecting account holder to act as a money mule. The money mule makes their own payment account available for transfers. Money is then paid into the account and the money mule is expected to transfer it as quickly as possible by 'cash transfer', using banks, among other channels, to a person located abroad. The reward is commission of between 5% and 20%, which the money mule is allowed to deduct from the transfer amount. Since a money mule helps to conceal the origin of unlawfully acquired funds, acting as a money mule can be a form of money laundering. The German term 'Finanzagent' – similar to the alternative term 'money transfer agents' in English – creates a possibility for confusion with registered agents under section 1 (9) of the Payment Services Supervision Act. Unlike registered agents, money mules do not act on behalf of a licensed institution.

It was reported in the private-sector consultation that, in addition to the corridors relevant for home remittances, there were also large numbers of transfers within Germany. Due to the relatively high transaction costs and the right to a basic payment account in Germany, transfers within Germany are ascribed a significant inherent risk. The legitimacy of such payments should always be subject to special scrutiny. According to law enforcement agencies, money or value transfer services are used, for example, when an account has been attached, in order to bypass the attachment with a transaction.

The de-risking carried out by many major banks in recent years also includes terminating correspondent banking relationships with high-risk jurisdictions.[50] This has caused a partial migration of transactions to licensed MVTS and also to unlicensed money transfer in the form of hawala banking. Law enforcement agencies take a critical view of this trend because it is almost impossible to trace incriminated funds in unlicensed money transfer and this significantly impedes investigation.

Agents in Germany do not have a licence of their own. As in other EU Member States, agents are used by a licensed payment or electronic money institution. They carry out money transfers on behalf of, and subject to the liability of, the foreign payment service provider and are contractually integrated into its organisation. In Germany, however, agents themselves are obliged entities under the Money Laundering Act. This goes beyond the minimum requirement under the Fourth EU Money Laundering Directive and the Directive amending the Fourth EU Money Laundering Directive. The necessity for this arose in 2011 in response to the changed market conditions following transposition of the First Payment Services Directive of 2007 into national law and the attendant implementation of the European passport for payment institutions. This was done, firstly, to counter the money laundering risks for Germany as a financial centre as a result of the initially unexpectedly large numbers of agents operating in Germany and, secondly, to enforce uniform anti-money laundering standards in Germany. To inform agents about their obligations under the Money Laundering Act, BaFin publishes a guidance notice on its website.[51]

Agents do not constitute a homogeneous sector. The bulk of agents are sole proprietors or micro-enterprises in the DNFBP sector such as call shops, kiosks and travel agencies. For such agents, money transfer is often merely a sideline. They are trained by the network operators and trust in the quality of that training. As well as these small individual enterprises in the DNFBP sector, institutions in the financial sector can also be agents. These institutions have comparatively high integrity standards and train their own staff in ML/TF prevention. Integrity is verified by the operator on registration. There is evidence with regard to some agents in the DNFBP sector of 'fronts' being used to circumvent signup verification.

50 See section 4.1.2.

51 BaFin, guidance notice (Merkblatt), "Hinweise für inländische Agenten gemäß § 1 Abs. 9 ZAG von Instituten mit Sitz im EWR nach dem Zahlungsdiensteaufsichtsgesetz (ZAG)".

Compliance with anti-money laundering obligations has been monitored since 2011 by BaFin staff, including by way of on-site inspections. Agents are not subject to any ongoing notification or reporting obligations towards BaFin, but have an obligation to provide BaFin with information and present documents. The 342 inspections carried out in the meantime[52] have led to improvement in the implementation of anti-money laundering standards among many agents. BaFin's supervisory activities have also resulted in a certain degree of market consolidation beneficial to the quality of preventive measures. There were still 8,600 agents active in Germany when checks began. This figure fell sharply to begin with and has settled down in recent years at about 5,500. Agents are registered in the register of institutions in the payment service provider's home Member State and are communicated to BaFin in notifications from home country supervisory authorities. As BaFin is not reliably notified when agents deregister, however, the current figure of 5,428 agents[53] is approximate.

In view of the particular threat posed by cash transfers by payment institutions and their agents, section 10 (4) of the Money Laundering Act stipulates a zero threshold for identification. Institutions are also subject to the Funds Transfer Regulation[54], which provides for the full traceability of transfers of funds between payment providers within the internal market. Traceability is likely to be more difficult, however, in the case of money transfers to Germany from a third country, notably with regard to the use of collective accounts for processing transfers. As Germany is a typical remitting country, however, traceability can be assumed to be good in most cases. Under section 10 (3) sentence 1 no. 2a of the Money Laundering Act, banks that offer MVTS outside of a business relationship must identify customers in the case of transfers upwards of €1,000.

The Supervisory Authority's level of information about market participants varies significantly. BaFin has wide-ranging information about the banks involved in the business. Firstly, the audit report on annual financial statements contains a reporting form under Annex 5 to section 27 of the Audit Report Regulation, with very clear information on the determination of inherent risk and the auditors' assessment of the precautions made by banks with regard to ML/TF. Secondly, BaFin has gained an insight into the business for some years by setting corresponding priorities in its own on-site inspections.

Payment institution auditors have been required up to now under the Audit Report Ordinance Concerning Payment Institutions (*Zahlungsinstituts-Prüfungsberichtsverordnung*)[55] to include an anti-money laundering section in their audit report on annual financial statements. In the narrative presentation submitted to date, however, auditors have not been under an obligation to assign a score to the measures taken. Based on the reports so far, BaFin rates staff integrity as high. Staff knowledge of anti-money laundering and the effectiveness of payment institutions' money laundering reporting officers are so far rated as adequate overall.

In the course of work for the National Risk Assessment, it was advocated that the reporting obligations for payment institutions be brought into line with those of credit and financial services institutions. In response, the Audit Report Ordinance Concerning Payment Institutions was revised accordingly in December 2018. The revised Ordinance contains a reporting form, based in substance on Annex 5, for the description and assessment of the arrangements for preventing money laundering and terrorist financing. This standardisation has considerably facilitated analysis by BaFin. Firstly, the scoring of auditor findings provides a clear initial impression of the overall situation with regard to ML/TF prevention and, secondly, information on inherent risk is included from institutions' own risk analysis

52 BaFin, internal survey, as of 31 December 2018.
53 BaFin, internal survey, as of 30 June 2018.
54 Regulation (EU) 2015/847.
55 Ordinance concerning the auditing of the annual financial statements of payment institutions and electronic money institutions and the reports to be compiled on such audits.

that would otherwise have to be requested from them on a case-by-case basis. The revision of the Audit Report Ordinance Concerning Payment Institutions also extends the risk-based reporting cycle to payment institutions.

With regard to agents, the Supervisory Authority previously only had notifications from home country supervisory authorities. Those notifications only stated an agent's name, contact details, management, type of payment services provided and internal control mechanisms. They provided BaFin with an overview of all agents active on the German market, but did not provide any support for a risk-based supervisory approach. In light of the fact that agents in Germany are obliged entities – an exceptional feature, internationally – and in light of the information available to date, supervision of agents is successful by international standards. The efficiency of the supervisory approach is limited, however, because supervision of the large numbers of agents through agent inspections alone ties up too much human resource capacity. Scope for improvement lies adjusting towards placing a greater emphasis on the significance of and the risk arising from each agent. It should also be noted that systemic deficiencies in an agent network can only be remedied by the network operators themselves, and not by sanctioning individual agents. Any such deficiencies should therefore be brought to the attention of the operators. In the past, the major operators had set up voluntary contact points, in particular for liaison with the FIU and law enforcement agencies. They did not constitute a binding point of contact for the Supervisory Authority, however.

In the course of work for the National Risk Assessment, it became clear that BaFin should obligate foreign payment service providers to appoint a central contact point[56] if the specific risk situation so warranted. Using the existing statutory provision under section 41 (1) of the Payment Services Supervision Act, this requirement was announced at the beginning of 2019 to operators in Germany that meet the criteria.[57] The central contact point will provide the Supervisory Authority in future, among other things, with the following data:

- Number of active and inactive agents in Germany
- Volume of payments and aggregate number of payments executed in Germany
- Volume of payments and number of payments executed in Germany per agent
- The three highest-volume corridors
- Date agent last received anti-money laundering training

The central contact point is also the permanent point of contact for the FIU and law enforcement agencies. The information provided by the central contact points enables BaFin to carry out its supervisory activities with regard to agencies on a risk basis. In view of the heightened threat situation, the supervisory activities are also to be widened in scope. In the private-sector consultation in November 2018, all involved welcomed the introduction of central contact points.

Agents themselves are under obligation to submit STRs. It is necessary for agents themselves to be under obligation to submit STRs under the Money Laundering Act particularly in the case of multiple agents. With multiple agents, the agent is the only one to have a full view of a customer's transactions. The bulk of STRs in connection with the MVTS business are submitted for national agents by the major foreign operators of agent networks – mostly by way of contractual outsourcing. According to the payment institutions, agents are free to submit

56 Central contact point (CCP) under the Second Payment Services Directive, Directive (EU) 2015/2366.

57 See Article 3 (1) of Delegated Regulation (EU) 2018/1108 of 7 May 2018.

STRs themselves or pass on a matter to operators for further investigation. Since the new FIU commenced operations, a total of some 7,000[58] STRs have been submitted by the three major operators. The matters reported were mostly cases where the frequency or size of transactions appeared anomalous because no family or business-related explanation was apparent to the obliged entity. More detailed information on payers, payees or the background to payments was not provided.

A central finding of BaFin's inspections of agents is that agents generally do not receive any feedback as to whether a suspicious transaction they have reported internally has resulted in an STR to the FIU under section 43 of the Money Laundering Act. This generally results in STRs being submitted by the BaFin inspectors under section 44 of the Money Laundering Act. BaFin has submitted 601 STRs under section 44 of the Money Laundering Act due to findings in inspections of agents since 2012.[59] The failure of operators to provide feedback to agents is a problem because, despite the use of outsourcing, agents remains ultimately responsible for complying with the obligation under section 43 of the Money Laundering Act and must therefore retain the possibility of submitting an STR themselves if the institution does not do so. In the course of the future working relationship with the central contact point, the quality of individual STRs is to be further improved in order to enhance their value to law enforcement agencies. Possibilities here include the ability to trace STRs back to the agent who submitted the internal report, establishing feedback from operators to agents on STRs submitted, and ensuring that the information provided is as detailed as possible. Initial discussions between individual providers and the FIU took place in late 2018 with a view to intensifying cooperation and improving the quality of STRs.

The power to impose fines and issue cautions has considerable practical relevance for the supervision of agents as the notification procedure means that BaFin has no advance influence over market entry.

In 2016, BaFin issued agents with 19 cautions and imposed 48 fines. In 2017, BaFin issued agents with 10 cautions and imposed 28 fines. In 2018, BaFin imposed 26 fines. In the 23 June 2017 revision of the Money Laundering Act, the obligations on agents and consequently the fineable offences were transferred from the Payment Services Supervision Act to the Money Laundering Act. This raised the standard of fault required for breach of obligations to be subject to a fine from negligence to recklessness. As a result, the number of fines decreased in 2017.

In the course of work for the National Risk Assessment, it became clear that, for the following infringements in particular, effective supervision of agents requires the ability already to impose fines if the infringements are committed negligently, as these cover the bulk of findings in on-site inspections:

- Failure to identify the contracting party or failure to do so completely
- Failure to ascertain the existence of a beneficial owner
- Failure to record information collected or obtained or failure to do so correctly or completely.

