



Bundeskriminalamt

**ANNUAL REPORT 2006**  
**Financial Intelligence Unit (FIU)**  
**GERMANY**

# 2006 Annual Report

## FIU GERMANY

### **Imprint**

Published by:  
BUNDESKRIMINALAMT  
FIU Germany  
65173 Wiesbaden

## Contents

1	Foreword	7
2	Reporting behaviour of parties required to report	8
2.1	Nationwide case statistics for 2006	8
2.2	Results of processing	23
2.3	Summary and evaluation	24
3	Monitoring of suspicious transaction reports	26
3.1	Introduction	26
3.2	Noteworthy cases	28
3.3	Trends	30
3.4	Typologies	35
3.5	Assessment	36
4	Follow-up responses by public prosecutors' offices pursuant to Sect. 11 (9) of the Money Laundering Act	37
4.1	Introduction	37
4.2	Statistical analysis	37
4.3	Analysis of contents	40
4.4	Use of the form "Reporting pursuant to section 11 (9) of the Money Laundering Act, Sections 482 and 475 of the Code of Criminal Procedure"	44
4.5	Summary and Outlook	45
5	Financing of terrorism	46
5.1	General remarks	46
5.2	The national situation	46
5.3	The international situation	51
5.4	Summary and outlook	53
6	National co-operation	54
6.1	The FIU as central office	54
6.2	National investigative authorities	55
6.3	Parties required to report pursuant to the Money Laundering Act	57
6.4	Reports made pursuant to Section 31b of the Fiscal Code	61
6.5	Case collection	61
6.6	FIU's Internet Site	62
6.7	The "electronic suspicious transaction report (eVA)" project	64
6.8	Status of implementation of the "Third EU Money Laundering Directive"	66

## Contents

7	International co-operation	68
7.1	Exchange of intelligence with other FIUs	68
7.2	Noteworthy cases identified on the basis of the international FIU intelligence exchange	69
7.3	The Egmont Group	71
7.4	Memorandum of Understanding (MoU)	71
7.5	FATF	72
8	Summary and Outlook	73
9	Appendices	74

## List of tables

Table 1:	“Reports filed pursuant to the Money Laundering Act” by reporting party	10
Table 2:	“Other reports indicating money laundering activity” by reporting party	12
Table 3:	Suspicious transaction reports pursuant to the Money Laundering Act by state	13
Table 4:	Reports of possible criminal offences from the perspective of the reporting parties (TOP 10)	14
Table 5:	Suspicious transaction reports on transfers of assets to foreign countries(TOP 10)	15
Table 6:	Suspicious transaction reports on transfers of assets from foreign countries (TOP 10)	15
Table 7:	Nationality (TOP 10)	16
Table 8:	Country of residence (TOP 10)	17
Table 9:	Suspects by occupation (TOP 10)	17
Table 10:	Corporate headquarters (TOP 10)	18
Table 11:	Business sectors (TOP 10)	18
Table 12:	Type of account	19
Table 13:	Grounds for suspicion indicated by the parties required to report	20
Table 14:	Connections to types of crime identified by Clearing Offices in cases forwarded to other investigative agencies (TOP 10)	24
Table 15:	Reports filed in connection with “phishing” / “financial agents” (quarterly figures 2006)	34
Table 16:	Follow-up responses pursuant to Section 11 (9) of the Money Laundering Act (2003-2006)	37
Table 17:	Follow-up responses pursuant to Sect. 11 (9) of the Money Laundering Act – annual comparison	39
Table 18:	Comparison between “number of suspicious transaction reports – number of follow-up responses“	40
Table 19:	Dismissal rates by state	41
Table 20:	Types of crime mentioned in follow-up responses pursuant to Sect. 11 (9) of the Money Laundering Act	43
Table 21:	Statistical distribution of suspicious transaction reports relating to the “Financing of Terrorism“	47
Table 22:	Exchange of intelligence with foreign FIUs (TOP 20)	68
Graph 1:	Suspicious transaction reports filed pursuant to the Money Laundering Act, 1995 – 2006	9
Graph 2:	Reports of possible criminal offences from the perspective of the reporting parties	14
Graph 3:	Results of processing by Money Laundering Clearing Offices of the state criminal police offices (LKÄ)	23
Graph 4:	Overall distribution of follow-up responses by German state	38
Graph 5:	Suspicious transaction reports indicating suspected involvement in the financing of terrorism	46



## 1 Foreword

The world's financial centres are subject to a variety of influencing factors which, inter alia, lead to increasingly shorter life cycles of modern financial products. This trend is supported and being facilitated by the high potential of innovation in the field of information and communications technology.

Against this background, the comprehensive and effective fulfilment of duties by all agencies involved in the suppression and prevention of money laundering and the financing of terrorism poses a real challenge.

The Central Office for Suspicious Transaction Reports (FIU) at the BKA has again made considerable efforts to fulfil its tasks assigned pursuant to Section 5 of the Money Laundering Act (MLA) in the best possible manner. This objective has been achieved – not least in view of the positive feedback received from the various parties.

A central measure within the context of optimising various structures and processes in the FIU was the formation of specialised working areas on January 1<sup>st</sup> 2006. During the year under review, the "strategic part of the FIU" succeeded in implementing various measures focused on "intensification of co-operation with the parties required to report and the addressees of the Money Laundering Act". They especially include publications (indicator papers, newsletters, expansion of the Internet site), lectures and presentations in Germany and abroad, strategic analyses and the forwarding of the results of the optimised monitoring of the suspicious transaction reports to the users.