BaFin has submitted a corresponding proposal for amendment of section 56 (1) of the Money Laundering Act in the course of transposing the Directive amending the Fourth EU Money Laundering Directive into national law. This amendment would affect the standard of fault for all obliged entities and would also significantly facilitate sanctioning by supervisory authorities for the DNFBP sector.

58 Over the period from establishment of the new FIU on 26 June 2017 to 29 May 2018.
59 BaFin, internal survey, as of 31 December 2018.

4.4.2 Electronic money

'Electronic money' is a legal term, created on the basis of requirements under EU law, and typologically only shares certain elements with the economic phenomenon of electronic money. Its predecessors are the prepaid card business (section 1 (1) sentence 2 no. 11 of the former version of the Banking Act) and the network money business (section 1 (1) sentence 2 no. 12 of the former version of the Banking Act), which were newly inserted into the list of what constitutes banking business on entry into force of the sixth major revision of the Banking Act as of 1 January 1998. On entry into force of the Fourth Financial Market Promotion Act (*Viertes Finanzmarktförderungsgesetz*) as of 1 July 2002, the foregoing two definitions were combined under the term electronic money business (section 1 (1) sentence 2 no. 11 of the former version of the Banking Act) and legislated as the issuance and management of electronic money. On transposition into national law of the fully harmonised Second Electronic Money Directive of 2009, the definition of electronic money business within the meaning of section 1 (1) sentence 2 no. 11 of the former version of the Banking Act was taken out of the list of what constitutes banking business within the meaning of section 1 (1) sentence 2 of the Banking Act and transferred in modified form in 2011 to section 1a (2) of the Payment Services Supervision Act 2009.

Electronic money is all electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of fund for the purpose of making payment transactions and which is accepted by a natural or legal person other than the issuer. The electronic money business is the issuance of such electronic money. Banks and electronic money institutions are authorised to issue electronic money in Germany. Seven electronic money institutions are licensed for the purpose by BaFin. The bulk of electronic money issuers on the German market are from other European countries and either use a branch in Germany or operate in Germany exclusively on a cross-border basis.

A defining feature of electronic money is a central entity that issues a prepaid stored value that can be used for payments to third parties. Examples of electronic money include prepaid cards, electronic vouchers, electronic wallets (also known as e-wallets or digital wallets) and prepaid credit cards. A prepaid credit card is generally understood to be a prepaid, reloadable prepaid card from an international card organisation such as Visa or Mastercard.

Electronic money institutions can use electronic money agents for the distribution and redemption of electronic money. An electronic money agent is any natural or legal person acting as an independent businessperson on behalf of the institution in the distribution and redemption of electronic money. Illegally earned money can primarily be laundered into the legal financial and economic cycle wherever prepaid cards are loaded. The distribution of electronic money through independent electronic money agents (such as kiosks and filling stations) significantly heightens the vulnerability of the electronic money business to ML/TF risks because it results in a segmentation of the business. The large number of parties involved places increased demands on risk management in the mostly foreign institutions. Use may also be made of online distribution intermediaries.

Due to the high inherent risk in principle of electronic money being misused for money laundering and terrorist financing, the European and in particular German legislators have imposed very strict requirements with regard to those misuse risks. Many risks are thus already mitigated by stipulations on specific product features or the distribution structure. The individual product features and distribution

channels are consequently tied to due diligence requirements that are graduated according to risk.

The threat of the sector being misused for money laundering and terrorist financing is therefore rated by the public agencies involved as low overall. No rising or falling trend is seen in this connection.

The vulnerability of electronic money products to being misused for money laundering and terrorist financing is rated as medium-high. This vulnerability is further reduced as a result of the mitigating measures taken by legislators, the Supervisory Authority and the sector itself.

One typology is what can be referred to as 'cross-loading' in conjunction with the use of prepaid cards on a credit balance basis. This involves the card being loaded by various third parties who have no direct link to the cardholder and usually also hold prepaid cards themselves. In this way, a large amount can be stored on a single prepaid card.

Anonymous prepaid cards known as open-loop cards that can be used at numerous acceptance points in principle pose a heightened ML/TF risk. These involve the card issuer and the many acceptance points. One example can be found in the prepaid credit cards from the major credit card organisations. Legislators recognised this risk at an early stage and have always legislated low thresholds. Among other restrictions, section 25i (2) of the Banking Act currently provides for a threshold of €100. Below this amount, customers do not have to be identified. No further reduction in the threshold is therefore needed in Germany in order to transpose the Directive amending the Fourth EU Money Laundering Directive into national law. Measures taken by institutions themselves to protect customers and prevent fraudulent use can further reduce the inherent risk. A serious risk, however, is posed by anonymous electronic money issued in third countries, which can significantly exceed national thresholds, and by products for which identification is required but which are from jurisdictions with significantly lower customer identification standards.

The combination of cash with an anonymous electronic money product constitutes a heightened abstract risk of terrorist financing because in principle it means an amount can be used anywhere in the world. In the opinion of the public agencies involved, however, ML/TF vulnerability is only related to a limited extent to a product's potential for anonymity. European products not requiring identification have only limited suitability for money laundering because of the low thresholds and other product restrictions. In terrorist financing, too, anonymity ceases to play a decisive role beyond a certain stage in preparations for a specific terrorist act. Electronic money products that require identification are more attractive in such cases because of the larger values they can store. This is because product vulnerability cannot be equated with the book money on a current account because electronic money issuers have far more limited scope for monitoring. For example, it is difficult or impossible to judge a customer's financial circumstances, there is no way of determining what size of transaction is normal for the customer without additional information, and it is also hard to ascertain the origin of funds that are merely transferred or debited from a reference account. Issuers are forced to rely instead on parameters relating to individual transactions, as these are their primary information source. Market participants state that they have placed special focus on systems to this end in recent years and subject such systems to continuous improvement. In the course of expanding ongoing supervision in this sector, BaFin will pay increased attention in future to risk adequacy in monitoring systems.

The use of monitoring systems in particular enables the sector to filter out anomalies and

thus submit STRs. Electronic money institutions have submitted about 100 STRs since the FIU commenced operations.[60] A large proportion of these, however, do not relate to conventional electronic money business, but to anomalies in financial transfer services, as a number of institutions are agents for foreign payment service providers. Relevant STRs related, for example, to the size of amounts loaded on prepaid cards, and in particular also to card loading by third parties.

The same applies to electronic money institutions as applies to payment institutions with regard to revision of the Audit Report Regulation Concerning Payment Institutions.

4.5 Other financial services

The following presents other services that are financial services within the meaning of section 1 (1a) sentence 2 of the Banking Act. Among those financial services, foreign currency dealing and factoring were rated as particularly susceptible to money laundering. These are considered in greater detail in the following.

4.5.1 Foreign currency dealing

Foreign currency dealing is operated in Germany by specialised bureaux de change and also by banks. The business includes exchanging legal tender banknotes and coins and the purchase and sale of traveller's cheques. Most banks provide foreign currency dealing for customers only; some no longer offer it at all. In most cases, foreign currency can only be ordered and redeemed via an account with the bank, meaning on a non-cash basis. Because there is an existing business relationship, such instances are not considered to involve heightened ML risk. The situation is different, however, with entities that provide foreign currency dealing for casual customers, and notably with bureaux de change. Bureaux de change mostly rely on casual custom. The following therefore relates to cash-based foreign currency dealing with casual customers.

Supervision of foreign currency dealing is subject to national legislation only and was introduced with the sixth major revision of the Banking Act. Since 1 January 1998, commercial foreign currency dealing has been classified as one of the financial services (section 1 (1a) no. 7 of the Banking Act). Placing it under supervision exclusively served the purpose of AML/CFT. The market declined sharply at first following the introduction of the euro, and for some years now has been constant or in slow decline. There are currently ten bureaux de change licensed by BaFin that specialise exclusively in foreign currency dealing and have been under supervision for many years.[61]

The threat of the sector being misused for money laundering and terrorist financing is rated by the public agencies involved as high overall. This assessment is primarily based on the fact that most transactions are in cash and many are below the threshold at which identification is required. Foreign currency dealing can also be one link in the chain comprising an international transaction and may have the purpose of interrupting the paper trail. No rising or falling trend is seen in this connection.

The vulnerability of foreign currency dealing to being misused for money laundering is rated medium-high. Foreign currency dealing is subject to enhanced due diligence requirements under section 25k (1) of the Banking Act. Irrespective of any specific thresholds under the Money Laundering Act, the general due diligence requirements under the Money Laundering Act must be fulfilled in the case of transactions with a value of €2,500 or higher that are not settled using an account that the customer has with the same institution. For transactions below this identification threshold, no records are usually

60 Over the period from establishment of the new FIU on 26 June 2017 to 29 May 2018.

61 BaFin, internal survey, as of 31 December 2018.

kept that allow them to be traced to the customer. Monthly returns from the bureaux de change show that untraced transactions account for the largest share. This anonymity limits the ability to monitor for smurfing. Prevention of smurfing in particular critically depends on employee vigilance. This vigilance is notably ensured by targeted training and a corresponding corporate culture. As the bureaux de change have been under BaFin supervision for over 20 years, AML awareness is very strong and there is intensive contact with the Supervisory Authority. For example, they have to submit to the Supervisory Authority audited annual financial statements with the reporting form under section 27 of the Audit Report Ordinance. The Supervisory Authority uses the resulting data to compile individual risk profiles.

Bureaux de change that exclusively specialise in foreign currency dealing have submitted a double-digit quantity of STRs since the FIU commenced operations.[62] Most of these related to foreign currency transactions carried out close to the Swiss border or in airport branches where customers provided no information on the source of the funds, or where the information they did provide was contradictory. In isolated cases, STRs were submitted in connection with the use of forged identity documents.

4.5.2 Factoring

Supervision of factoring is subject to national legislation only and was introduced with the 2009 Annual Tax Act (*Jahressteuergesetz 2009*) of 24 December 2008. It was placed under supervision because of its comparability with banks due to the financing function; among other things, factoring involves granting a bridging loan up to the due date of a receivable. There are 186 institutions which provide factoring alongside finance leasing[63].

The threat of the sector being misused for money laundering is rated by the public agencies involved as medium overall. No rising or falling trend is seen in this connection.

The vulnerability of factoring to being misused for money laundering is rated medium. In the business relationship between a factoring institution and a factoring customer, actual payments by debtors are made as a rule on a non-cash basis using banks, for example by direct debit or bank giro transfer. The debtor is not always known at the time the factoring agreement is entered into, or there is not always full information on the company concerned. This constitutes a heightened ML risk. Under section 25k (2) of the Banking Act, factoring institutions must therefore take reasonable measures to combat a perceptibly higher risk of money laundering when accepting payments from debtors who were unknown when the factoring agreement was entered into. The risk also depends on what is being factored. Attractive items for money launderers include sales of high-priced goods such as jewellery or the billing of expensive services where it is hard to verify that the services have actually been performed. The addition of the factoring institution as an intermediary interrupts the paper trail associated with the payments, making transactions difficult or time-consuming to trace.

Risk-based supervision of the sector in relation to ML/TF has been established since the beginning of 2018. This supervision was previously integrated into sectoral supervision under the Banking Act. Supervision specifically for ML/TF will further improve the quality and effectiveness of the supervision process. In particular, it is necessary to raise awareness in the sector with regard to the possibilities for ML and TF. One possible approach, for example, would be targeted training courses by factoring institutions in which relevant money laundering transactions are explained to staff in detail. The narrow scope of the

62 Over the period from establishment of the new FIU on 26 June 2017 to 29 May 2018.
63 BaFin, internal survey, as of 30 June 2018.

business would enable strong focus and efficient implementation here. This could also result in an increase in the numbers of STRs submitted by the sector. Past reporting has always been at a low level (for example with a single-digit number of STRs a year in North Rhine-Westphalia).

In the course of work for the National Risk Assessment, international factoring was identified as an important factor for risk-based supervision. Export and import factoring both play a part here. Export factoring is where domestic companies (exporters) use a factor in Germany for their cross-border trade. Import factoring is where foreign companies use a factor in Germany for imports. In these forms of international factoring, factoring is done either directly or through a factoring partner for international cooperation in the countries concerned. Looking ahead, BaFin will examine what role international factoring plays for the German market and on what scale the individual factoring institutions are involved.

4.6 New phenomena in the financial sector

4.6.1 Fintechs

There is no uniform or binding national or international definition of fintech. Fintech business models are diverse and – depending on how they are implemented – may require a license from BaFin. The term 'fintech' is short for 'financial technology' and refers to undertakings or units of existing undertakings that combine financial services with modern, innovative technologies. Products and services offered by the new market players tend to be Internet-based and application-oriented. Fintechs aim to add value for customers with benefits such as ease of use, efficiency, transparency and automation. Rather than always being in competition with them, some fintechs also complement the conventional service providers such as banks, insurers and securities firms. They are drivers of digital innovation across the entire financial market.[64]

In view of the issue's major relevance, the Federal Ministry of Finance established a Fintech Council on 22 March 2017. Two years after its foundation, the Fintech Council convened for the first time with its new members on 21 March 2019. It is currently made up of 29 members, who are experts in questions of digital technology and how it impacts the financial market. They advise the Federal Ministry of Finance and the Federal Government on a voluntary basis, providing input on subjects including artificial intelligence, cloud computing, blockchain and data protection. The Council will continue to convene at least twice a year at the Finance Ministry. The Fintech Council creates a dialogue that is grounded in the practical realities, thus contributing to a better understanding of technological developments and the potential, the opportunities and the risks that they open up. In this, the Council ultimately helps boost Germany's standing as a financial location.

The European Commission also published a FinTech Action Plan on 8 March 2018 to find answers to the numerous challenges arising from the rapid pace of innovation in the financial sector.

In the course of the National Risk Assessment, it was determined that the fintech nature of an undertaking does not automatically mean heightened ML/TF risk relative to other undertakings in the same sector. This is because fintechs requiring a license, rather than offering new products, merely tend to sell their products – such as current accounts or health insurance policies – in an innovative manner. Heightened ML/TF risk can nevertheless always result from the specific business model. This could arise, for example, where an established provider cooperates with a fintech that is not subject to licensing.

64 See BaFin, Annual Report 2015, p. 20.

Supervision of fintechs is governed by the principle of 'same business, same risk, same rules' in conjunction with the proportionality principle. If a fintech operates a business for which it requires a license, it is supervised like any other undertaking in the same sector.

There are a large number of diverse business models in the fintech sector. The recent past has consequently seen a massive rise in the number and complexity of issues involved in assessing specific fintech business models for licensing requirements under supervisory legislation (such as the Banking Act, the Investment Code, the Insurance Supervision Act and the Payment Services Supervision Act). Whether a fintech's business model requires a license under supervisory legislation depends on its specific implementation.

Among banks especially, there is frequently cooperation between established banks and fintechs with aims such as making specific bank products more user-friendly. If a fintech carries out transactions relevant under the Money Laundering Act on behalf of a bank, the bank is responsible as the obliged entity for the transaction's proper execution. An urgent concern of the Supervisory Authority is to ensure that all requirements under the Money Laundering Act are met in the process. In light of this standout role of banks as the point of intersection with other fintechs whose business model is not subject to supervision, BaFin has established a Fintech Competence Centre. This pools all responsibilities in connection with fintechs. The staff involved can thus closely examine each business model and above all make cross-comparisons so as to spot trends and developments at an early stage, gauge their supervisory relevance and take any action needed.

The money laundering potential of fintech business models varies with their proximity to the actual provision of payment services. ML potential tends to be low with pure-play technology providers that cannot be used to carry out transactions themselves. The risk is significantly greater with fintechs that provide payments (and most of all money transfer providers) or accept funds.

Fintech-related STRs submitted to the FIU confirm this finding. In addition to STRs from fintechs that require a license, most of which are registered as a financial services provider or credit institution, the FIU also encounters reference in STRs to fintechs that are domiciled abroad. These are primarily providers of money transfers and providers of access to and trade in crypto assets. The number of STRs and transactions identified for the latter group runs into four digits. There are scarcely any STRs for other sectors where fintechs are fundamentally active.

The subject of crypto assets is covered in detail in section 6.

4.6.2 Crowdfunding

The term 'crowdfunding' generally refers to the direct funding of specific projects by a large number of donors. Fundraising usually takes place online. Crowdfunding platforms offer an alternative to conventional sources of finance such as loans, venture capital, business angels and subsidies.

Crowdfunding platforms are very varied in their implementation. Four main models are distinguished in practice: donation-based and reward-based crowdfunding, which are also known as crowd sponsorship, and crowd lending and crowd investing, where the lender or investor speculates on financial gain. Not all crowdfunding platforms and projects neatly fit under one single model. A research report compiled on behalf of the Federal Ministry of Finance by researchers at ifo Institute, Trier University and

Humboldt-Universität zu Berlin provides an overview of crowd investing platforms in the German market.[65] The focus in terms of anti-money laundering law is on crowd lending and crowd investing. Donation-based crowdfunding and crowd lending are most relevant to terrorist financing.

In practice, business models tend to be such that crowd investing platforms act as financial investment intermediaries within the meaning of section 34f of the Trade Regulation Code (*Gewerbeordnung*) and crowd lending platforms as loan intermediaries within the meaning of section 34c of the Trade Regulation Code. No cases of money laundering via crowdfunding platforms in Germany have yet come to light. The public agencies involved nevertheless see a potential ML/TF risk due to the anonymity that is generally possible in connection with these funding methods. This is still a relatively recent issue and is continuously monitored due to the abstract risk situation in order to respond to new developments at short notice. The assessment of the ESAs in revision of the Risk Factors Guidelines will also be taken into account in the course of ongoing monitoring.

4.6.3 Mobile money

Mobile money transfer and in particular the M-Pesa system most widely known in Africa has not yet become established in Germany as a pure mobile payment system. This is expected to gain importance in the years ahead, as trends in the USA and China show. Primarily because of the regulatory regime applicable in Germany, however, it is expected that the risk of misuse for terrorist financing will remain low.

65 See Federal Ministry of Finance, Praxiserfahrungen mit den durch das Kleinanlegerschutzgesetz vom 3. Juli 2015 eingeführten Befreiungsvorschriften in § 2 a bis § 2 c Vermögensanlagengesetz (Experiences in practice with the exemption regulations in sections 2a–2c of the Capital Investments Act introduced by the Retail Investor Protection Act of 3 July 2015), p. 19.

5 Designated non-financial businesses and professions (DNFBP) sector

5 Designated non-financial businesses and professions (DNFBP) sector

5.1 Real estate sector

The German real estate market is of great global importance and is particularly attractive both to international and to national investors. Real estate is highly important to the economy and society overall. High transaction amounts and stable values make real estate among the most important investment choices in Germany. This makes the German real estate sector susceptible to money laundering activities and makes it an elevated risk sector. As in other sectors, there is an added possibility of concealment both of the source of funds and of the related ownership structures due to the multitude of options for the legal structuring of real estate transactions available to domestic and foreign legal entities and also to private individuals.[66] The money laundering risk for the German real estate sector is therefore rated as high overall. Terrorist financing risk is rated as medium.

As property owners in Germany are recorded in the land register, there is mostly a high degree of transparency regarding ownership. It should be noted in this connection that the *Länder* are currently developing a nationally uniform land register database. A joint *Länder* portal based on this allows nationwide data queries, notably for law enforcement agencies.

Despite the high degree of transparency regarding ownership due to the land registers, the public agencies involved in the Assessment single out two situations in which incriminated assets are harder to trace. This is always the case when beneficial ownership of a property and formal ownership of the same property diverge. Deeply interlocking structures and networks of companies are susceptible to this, as are arrangements where property is held for another party (such as in trust or acting for an undisclosed principal). In light of this, the real estate sector, like other sectors, is subject to particular risk of money laundering due to the effective anonymity that can be achieved with the aid of share deals and interlocking shareholdings (especially involving foreign shell companies).

Share deals are real estate investments where the investors, rather than acquiring a property themselves, buy shares in a property vehicle that itself holds one or more properties. The property continues to be owned by the property vehicle, while investors only acquire indirect ownership of it by virtue of being shareholders as a result of the share deal. Legally speaking it is a purchase of a business enterprise or an interest in a business enterprise and not a real estate purchase. It should be noted in this connection that a purchase of shares in an *Aktiengesellschaft* (a public limited company) does not normally have to be notarised. A share purchase agreement only needs to be notarised if shares in a GmbH (a private limited company) are transferred or encumbered or an obligation to do so is created (on acquiring a GmbH & Co. KG – a limited partnership where the general partner is a GmbH – both the acquisition of the shares in the GmbH and the acquisition of the limited partner shares must normally be notarised because they constitute a single legal transaction). Share deals can therefore be used deliberately to bypass notaries. In light of this, credit institutions in particular that finance or advise on share deals should be especially vigilant with

66 See FIU key issues paper: Priority risk areas in FIU operations to combat money laundering and terrorist financing, 2019.

a regard to any ML/TF risk. Lawyers, auditors, tax advisers and notaries who are involved in or advise on the structuring of such transactions should likewise exercise particular vigilance and keep a constant watch on the risks described in this context.

The public agencies involved in the National Risk Assessment assume that evading mechanisms will gain in importance in the real estate sector as in other sectors due to the reform of the law regarding asset recovery (for more on asset recovery, see section 3.1.5.5). Since then, it is thought that, rather than luxury properties being purchased for money laundering purposes, such properties may increasingly be rented using incriminated funds. Risk consciousness among estate agents acting as letting intermediaries is therefore particularly important. This phenomenon will be regularly evaluated and monitored in future. The Directive amending the Fourth EU Money Laundering Directive now stipulates that in addition to estate agents acting for the sale and purchase of real estate, agents acting as letting intermediaries are now also subject to anti-money laundering law in relation to transactions where the monthly rent is upwards of €10,000. This requirement will be transposed into national law in the Money Laundering Act as of 10 January 2020.

Most STRs on the real estate sector have so far been submitted by credit institutions, followed by public agencies and other obliged entities that send intelligence from real estate transactions and tax audits to the FIU.[67] Only occasionally are STRs submitted in this sector by estate agents, notaries and lawyers, even though these professions are frequently and closely involved in transactions. From a preliminary survey, the FIU has received over 1,000 STRs (from 2017 and 2018) in connection with real estate transactions. 80% of these came from the financial sector, 6% from the DNFBP sector, and 14% from public authorities and other reporting entities. A priority is therefore on further raising awareness among obliged entities in the DNFBP sector in order to further improve AML/CFT in the real estate sector. To this end, the FIU has published a paper on indications of money laundering and terrorist financing in the real estate sector, although this work is not yet complete. In some cases, however, a suspicion of money laundering or terrorist financing can be based on other indications. A risk-based approach should therefore be taken to assess whether a case in question might involve money laundering or terrorist financing.

A case study on organised crime in the 'clan' milieu showed that auctions pose heightened ML risk, particularly in view of the large cash payments that are seen in this connection. According to the police forces involved in the National Risk Assessment, auctions are frequently used by suspected criminals to acquire real estate or high-value goods. The groupings in question increasingly used foreclosure auctions to purchase real estate with incriminated funds. The Federal Government takes these findings from the National Risk Assessment very seriously and will therefore make auctions by public authorities subject to anti-money laundering obligations in future. Corresponding provisions are included in the draft act for transposition into national law of the Directive amending the Fourth EU Money Laundering Directive.

5.2 Trade in goods

Traders in goods are obliged entities under section 2 (1) no. 16 of the Money Laundering Act. The Money Laundering Act clearly defines which undertakings constitute traders in goods. Traders in goods are defined as anyone who sells goods commercially, no matter on whose behalf or for whose account they trade (and hence also include, for example, auctioneers, commercial agents and commission agents). Obliged entities in this group only need to establish a risk management

67 See FIU key issues paper: Priority risk areas in FIU operations to combat money laundering and terrorist financing, 2019.

system if they accept or pay out at least €10,000 in cash. The first cash payment in such an amount triggers the risk management obligation. Money laundering risk for trade in goods was rated in the National Risk Assessment as medium-high. Terrorist financing risk was rated medium.

Due to the large sums involved, trade in high-value goods (notably luxury goods, motor vehicles and antiques) is generally also suited to laundering incriminated funds into the legal economy.[68] The motor vehicle trade (and, most of all, the used car segment) is highly significant in terms of money laundering because many transactions are made in cash. It should also be noted in this connection that unlike its neighbours, Germany does not set any upper limit on cash payments. In the luxury cars segment especially, therefore, the motor vehicle trade[69] is particularly well suited to the laundering of incriminated funds into the economy. The high risk-affinity of the motor vehicle trade in Germany was recently confirmed by the success of a Europol investigation (Operation Cedar). A professional money laundering organisation in Germany, among other countries, was shown to use incriminated funds to buy used cars and other luxury goods (boats, works of art, construction machinery, etc.) and then export them and resell them abroad in order to conceal the incriminated source of the funds used. At its height, €1 million a week is estimated to have been laundered in this way Europe-wide.

From past clearing and money laundering investigations, the investigating authorities report that the trade in or the purchase of vehicles of all kinds is frequently given as the reason for carrying, in some cases very large, amounts of cash discovered in controls at home and abroad. Trade in vehicles, works of art and also construction machinery is also repeatedly stated as the reason for physically carrying cash in instances where cash is properly declared on entering or leaving the country. Experience has shown that incriminated cash from neighbouring European states is frequently brought into Germany in this way for money laundering purposes. This is often performed by cash couriers who work in closed groups, have no relation to the predicate offence and move what can easily amount to several hundreds of thousands of euros around Europe by land. Funds are thus used to buy vehicles, construction machinery and so forth in cash and hence laundered into the Germany economy almost without detection. In some cases, cash couriers use registered car dealerships of their own for this purpose. Alternatively, where the sum to be laundered is too big or anomalous for a single firm, the cash may be deliberately spread across multiple cooperating car dealerships. The money is then usually transferred back by selling the vehicles abroad and exporting them. Anomalous features of this modus operandi include:

- Strict and clear separation between predicate offence and money laundering activities
- Use of networks of companies in Germany and abroad
- Closed nature of the money laundering groupings
- Use of cash-intensive lines of business for placing the funds
- Commingling of legal and illegal business activities
- Avoidance of the banking sector in Germany/Western Europe due to the AML arrangements in force.

68 See FIU key issues paper: Priority risk areas in FIU operations to combat money laundering and terrorist financing, 2019.

69 See also Typologiepapier – Besondere Anhaltspunkte für Geldwäsche im Kfz-Handel – Verpflichtete nach § 2 Abs. 1 Nr. 16 GwG (Typologies – Special indications for car dealerships – obliged entities under section 2 (1) no 16 of the Money Laundering Act), FIU, 2018.

According to a preliminary survey, since the FIU was brought under the Central Customs Authority, it has received about 640 STRs that were either submitted by car dealers or where "anomalies in connection with the sale/purchase of motor vehicles" were stated as the reason for the report.[70] 65% of these reports came from the financial sector, 30% from the DNFBP sector, and 5% from public agencies and other obliged entities.

Regarding the high-value art trade, cases have been observed in the past of expensive works of art being brought under or bought and sold by offshore companies. It can be assumed that this is often done to achieve anonymity in order to facilitate money laundering activities. The art trade in general is rated as vulnerable to money laundering. On transposition into national law of the Directive amending the Fourth EU Money Laundering Directive, art storage providers will also become obliged entities in addition to the art trade intermediaries that are already obliged entities as traders in goods under the Money Laundering Act. An art trade intermediary is anyone who commercially arranges contracts of sale or for the rental of works of art. Under Article 2 (1) (3) (i) of the Directive, art trade intermediaries for this purpose specifically include art galleries and auction houses. The activities of art trade intermediaries who already came under the definition of traders in goods under the previous law because of trading on another's behalf or account (see section 1 (9) of the Money Laundering Act) now come under the definition of the art trade intermediary. Works of art are all items listed under heading 53 of Annex 2 to section 12 (2) no. 1 and no. 2 of the Value Added Tax Act (*Umsatzsteuergesetz*). These include pictures, original engravings and original sculptures and statuary. Art storage providers are subject to the requirements of the Money Laundering Act where storage takes place in a free zone within the meaning of Article 243 onwards of the Union Customs Code (UCC). Free zones within this meaning on German territory are the free ports of Bremerhaven and Cuxhaven.

70 See FIU key issues paper: Priority risk areas in FIU operations to combat money laundering and terrorist financing, 2019.

Regarding the trade in precious stones and precious metals, there are indications of this sector being highly susceptible to money laundering. In has been known to be common for the €10,000 threshold on cash payments to be deliberately circumvented. Various supervisory authorities and the *Länder* report that there have been frequent cases of an amount below that threshold being selected in cash sales in order to prevent identification. Consideration should therefore be given to creating an identity verification requirement for cash payments upwards of a significantly smaller threshold amount. A lowering of the cash threshold in this segment to €2,000 is planned in the draft act for transposition into national law of the Directive amending the Fourth EU Money Laundering Directive.

For the prevention of money laundering in the trade in goods, it is very important for the risk assessment to incorporate knowledge from the DNFBP sector (and in particular from traders in goods) in addition to knowledge from the financial sector. The following anomalies can be noted in this connection as risk factors evidencing concealment techniques relating to trade in goods:

- Traders in goods in Germany receive sometimes large payments from third parties for goods or services ordered by shell companies incorporated in offshore jurisdictions that have no connection with the final place of delivery.

- Discrepancies between the amount invoiced for goods and what would be a reasonable market value, or other discrepancies such as between the invoiced amount and the transaction total shown in transportation and accompanying documents.

- Use of traded goods as a medium of exchange and store of value, such as when cash of unknown origin is invested in high-value goods.

The National Risk Assessment gave rise to indications, especially in the recent past, of members of organised crime groups (mostly from what is referred to as the clan milieu) increasingly dispensing with purchases of high-value goods and instead renting or leasing them on a long-term basis. Most of the goods concerned are motor vehicles or jewellery (such as watches and chains). The public agencies involved in the National Risk Assessment assume that this phenomenon could involve evading mechanisms due to the reform of the law regarding asset recovery (for more on asset recovery, see section 3.1.5.5) and that the conduct could be intended to make asset recovery more difficult overall. This phenomenon will continue to be monitored and it is to be evaluated whether there is a need for legislative action in this regard. Looking ahead, BaFin should consequently pay increased intention in the AML supervision of leasing companies to ensuring that due diligence requirements are met in particular on leasing transactions involving motor vehicles, construction machinery and jewellery.

5.3 Gambling sector

Gambling brings together two elements that make the sector particularly susceptible for the laundering, concealment and structuring of incriminated funds. These are the frequently large transaction amounts that in offline gambling are often paid in cash and the high throughput and transaction speeds with which funds can be turned over and relocated. Online gambling additionally compounds the risks inherent to gambling with the risks specific to Internet-based transactions: A large variety of payment methods are available online (including payment in crypto assets), many of which do not reveal the source of funds and the identity of the payer. There is also the danger of technical manipulation (such as hacking) to intervene in the outcome of games of chance and deliberately circumvent technical security measures. In light of this, the gambling sector is rated with a high money laundering threat. The terrorist financing threat is assumed to be low.

There are many ways in which the gambling sector can be used and misused for money laundering purposes. Both the interpretation and application guidance on the Money Laundering Act issued by the *Länder* supreme gambling supervisory authorities[71] and the FIU typology paper[72] on the gambling sector provide an overview of the main risks for the sector and help with effective application of the risk mitigation requirements laid down in the Money Laundering Act. The fundamental susceptibility of German casinos to being used as a currency exchange service is countered by detailed compliance measures for casino operators (for example in the choice of payment methods for paying out winnings).

The placement of illegal funds as the account balance on the player's own gaming account or that of another player is also seen as a money laundering risk in gambling. Little or no actual gambling is engaged in. After a certain time, the gaming account holder asks for the unused or barely used credit balance to be returned to their bank account. Betting accounts with foreign online providers are considered particularly susceptible to this. The funds transfer verifiably originated by the gambling operator is declared as winnings and taxed as necessary. This exploit can be performed with a single gaming account; frequently, however, multiple accounts are held and used in parallel in order to conceal money laundering activity. In frequent cases, the return transfer is made to

71 Auslegungs- und Anwendungshinweise zum Geldwäschegesetz (GwG) für Veranstalter und Vermittler von Glücksspielen, Gemeinsame Hinweise der Obersten Glücksspielaufsichtsbehörden der Länder, 2019.

72 Typologien der Geldwäsche und Terrorismusfinanzierung, Besondere Anhaltspunkte für die Glücksspielbranche (ML/TF Typologies – Special indications in the gambling industry), FIU, 2018.

the same bank account or else to several bank accounts opened in the same person's name.

Another widespread typology in gambling is for a money launderer to purchase (usually in cash) a legitimate payout claim from another player. The money launderer presents themselves as the 'genuine' winner vis-à-vis the gambling operator and has the sum transferred – declared as winnings on the transfer – to their own account. In this way, incriminated cash is exchanged for a payout claim.

There is also the possibility of money laundering in combination with regular involvement in actual gambling in situations where the risk of loss to the criminal is calculable. That is always the case where the outcome of the game is previously known for reasons such as:

- Technical manipulation of purely computer-controlled games
- Corruption and influencing of sports events
- Deliberately losing in online games where several users play against each other so that another user wins
- Collusion with one or more of the gambling operator's employees.
- Engaging in gambling with a certain control of the gambling risks (such as by simultaneously betting on win/lose in sports betting events or on several different horses in horse races).

As well as by the use of legal gambling outlets, money laundering activities also take the form of investment in the sector itself. Incriminated funds are used to establish or finance a bricks-and-mortar casino or an online gambling platform. In addition, incriminated funds are incorporated into a gambling operation's accounts, either by reporting higher revenues than are actually generated or by the gambling operator's entire business being a simulation with all funds recorded in the accounts originating from other, illegitimate activities.

The interpretation and application guidance contains enforcement guidance for supervisory authorities with regard to online sports betting. Among other things, there will be a graduated system in future between supervision of intermediaries and supervision of operators. Online sports betting can also be prohibited if there are found to be material violations of the Interstate Treaty on Gambling (*Glücksspielstaatsvertrag* – an agreement between the sixteen *Länder*). Online casinos, online poker and secondary lotteries are illegal in Germany (except under prior licence at *Länder* level). Supervisory authorities therefore prohibit such activities by operators and intermediaries in Germany from the outset. However, the means available to administrative enforcement often fail in the face of foreign providers due to the lack of any international agreement. Experience has shown mutual legal assistance requests with relevant EU Member States so far to take a very long time and in many cases to be ineffective because the laws there massively favour illegal gambling activities in Germany.

5.4 Service providers for companies, Treuhand assets and Treuhänder

Service providers for companies, Treuhand assets and Treuhänder (civil-law trusts and civil-law trustees) were added as obliged entities under the Money Laundering Act in the revision of the Act on 21 August 2008. The reason for including Treuhand service providers is because criminals often rely on trust vehicles or interlocking and complex cross-border shareholdings in order to

conceal incriminated funds. These make it possible to conceal business activities and transactions. Using the services of these professions is an alternative to the heavily monitored financial sector. Services for Treuhand assets and Treuhänder are frequently provided in Germany by legal advisory professions. The provision in section 2 (1) no. 13 of the Money Laundering Act is therefore primarily to be construed as a backstop that only applies where a Treuhänder or service provider is not already among the obliged entities under section 2 (1) no. 10 to 12 (see section 5.5). This group of obliged entities also encompasses office service providers and companies that set up or acquire shelf companies (mostly GmbHs and Ltds) to hold and/or sell. The money laundering risk for the group of obliged entities analysed here (obliged entities under section 2 (1) no. 13 of the Money Laundering Act) is rated medium-low. Terrorist financing risk is rated as low.

Office service providers in Germany are frequently found in conurbations and economic centres and are frequently used by startups. They primarily provide office space, meeting rooms and business addresses together with telephone and postal contact options (such as acceptance and forwarding) for a limited period. Office service providers in Germany do not assume functions such as management or holding shares in companies on a fiduciary basis. In addition, they mainly operate on the basis of ongoing customer relationships (limited-term contracts) without anomalous cash transactions. German office service providers cannot therefore be compared with their foreign counterparts.

The competent supervisory authorities face practical problems in terms of identifying the service providers and the group to be monitored because of the provision in the Money Laundering Act being primarily intended as a backstop and of it being directly tied to a specific activity. Despite the low risk, this group of obliged entities should continue to be analysed in order to be able to detect any changes that are liable to increase risk at an early stage. If the risk rating increased, consideration could be given to measures such as a requirement to appoint and provide notice of a money laundering reporting officer.

5.5 Legal and liberal professions

Obliged entities under the Money Laundering Act in the legal and liberal professions sector in Germany comprise auditors, tax advisers, lawyers and notaries. Money laundering risk for lawyers and notaries is rated as high. The money laundering risk for tax advisers and auditors is rated as medium. A notable money laundering risk in this sector is seen in connection with trust and escrow accounts and requires special vigilance (also, and particularly, in connection with payments in cash and payments from abroad/high-risk jurisdictions). Terrorist financing risk is rated as medium-low for the four professions.

These four liberal professions are subject to mandatory membership of the respective professional governing bodies. The professional governing bodies are responsible for representing their members' interests. They monitor compliance with professional requirements and promote professional development. In the case of lawyers and tax advisers, the regional professional governing bodies additionally perform the function of money laundering supervision with regard to AML/CFT. This function is provided in the case of auditors by the Chamber of Public Auditors (Wirtschaftsprüferkammer). For notaries, the supervisory function is performed by the president of the competent regional court.

Regarding notaries, by which civil law notaries are meant, it can be said overall that there is a certain conflict between obligations under the Money Laundering Act and the Federal Notarial

Code (*Bundesnotarordnung*). A notary is an office holder (holder of public office, exercising public functions) who acts in all instances under public law. Notaries perform various activities, including notarial authentication, contract drafting and provision of advice. The high money laundering risk in connection with notaries is to be seen in particular as arising from their role in real estate transactions. Notaries are normally involved in all such transactions. The only exceptions that can arise are in connection with share deals (see section 5.1). Notaries frequently also play an important part in connection with incorporations.

In the course of their work, auditors and tax advisers gain a detailed insight into the structures and finances of business enterprises and can form a clear picture both of sources of income and of the beneficial owners. This makes them the obliged entities best placed to detect anomalies within a company. Particular attention should be paid in future work to the risk of 'fronts' using nominees being deployed, especially in the real estate sector.

Trust and escrow accounts involve heightened money laundering risk, especially in connection with cash deposits. This is a particularly common practice among lawyers.[73] However, it has also been known for such accounts to be used in the case of notaries for cash deposits and payments to and from other countries (including high-risk jurisdictions). Lawyers and notaries need to exercise vigilance here in their capacity as obliged entities. Banks, too, should keep a close watch on such accounts and not rely on due diligence requirements being met by this group of obliged entities. Supervisory authorities in particular should step up their activities in this area and keep a constant watch on the associated risks.

The small number of STRs submitted in the past by members of the liberal professions can partly be explained by the law as it has stood so far. Under section 43 (2) sentence 1 of the Money Laundering Act, obliged entities are exempt from the reporting obligation if the reportable matter relates to information they received in the context of a client relationship subject to professional secrecy. In accordance with the Money Laundering Directive, Member States do not apply the suspicious transaction reporting obligation to legal professionals only where information is obtained in the course of providing legal advice or representing a client in judicial proceedings. The changes planned on transposition into national law of the Directive amending the Fourth EU Money Laundering Directive will restrict the scope of this privilege more closely to legal advice and legal representation activities. In addition, the reporting obligation under section 43 (2) sentence 2 is to continue to apply in the event of an acquisition listed in section 1 of the Real Property Transfer Tax Act (*Grunderwerbsteuergesetz*) where a specific case group, as defined by statutory instrument under subsection (6), in connection with real estate transactions applies and the latter fact follows from information that the obliged entities have obtained or received in the exercise, in relation to the transaction concerned, of the general due diligence requirements under section 10 (1) no. 1 to 4.

According to the findings of this National Risk Assessment (see section 5.1), the real estate sector displays specific money laundering risks. The provision cited takes account of the risks in real estate transactions and the substantial involvement of the legal professions in the sector, particularly in contract drafting, legal advice and notarial authentication. Against the background of the professional secrecy obligations, subsection (6) stipulates matters that are reportable under subsection (1) read in conjunction with subsection (2) sentence 3. Extending application to all acquisitions that come under section 1 of the Real Property Transfer Tax Act will ensure that in future, the suspicious transaction reporting obligation applies not only on the direct transfer of rights in rem,

73 See Dark figure study on the prevalence of money laundering in Germany and the risks of money laundering in individual economic sectors, Kai Bussmann, 2016.

but also in cases where real property is acquired by the sale of shares in a property vehicle.

5.6 Financial undertakings

Financial undertakings are undertakings that are supervised to a certain degree but do not need a license from BaFin for their business model. To date, financial undertakings have been defined as a residual category with reference to section 1 (3) of the Banking Act; however, they are to be distinguished from credit institutions and financial services institutions. The current definition in section 1 (3) of the Banking Act is based on various European legislation (among them the Banking Directive and the Investment Services Directive). That definition under section 1 (3) of the Banking Act does not so far reflect any anti-money laundering considerations, however. In the course of this National Risk Assessment, it was consequently established that a major risk with a view to financial undertakings is that it is not possible to capture the full group of obliged entities. This legal uncertainty with regard to obliged entity status means that the supervisory authorities only have limited experience from their supervisory activities. As financial undertakings do not need a license, there is no practical means of identifying the entire group of obliged entities. Financial undertakings were consequently rated with medium ML/TF risk.

In response, in the course of transposing the amending directive into national law, a definition of the term 'financial undertaking' will be added to the Money Laundering Act that is separate from the definition of financial undertakings in the Banking Act. The definition of financial undertakings in section 1 (3) of the Banking Act has not proved useful for the purposes of money laundering legislation as the banking and securities law stipulations of the Banking Act do not give sufficient account to anti-money laundering considerations.

5.7 Catering

The catering sector is an important cultural and economic factor in Germany. Concerning this sector, it was established in the course of work for the National Risk Assessment that catering and hotel businesses are also frequently used for active money laundering. In view of the value of the services provided by the sector, such businesses have little susceptibility to being unwittingly misused by customers for money laundering on a significant scale. Conversely, there are also cases of direct investment in such businesses by OC (see, for example, the comments on shisha bars in section 3.1.2). It has also been known for targeted investment from the milieu of terrorist organisations to be used to generate long-term cash flows (see section 3.2.2). Addition to the list of obliged entities under the Money Laundering Act would make no sense in this situation, as that would primarily involve the fulfilment of due diligence requirements vis-à-vis customers. External audits (by the revenue administration) and inspections by the Financial Monitoring Unit to Combat Illicit Employment have generated deep insights into the true economic activities of this sector. Use of these insights is to be further expanded in future in order to detect incriminated funds invested when setting up a business (such as to purchase fixtures and fittings) or in the running operation (revenue padding). The findings should also generally be made available to the FIU and subsequently to law enforcement agencies. While the focus of the revenue administration is on equal and lawful taxation, it is questionable whether the existing potential has so far been fully exploited given the numbers of STRs actually generated (about 400 per year).

6 Crypto assets

6 Crypto assets

Recent years have seen crypto assets surge in importance in the public eye and they have attracted considerable attention. Their global market capitalisation peaked at about €700 billion in 2018 before falling again in the last few months. The rapid spread of crypto assets has also increased the related risks. The FATF has consequently sharpened the focus on this sector in recent months. Overall, with regard to the many different crypto assets, no large-scale money laundering activities are discernible yet. For one thing, crypto assets (in the form of cryptocurrencies) fluctuate significantly in value; for another, it is often easier to launder funds with far less effort using other anonymous means of payment (most of all cash). In light of this, the money laundering threat for Germany is currently rated medium-low. Developments should nevertheless be closely monitored, as it cannot be ruled out that money laundering activities may increase.

A key exception in this context relates to existing incriminated crypto assets such as those generated from criminal offences on the dark web or from crypto Trojans. The ensuing digital money laundering activities can be described as all-digital or seamless crypto money laundering. It is also conceivable that offenders might mine their own currency and declare their illegal crypto assets as a product of that mining in order to conceal its illegal origin. Procurement and operation of the relatively expensive mining kit can itself be paid for out of incriminated funds. Also, the placement of large transactions does not stand out in many cases in light of the frequent speculation with crypto assets.

Crypto assets have also been known to be used in connection with online fraud offences (as with fake shops). Fraud offences of this kind involve deceiving the victims into originating transfers to accounts used by the perpetrators. The accounts are held by fronts and the funds are transferred from them to the perpetrators via multiple intermediate stages. Cases have been seen in the recent past where, instead of being transferred to foreign accounts and withdrawn in cash by a front, funds are exchanged for crypto assets and put to further use in that form.

Crypto assets can in principle be used to conceal incriminated funds in various ways. Use is made here of 'mixer' or 'tumbler' services that mix crypto assets of different origins. Considerable analytical effort is then needed to trace where the assets in the mixed amount originate. The concealment aspect is particularly important given the widespread use of crypto assets as a means of payment on the dark web. Corresponding services that can be used for this purpose, such as the 'mixers' just mentioned, operate globally and do not require a physical presence. The money laundering potential also increases further when funds are exchanged between different crypto assets.

Crypto assets can be anonymous or pseudonymous. Pseudonymity permits transaction patterns to be analysed in public blockchains and hence allows the analysis of suspicious movements (examples include Bitcoin and Ethereum). Users operate under the pseudonym of their public key. All transactions can be publicly inspected and their entire history can be traced if needed. It should be borne in mind, however, that the possibility of creating any number of public keys and hence pseudonyms can render it significantly more difficult to trace the transaction history for a specific person or organisation. Particular susceptibility for money laundering, however, is seen in crypto assets which

offer users complete anonymity and transactions in which are untraceable (examples are Monero and Zcash). User anonymity makes it easy to conceal transactions and hence impossible to trace the funds involved. Full anonymity also broadens the scope for misuse for further criminal activities. In light of this, special attention should be paid in future to the development of anonymous crypto assets where both the payer and the payee remain completely anonymous. Although they still have relatively small market capitalisation, anonymous crypto assets are becoming increasing popular on the dark web, where they could become a real alternative to Bitcoin. This notably applies to Monero. One thing that should not be underestimated, however, is the strong innovation drive behind crypto assets, as a result of which pseudonymous crypto assets could possibly develop in the direction of greater anonymity.

The risk of crypto assets being used for terrorist financing is currently rated as low. Depending on various developments, it cannot be ruled out that the risk potential will increase in the years ahead. There is evidence of the use of crypto assets in the fields of right-wing extremism and Islamism, although there is no reliable evidence of such assets being used to finance terrorism on a large scale. This assessment is borne out by the current situation – especially with regard to fund transfers – under which there has so far been no need, except in individual cases, for crypto assets in particular to be used for terrorist financing.

Unlike pseudonymous crypto assets, cash leaves no traces and is easy to handle, which is why it can be assumed, for example, that money transfers relating to terrorist financing continue to take place – as well as via hawala and money transfer services – primarily by the use of cash couriers (see section 3.2.3). Making pseudonymous crypto assets anonymous takes a certain amount of technical input such as the use of anonymising services and 'mixer' or 'tumbler' services or, for example, Darkwallet, a software application that has built-in anonymising features. Using crypto assets also requires a basic technical understanding, especially in connection with the dark web. Moreover, crypto assets continue to be less of a means of payment (or of transfer) than an object of speculation, because they fluctuate significantly in value. This could change with the advent of what are known as stablecoins. These are cryptocurrencies that have a mechanism to keep their value stable. If they become widespread, this could lead to an increase in ML/TF risks.

In connection with the dark web, crypto assets provide a means for individual offenders in particular to acquire firearms because of the frequent lack of any connection to established, physical weapons markets. Aside from donation appeals and lack of intelligence about the volume of donations they actually generate, however, it is assumed that crypto assets are used for terrorist financing in isolated instances only.

Germany already has the effective legal and technical wherewithal to secure and dispose of incriminated crypto assets. State agencies have gained most practical experience in this regard so far with Bitcoin due to the dominance of this cryptocurrency as a means of payment on the dark web. Given the increasingly widespread use of Monero on the dark web, this cryptocurrency is also expected to gain practical significance with regard to securing and disposal.

The G20 states have consequently agreed to regulate crypto assets for the purpose of AML/CFT. The Directive amending the Fourth EU Money Laundering Directive also accommodates this aim. It thus extends the substantive scope of the Fourth EU Money Laundering Directive to providers of exchange services between virtual currencies and fiat currencies and to custodian wallet providers. This is to enable competent authorities for AML/

CFT to monitor the use of crypto assets via obliged entities. The amending directive defines crypto assets ("virtual currencies") as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically".

In the course of 2019, the Money Laundering Act will be revised with regard to crypto assets in line with the requirements of the Directive amending the Fourth EU Money Laundering Directive. Custodian wallet providers, which provide services to safeguard cryptocurrencies (such as Bitcoin) or cryptographic keys, are to be added to the list of obliged entities under the Money Laundering Act. The process of exchanging crypto assets into legal tender plays a major part in AML because conversion into non-cash, legal means of payment removes the anonymity or pseudonymity of incriminated funds. In this context, from administrative practice at BaFin, the exchange platforms that are also covered by the amending directive and that exchange between fiat currencies and cryptocurrencies already need a license for the bulk of crypto assets and therefore constitute financial services institution that are obliged entities under the Money Laundering Act. The supplementary provisions thus provide statutory backing for this administrative practice, which also covers exchange between one cryptocurrency and another.

List of tables

List of figures

List of annexes

Annex 1: Private sector/financial sector participants

Working Group B: Money Laundering in the Financial Sector: Participants		
1	**Banks**	
		Bausparkasse Schwäbisch Hall AG
		Bayerische Landesbank
		Berliner Volksbank eG
		BNP Paribas S.A. Niederlassung Deutschland
		Bürgschaftsbank Baden-Württemberg GmbH
		Commerzbank AG
		DB Privat- und Firmenkundenbank AG
		DekaBank Deutsche Girozentrale
		Deutsche Bank AG
		Deutsche Börse AG/Clearstream Banking AG
		Deutsche Kreditbank AG
		Deutsche Pfandbriefbank AG
		DZ Bank AG
		GenoTec GmbH
		Hamburger Sparkasse AG
		ING-DiBa AG
		Investitionsbank Berlin
		Joh. Berenberg, Gossler & Co. KG
		Landesbank Hessen-Thüringen Girozentrale
		PSD Bank Berlin-Brandenburg eG
		Raiffeisenbank Kraichgau eG
		Santander Consumer Bank AG
		solarisBank AG
		Sparda-Bank West eG
		Sparkasse Oder-Spree
		Sparkasse Pforzheim Calw
		Targobank AG
		UBS Europe SE
		UniCredit Bank AG
		Wüstenrot Bank AG Pfandbriefbank
		Wüstenrot Bausparkasse AG

2	**Insurers**	
		AachenMünchener Lebensversicherung AG
		Allianz Lebensversicherung AG
		AXA Lebensversicherung AG
		Cosmos Lebensversicherungs-AG
		Debeka Lebensversicherungsverein a. G.
		ERGO Lebensversicherung AG
		Generali Versicherung AG
		HDI Lebensversicherung AG
		IDEAL Lebensversicherung a. G.
		Provinzial Rheinland Lebensversicherung AG
		R+V LEBENSVERSICHERUNG AG
3	**Asset management companies**	
		Allianz Global Investors GmbH
		BNY Mellon Service Kapitalanlage-Gesellschaft mbH
		capiton AG
		Deka Investment GmbH
		HANSAINVEST Hanseatische Investment-GmbH
		Helaba Invest Kapitalanlagegesellschaft mbH
		LaSalle Investment Management Kapitalverwaltungsgesellschaft mbH
		Schroder Real Estate Kapitalverwaltungsgesellschaft mbH
		Siemens Fonds Invest GmbH
4	**Money or value transfer services**	
		Euronet Payment Services Ltd. (trading name: RIA)
		mobilcom-debitel Shop GmbH as agent for Euronet Payment Services Limited
		MoneyGram International Ltd.
		DB Privat- und Firmenkundenbank AG as agent of Western Union
		ReiseBank AG as agent for Western Union
		Western Union Payment Services Ireland Ltd. (WUPSIL)
		Ziraat Bank International AG

5	**Industry associations**	
		Bitkom – Digitalverband (Federal Association for Information Technology, Telecommunications and New Media)
		BVI – Deutscher Fondsverband (German Investment Funds Association)
		BVZI – Bundesverband der Zahlungsinstitute (Federal Association of Payment and E-Money-Institutions)
		DK – Deutsche Kreditwirtschaft (German Banking Industry Committee)
		EMA – E-Geld Verband (Electronic Money Association)
		GDV – Gesamtverband der Deutschen Versicherungswirtschaft (German Insurance Association)
		VAB – Verband der Auslandsbanken (Association of Foreign Banks in Germany)
6	**Auditors and industry association audit bodies**	
		BDO AG Wirtschaftsprüfungsgesellschaft
		Deloitte GmbH Wirtschaftsprüfungsgesellschaft
		Ernst & Young GmbH
		Wirtschaftsprüfungsgesellschaft
		KPMG Wirtschaftsprüfungsgesellschaft AG
		Mazars GmbH & Co. KG
		Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft
		PricewaterhouseCoopers GmbH
		Wirtschaftsprüfungsgesellschaft
		Audit office of Genossenschaftsverband Bayern e.V. (GVB)
		Audit office of Rheinischer Sparkassen- und Giroverband (RSGV)

Source: BaFin

Annex 2: Private sector/DNFBP sector participants

Working Group C: Money Laundering in the DNFBP Sector: Participants		
1.	**Financial services companies**	
		Financial Planning Standards Board Deutschland
		AfW – Bundesverband Finanzdienstleistung (Federal Financial Services Association)
2.	**Insurance brokers**	
		Bundesverband Deutscher Versicherungskaufleute (Association of German Insurance Agents)
3.	**Legal professions/legal advisers**	
		Bundesnotarkammer (Federal Chamber of Civil Law Notaries)
4.	**Tax advisers and auditors**	
		Bundessteuerberaterkammer (Federal Chamber of Tax Advisers)
		Institut der Wirtschaftsprüfer – IDW (Institute of Public Auditors in Germany)
		Wirtschaftsprüferkammer (Chamber of Public Auditors)
		Deutscher Steuerberaterverband (German Association of Tax Advisers)
5.	**Estate agents/developers**	
		Immobilienverband Deutschland – IVD (Real Estate Association)
6.	**Traders in goods**	
		Deutscher Industrie- und Handelskammertag (Association of German Chambers of Commerce and Industry)
		Verband der Automobilindustrie (German Association of the Automotive Industry)
		Zentralverband Deutsches Kraftfahrzeuggewerbe – ZDK (Central Association of the German Motor Vehicle Industry)
		Bundesverband der Edelstein- und Diamantindustrie (Federal Association of the Precious Stones and Diamond Industry)
		Fachvereinigung Edelmetalle (Precious Metals Association)
		Handelsverband Deutschland – HDE (German Retail Federation)
		Zentralverband für Uhren, Schmuck und Zeitmesstechnik (Central Association for Watches, Jewellery and Chronometry)
7.	**Antiques sector**	
		Kunsthändlerverband Deutschland (German Art Dealers Association)
		Bundesverband Deutscher Galerien und Kunsthändler (Association of German Galleries and Fine Art Dealers)
		Bundesverband deutscher Kunstversteigerer (Association of German Art Auctioneers)
		Verband deutscher Antiquare (Association of German Antiquarian Booksellers)

8.	**Gambling**	
		Deutscher Spielbankenverband (German Casino Association)
		Deutscher Sportwettenverband (German Sports Betting Association)
		Deutscher Lotto- und Totoblock (German Lotto and Toto Block)
9.	**Service providers**	
		Kerberos Compliance-Management Systeme GmbH
		Bundesverband Deutscher Unternehmensberater – BDU (Federal Association of German Management Consultants)
		Bundesverband Deutscher Inkasso-Unternehmen (Federal Association of German Debt Collection Companies)
		Bundesverband für Inkasso und Forderungsmanagement (Federal Association for Debt Collection and Receivables Management)
10.	**Expert consultations – gambling sector:**	
		Deutscher Online Casino Verband (German Online Casino Association)
		Deutscher Sportwettenverband (German Sports Betting Association)
		Bund-Länder-Arbeitsgruppe Glücksspiel (Federal/*Länder* Working Group on Gambling)
11.	**Expert consultations – NGOs:**	
		VENRO
		DZI – Deutsches Zentralinstitut für soziale Fragen (German Central Institute for Social Issues)
		Brot für die Welt (Bread for the World)
		ADRA Germany
		Maecenata Foundation
		Bundesverband Deutscher Stiftungen (Association of German Foundations)

Annex 3: Private-sector consultation

Financial sector: timeline

Period	Work stage
To August 2018	Compilation of questionnaires and selection of participating undertakings
Mid-August 2018	Letters sent to management and questionnaires emailed to money laundering reporting officers of participating undertakings
Mid-September 2018	Deadline for return of questionnaires
To mid-October 2018	Evaluation of questionnaires by Financial Sector working group leaders and preparation of expert consultations
Mid-November 2018	Eight expert consultations at BMF with representatives of the private sector (banks, insurance undertakings, asset management companies, MVTS undertakings, industry associations and audit firms)
Early December 2018	Final evaluations by Financial Sector working group with the aid of the findings from the questionnaires and expert consultations

DNFBP sector: timeline

Period	Work stage
To October 2018	Compilation of questionnaire and selection of participating industry associations
Early October 2018	Expert consultation with NGO representatives
Late October 2018	Questionnaire sent to participating DNFBP sector industry associations
Late November 2018	Further expert consultation with NGO representatives
Mid-December 2018	Deadline for return of questionnaires from DNFBP sector and evaluation of questionnaires by DNFBP Sector working group leaders
Mid-December 2018	Expert consultation with gambling sector representatives
Mid-December 2018	Final evaluation and consistency checking by DNFBP Sector working group

Annex 4: Cross-border threats

Country	ML threat					Direction of threat				TREND		
	high	medium/high	medium	medium/low	low	inbound	outbound	both directions	unclear	no change	increasing	decreasing
										→	↑	↓
USA				x				x		x		
France			x			x				x		
United Kingdom		x						x			x	
Netherlands			x					x		x		
China	x							x		x		
Italy		x						x		x		
Austria				x				x				x
Poland			x					x		x		
Switzerland		x						x				x
Belgium				x				x		x		
Czech Republic			x			x					x	
Hungary			x			x		x			x	
Turkey	x							x		x		
Russia	x							x		x		
Luxembourg			x					x		x		
Denmark			x					x		x		
Caribbean islands (Cayman Islands, British Virgin Islands, Bermuda)	x							x		x		
Channel Islands (Guernsey, Jersey), Isle of Man	x							x		x		
Lebanon		x						x		x		
Panama		x						x		x		
Liechtenstein			x				x					x
Cyprus	x							x		x		
Malta	x							x		x		
Singapore			x					x		x		
Lithuania			x				x			x		
Estonia				x				x		x		
Latvia		x				x				x		
Vanuatu					x			x		x		

Source: Working Group A

Annex 5: Amendments to the Act on the Detection of Proceeds from Serious Crimes (Money Laundering Act) (*Geldwäschegesetz – GWG*)

	Entry into force	Promulgation	Amending act	EU directive/amendments	Signed into law	Source
1	30 November 1993	29 October 1993	Act on the detection of proceeds from serious crimes (Money Laundering Act)	Transposition into national law of the First Money Laundering Directive (Directive 91/308/EEC) of 10 June 1991	25 October 1993	BGBl. I 1993, p. 1770
2	15 August 2002	14 August 2002	Article 1 of the Act on the Improvement of Anti-Money Laundering and of Countering the Financing of Terrorism (*Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und Steuerhinterziehung*)	Transposition into national law of the requirements of the Second Money Laundering Directive (Directive 2001/97/EC) of 4 December 2001	8 August 2002	BGBl. I 2002, p. 3105
3	21 August 2008	20 August 2008	Article 2 of the Act Supplementing Anti-Money Laundering and Countering the Financing of Terrorism (*Geldwäschebekämpfungsergänzungsgesetz – GwBekErgG*)	Transposition into national law of the Third EU Money Laundering Directive (Directive 2005/60/EC) of 26 October 2005	13 August 2008	BGBl. I 2008, p. 1690
4	4 August 2009	3 August 2009	Article 4 of the Act on Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)	Section 1 (revision of the definition of terrorist financing)	30 July 2009	BGBl. I 2009, p. 2437
5	31 October 2009	29 June 2009	Article 5 of the Act Implementing the Second Payment Services Directive (*Zahlungsdiensteumsetzungsgesetz*)	Section 2, section 9, section 12, section 16	25 June 2009	BGBl. I 2009, p. 1506
6	1 November 2010	24 June 2009	Article 5 of the Act on Identity Cards and Electronic Identification and for the Amendment of Further Provisions (*Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften*)	Section 6, section 8	18 June 2009	BGBl. I 2009, p. 1346
7	9 March 2011	8 March 2011	Article 7 of the Second Electronic Money Directive Transposition Act (*Gesetz zur Umsetzung der Zweiten E-Geld-Richtlinie*)	Section 9 Section 1, section 2, section 16	1 March 2011	BGBl. I 2011, p. 288
8	1 July 2011	25 June 2011	Article 5 of the UCITS IV Transposition Act (*OGAW-IV-Umsetzungsgesetz*)	Section 2, section 16	22 June 2011	BGBl. I 2011, p. 1126
9	29 December 2011	28 December 2011	Article 1 of the Act for the Improvement of Anti-Money Laundering (*Gesetz zur Optimierung der Geldwäscheprävention*)	Section 1, section 2, section 3, section 4, section 5, section 6, section 7, section 9, section 10, section 11, section 12, section 13, section 14, section 16, section 16a, section 17	22 December 2011	BGBl. I 2011, p. 2959

	Entry into force	Promulgation	Amending act	EU directive/amendments	Signed into law	Source
10	1 January 2012	8 December 2011	Article 9 of the Act for the Transposition of Directive 2010/78/EU of 24 November 2010 Regarding the Establishment of the European System of Financial Supervision	Section 16a	4 December 2011	BGBl. I 2011, p. 2427
11	29 December 2011	28 December 2011	Article 1 of the Act for the Improvement of Anti-Money Laundering (*Gesetz zur Optimierung der Geldwäscheprävention*)	Section 3, section 6, section 9	22 December 2011	BGBl. I 2011, p. 2959
12	26 February 2013	25 February 2013	Article 1 of the Act Supplementing the Money Laundering Act (*Gesetz zur Ergänzung des Geldwäschegesetz*)	Section 1, section 2, section 3, section 4, section 6, section 9, section 9a, section 9b, section 9c, section 9d, section 11, section 13, section 16, section 16a, section 17	18 February 2013	BGBl. I 2013, p. 268
13	4 July 2013	3 July 2013	Article 4 of the Act for Transposition of Directive 2011/89/EU of the European Parliament and of the Council of 16 November 2011 amending Directives 98/78/EC, 2002/87/EC, 2006/48/EC and 2009/138/EC as regards the supplementary supervision of financial entities in a financial conglomerate (*Gesetz zur Umsetzung der Richtlinie 2011/89/EU*)	Section 12	27 June 2013	BGBl. I 2013, p. 1862
14	13 July 2013	12 July 2013	Article 2 of the Act Amending the Act on the Kreditanstalt für Wiederaufbau and Other Acts (*Gesetz zur Änderung des Gesetzes über die Kreditanstalt für Wiederaufbau und weiterer Gesetze*)	Section 16	4 July 2013	BGBl. I 2013, p. 2178
15	24 December 2013	23 December 2013	Article 9 of the Act Aligning the Investment Tax Act and Other Acts to the AIFM Transposition Act (*AIFM-Steuer-Anpassungsgesetz*)	Section 2, section 5, section 16	18 December 2013	BGBl. I 2013, p. 4318
16	1 January 2014	3 September 2013	Article 6 of the CRD IV Transposition Act (*CRD IV-Umsetzungsgesetz*)	Section 3, section 5, section 7, section 12, section 16	28 August 2013	BGBl. I 2013, p. 3395
17	19 July 2014	18 July 2014	Article 8 of the Act Adjusting Financial Market Legislation (*Gesetz zur Anpassung von Gesetzen auf dem Gebiet des Finanzmarktes*)	Section 3,section 5, section 12, section 16	15 July 2014	BGBl. I 2014, p. 934
18	20 June 2015	19 June 2015	Article 2 of the Act Modifying the Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)	Section 1	12 June 2015	BGBl. I 2015, p. 926

	Entry into force	Promulgation	Amending act	EU directive/amendments	Signed into law	Source
19	1 January 2016	10 April 2015	Article 2 of the Act to Modernise Financial Supervision of Insurance Undertakings (*Gesetz zur Modernisierung der Finanzaufsicht über Versicherungen*)	Section 2, section 5, section 12	1 April 2015	BGBl. I 2015, p. 434
20	8 September 2015	7 September 2015	Article 346 of the Tenth Competence Reassignment Ordinance (*Zehnte Zuständigkeitsanpassungsverordnung*)	Section 1, section 5, section 6, section 7, section 11, section 12	31 August 2015	BGBl. I 2015; p. 1474
21	18 August 2016	18 June 2016	Article 7 of the Act Transposing the Directive on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (*Gesetz zur Umsetzung der Richtlinie über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten sowie den Zugang zu Zahlungskonten mit grundlegenden Funktionen*)	Section 3, section 4	11 April 2016	BGBl. I 2016, p. 720
22	26 June 2017 (Recast)	24 June 2017	Article 1 of the Act on the Implementation of the Fourth EU Anti-Money Laundering Directive, the EU Funds Transfer Regulation and on the Reorganisation of the Financial Intelligence Unit (*Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen*)	Transposition into national law of the Fourth EU Money Laundering Directive (2015/849/EU) of 20 May 2015	23 June 2017	BGBl. I 2017, p. 1822
23	14 July 2017	13 July 2017	Act on the Exercise of Options under the EU Prospectus Regulation and the Amendment of Further Financial Markets Legislation (*Gesetz zur Ausübung von Optionen der EU-Prospektverordnung und zur Anpassung weiterer Finanzmarktgesetze*)	Amendments to section 2, section 3, section 20 and section 22 of the Money Laundering Act	10 July 2017	BGBl. I 2017, p. 1102

Source: Federal Ministry of Finance

Annex 6: Amendments to the Criminal Code (*Strafgesetzbuch*) (excerpts: sections 89a, 89b, 89c, 129a, 129b and 261 of the Criminal Code)

I. Section 89a of the Criminal Code: Preparation of a serious violent offence endangering the state

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
1	4 August 2009	3 August 2009	Article 1 of the Act on Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)	New	30 July 2009	BGBl. I 2009, p. 2437
2	20 June 2015	19 June 2015	Article 1 of the Act Modifying the Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)	New: Subsection (2a)	12 June 2015	BGBl. I 2015, p. 926
3	1 July 2017	21 April 2017	Article 1 of the Act Reforming Asset Recovery under Criminal Law (*Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung*)	Deletion of "Section 73d shall be applied"	13 April 2017	BGBl I 2017, p. 872

II. Section 89b of the Criminal Code: Establishing contacts for the purpose of committing a serious violent offence endangering the state

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
1	4 August 2009	3 August 2009	Article 1 of the Act on Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)	New	30 July 2009	BGBl. I 2009, p. 2437

III. Section 89c of the Criminal Code: Terrorist financing

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
1	20 June 2015	19 June 2015	Article 1 of the Act Modifying the Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)	New	12 June 2015	BGBl. I 2015, p. 926

IV. Section 129a of the Criminal Code: Forming terrorist organisations

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
1	20 September 1976	20 August 1976	Article 1 of the Act Amending the Criminal Code, the Code of Criminal Procedure, the Courts Constitution Act, the Federal Lawyers' Act and the Prison Act (*Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung, des Gerichtsverfassungsgesetzes, der Bundesrechtsanwaltsordnung und des Strafvollzugsgesetzes*)	New	18 August 1976	BGBl. I 1976, p. 2181
2	1 July 1980	3 April 1980	Article 1 of the Eighteenth Criminal Law Amendment Act: Act to Combat Environmental Crime (*Achtzehntes Strafrechtsänderungsgesetz – Gesetz zur Bekämpfung der Umweltkriminalität*)		28 March 1980	BGBl. I 1980, p. 373
3	1 May 1986	17 April 1986	Article 1 of the Twenty-third Criminal Law Amendment Act: Suspended Sentences of Imprisonment (*Dreiundzwanzigstes Strafrechtsänderungsgesetz – Strafaussetzung zur Bewährung*)		13 April 1986	BGBl. I 1986, p. 393
4	1 January 1987	30 December 1986	Article 1 of the Prevention of Terrorism Act (*Gesetz zur Bekämpfung des Terrorismus*)		19 December 1986	BGBl. I 1986, p. 2566
5	1 April 1998	30 January 1998	Article 1 of the Sixth Criminal Law Reform Act (*Sechstes Gesetz zur Reform des Strafrechts*)		26 January 1998	BGBl. I 1998, p. 164
6	1 January 1999	19 November 1998	Notice of the Revised Criminal Code (*Bekanntmachung der Neufassung des Strafgesetzbuchs*)		13 November 1998	BGBl. I 1998, p. 3322
7	30 June 2002	29 June 2002	Article 2 of the Act to Introduce the Code of Crimes against International Law (*Gesetz zur Einführung des Völkerstrafgesetzbuches*)		26 June 2002	BGBl. I 2002, p. 2254
8	30 August 2002	29 August 2002	Article 1 of the 34th Criminal Law Amendment Act (*34. Strafrechtsänderungsgesetz*)		22 August 2002	BGBl. I 2002, p. 3390
9	28 December 2003	27 December 2003	Article 1 of the Act Transposing the Council Framework Decision of 13 June 2002 on Combating Terrorism and Amending Other Acts (*Gesetz zur Umsetzung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze*)		22 December 2003	BGBl. I 2003, p. 2836

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
10	30 July 2016	29 July 2016	Article 8 of the Act to Improve Information Exchange in the Fight Against International Terrorism (*Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus*)		26 July 2016	BGBl. I 2016, p. 1818
11	22 July 2017	21 July 2017	Article 1 of the Fifty-fourth Act Amending the Criminal Code – Transposition of Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime (*Vierundfünfzigstes Gesetz zur Änderung des Strafgesetzbuches – Umsetzung des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität*)		17 July 2017	BGBl. I 2017, p. 2440
12	22 December 2018	21 December 2018	Article 14 of the Act Implementing the Act Introducing the Right to Marriage for Same-Sex Individuals (*Gesetz zur Umsetzung des Gesetzes zur Einführung des Rechts auf Eheschließung für Personen gleichen Geschlechts*)		18 December 2018	BGBl. I 2018, p. 2639

V. Section 129b of the Criminal Code: Criminal and terrorist organisations abroad; confiscation

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
1	30 August 2002	29 August 2002	Article 1 of the 34th Criminal Law Amendment Act (*34. Strafrechtsänderungsgesetz*)	New	22 August 2002	BGBl. I 2002, p. 3390
2	28 December 2003	27 December 2003	Article 1 of the Act Transposing the Council Framework Decision of 13 June 2002 on Combating Terrorism and Amending Other Acts (*Gesetz zur Umsetzung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze*)		22 December 2003	BGBl. I 2003, p. 2836
3	8 September 2015	7 September 2015	Article 220 of the Tenth Competence Reassignment Ordinance (*Zehnte Zuständigkeitsanpassungsverordnung*)	Federal Ministry of Justice (BMJ) amended to Federal Ministry of Justice and Consumer Protection (BMJV)	31 August 2015	BGBl. I 2015, p. 1474
4	1 July 2017	21 April 2017	Article 1 of the Act Reforming Asset Recovery under Criminal Law (*Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung*)		13 April 2017	BGBl. I 2017, p. 872

VI. Section 261 of the Criminal Code: Money laundering; hiding unlawfully obtained financial benefits

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
1	22 September 1992	22 July 1992	Article 1 of the Act to Combat Illicit Traffic in Narcotic Drugs and Other Forms of Organised Criminality (*Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität*)	New	15 July 1992	BGBl. I 1992, p. 1302
2	9 May 1998	8 May 1998	Article 1 of the Act on Improving the Fight against Organised Crime (*Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität*)		4 May 1998	BGBl. I 1998, p. 845
3	28 December 2001	27 December 2001	Article 4 of the Act on the Combat of Value Added Tax Evasion and for the Amendment of Other Tax Acts (*Steuerverkürzungsbekämpfungsgesetz*)		19 December 2001	BGBl. I 2001, p. 3922
4	30 August 2002	29 August 2002	Article 1 of the 34th Criminal Law Amendment Act (*34. Strafrechtsänderungsgesetz*)		22 August 2002	BGBl. I 62002, p. 37390
5	28 December 2003	27 December 2003	Article 1 of the Act Transposing the Council Framework Decision of 13 June 2002 on Combating Terrorism and Amending Other Acts (*Gesetz zur Umsetzung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze*)		22 December 2003	BGBl. I 2003, p. 2836
6	28 December 2003	27 December 2003	Article 1 of the Thirty-fifth Criminal Law Amendment Act Transposing the Council Framework Decision 28 May 2001 Combating Fraud and Counterfeiting of Non-cash Means of Payment (*Fünfunddreißigstes Strafrechtsänderungsgesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union vom 28. Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln*)		22 December 2003	BGBl. I 2003, p. 2838
7	1 August 2004	26 July 2004	Article 6 of the Act Implementing the Reform of the Common Agricultural Policy (*Gesetz zur Umsetzung der Reform der Gemeinsamen Agrarpolitik*)		21 July 2004	BGBl. I 2004, p. 1763
8	1 January 2005	5 August 2004	Article 11 of the Act to Control and Limit Immigration and to Regulate the Residence and Integration of Union Citizens and Foreigners (*Zuwanderungsgesetz*)		30 July 2004	BGBl. I 2003, p. 1950

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
9	19 February 2005	18 February 2005	Article 1 of the Thirty-seventh Criminal Law Amendment Act – Sections 180b and 181 of the Criminal Code (*Siebenunddreißigstes Strafrechtsänderungsgesetz – §§ 180 b, 181 StGB*)		11 February 2005	BGBl. I 2005, p. 239
10	1 January 2008	31 December 2007	Article 4 on the Act on the Reform of Telecommunications Surveillance and Other Measures of Undercover Investigation and for Transposition of Directive 2006/24/EC (*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*)		21 December 2007	BGBl. I 2007, p. 3198
11	19 March 2008	18 March 2008	Article 3 of the Act on the Reform of Precursors Control Law (*Gesetz zur Neuregelung des Grundstoffüberwachungsrechts*)		11 March 2008	BGBl. I 2008, p. 306
12	21 August 2008	20 August 2008	Article 1 of the Act Supplementing Anti-Money Laundering and Countering the Financing of Terrorism (*Geldwäschebekämpfungsergänzungsgesetz*)	Transposition into national law of the Third EU Money Laundering Directive (Directive 2005/60/EC) of 26 October 2005	13 August 2008	BGBl. I 2008, p. 1690
13	4 August 2009	3 August 2009	Article 1 of the Act on Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)		30 July 2009	BGBl. I 2009, p. 2437
14	1 September 2009	31 July 2009	Article 1 of the Forty-third Act Amending the Criminal Code – Sentencing in the case of contribution to discovery and to prevention (*Dreiundvierzigstes Gesetz zur Änderung des Strafgesetzbuchs – Strafzumessung bei Aufklärungs- und Präventionshilfe*)		29 July 2009	BGBl. I 2009, p. 2288
15	3 May 2011	2 May 2011	Article 1 of the Act on the Improvement of Anti-Money Laundering and of Countering Tax Evasion (*Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und Steuerhinterziehung*)		28 April 2011	BGBl. I 2011, p. 676
16	1 January 2014	16 October 2013	Article 5 of the Act on the Modernisation of the Utility Model Act and Amendment of the Provisions on Notices of Exhibition Protection		10 October 2013	BGBl. I 2013, p. 3799
17	1 September 2014	29 April 2014	Article 1 of the Forty-eight Criminal Law Amendment Act – Extension of the Offence of Bribery of Members of Parliament (*Achtundvierzigstes Strafrechtsänderungsgesetz – Erweiterung des Straftatbestands der Abgeordnetenbestechung*)		23 April 2014	BGBl. I 2014, p. 410

	Entry into force	Promulgation	Amending act	Amendments	Signed into law	Source
18	20 June 2015	19 June 2015	Article 1 of the Act Modifying the Prosecution of the Preparation of Serious Violent Offences Endangering the State (*Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten*)		12 June 2015	BGBl. I 2015, p. 926
19	24 October 2015	23 October 2015	Article 14 of the Act to Expedite Asylum Procedures (*Asylverfahrensbeschleunigungsgesetz*)		20 October 2015	BGBl. I 2015, p. 1722
20	26 November 2015	25 November 2015	Article 1 of the Prevention of Corruption Act (*Gesetz zur Bekämpfung der Korruption*)		20 November 2015	BGBl I 2015; p. 2025
21	2 July 2016	1 July 2016	Article 16 of the First Act Revising Financial Market Provisions on the Basis of European Legislation (*Erstes Gesetz zur Novellierung von Finanzmarktvorschriften auf Grund europäischer Rechtsakte*)		30 June 2016	BGBl. I 2016, p. 2226
22	15 October 2016	14 October 2016	Article 1 of the Act Enhancing the Fight Against Human Trafficking and Amending the Federal Central Register Act and Book VIII of the Social Code (*Gesetz zur Verbesserung der Bekämpfung des Menschenhandels und zur Änderung des Bundeszentralregistergesetzes sowie des Achten Buches Sozialgesetzbuch*)		11 October 2016	BGBl. I 2016, p. 2226
23	19 April 2017	18 April 2017	Article 1 of the Fifty-first Act Amending the Criminal Code – Criminal Liability for Sports Betting Fraud and Manipulation of Professional Sports Championships (*Einundfünfzigstes Gesetz zur Änderung des Strafgesetzbuches – Strafbarkeit von Sportwettbetrug und der Manipulation von berufssportlichen Wettbewerben*)		11 April 2017	BGBl. I 2017, p. 815
24	1 July 2017	21 April 2017	Article 1 of the Act Reforming Asset Recovery under Criminal Law (*Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung*)		13 April 2017	BGBl. I 2017, p. 872
25	3 January 2018	24 June 2017	Article 2 of the Second Act Revising Financial Market Provisions on the Basis of European Legislation (*Zweites Gesetz zur Novellierung von Finanzmarktvorschriften auf Grund europäischer Rechtsakte*)		23 June 2017	BGBl. I 2017, p. 1693

Source: Federal Ministry of Finance

Published by
Federal Ministry of Finance
L C 3 (Department of Public Relations)
Wilhelmstrasse 97
10117 Berlin
Germany
www.federal-ministry-of-finance.de

October 2019

national-risk-assessment.de