The national and international exchange of intelligence within the FIU network and the resulting initiation of new accordingly the support of ongoing investigations by public prosecutors' offices, was conducted by the "operational part of the FIU" with great success during the reporting year.

The activities of the FIU Germany contributed to the success achieved in the fields of prevention and suppression of money laundering as well as the financing of terrorism.

In doing so, the FIU has always received constructive support from the various agencies involved in Germany and abroad. We, the FIU, therefore wish to express our thanks to the staff members of all our co-operation partners in Germany and abroad.

Dr. Michael Dewald  
Head of FIU Germany

## 2 Reporting behaviour of parties required to report

### 2.1 Nationwide case statistics for 2006

#### 2.1.1 Suspicious transaction reports filed pursuant to the Money Laundering Act (MLA)

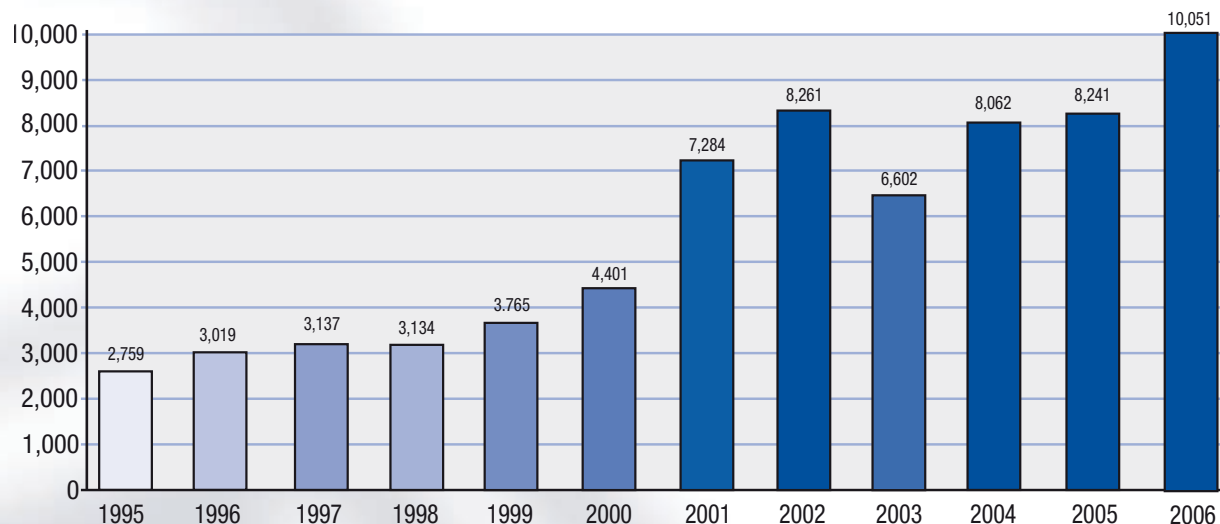
In 2006, a total of **10,051** suspicious transaction reports were filed pursuant to the Money Laundering Act. This is the largest number of reports filed since the Money Laundering Act came into force in 1993. Compared with the previous year (**8,241** suspicious transaction reports), a considerable increase of 22% (**1,810** reports) was recorded, without any comparable key contributors like in 2001 and 2002 (introduction of the euro, terrorist attacks) having been the reason. The increase is mainly due to the credit unions and co-operatives (+606), financial transfer service providers (+413), other credit institutions (+403) and savings banks / state central banks (+378).

The following graph illustrates the development of the suspicious transaction reports filed with the clearing offices in the German states pursuant to the Money Laundering Act between 1995 and 2006. The figures exclusively refer to initial reports. Follow-up reports relating to previously submitted reports are not considered.





**Graph 1: Suspicious transaction reports filed pursuant to the Money Laundering Act, 1995 – 2006**



During the year under review, credit institutions filed about **81%** of all suspicious transaction reports pursuant to the Money Laundering Act. Thus, their percentage share in the total number of reports remained unchanged compared to the previous year. The same applies to the number of reports filed by financial service providers (about 18% in 2006 and 2005).

The number of reports filed by insurance companies remains unchanged with 35 reports. However, it has to be taken into account that insurance companies are to be regarded as "institutions" as defined in Section 1 (4) of the Money Laundering Act (with the corresponding obligations) only when issuing accident insurance policies with premium return clauses (2006: one report) or life insurance policies (2006: 15 reports). With all other insurance products (2006: 20 reports / 2005: 17 reports), they are regarded as "other self-employed persons engaged in trade" ("other business persons" under the Money Laundering Act).

In contrast to this, reports filed by parties required to report pursuant to Section 3 (1) of the Money Laundering Act, such as real-estate brokers (1), lawyers (3), auditors (2), tax consultants (2), "other business persons" (2) and "other parties required to report in accordance with Section 3 (1) of the Money Laundering Act" (3) declined by approximately **46%** (from 24 to 13 reports).

The reporting behaviour of the parties required to report pursuant to Section 3 (1) of the Money Laundering Act must be described as inadequate, also in view of the large number of natural persons and legal entities belonging to this group.



Table 1: "Reports filed pursuant to the Money Laundering Act" by reporting party

			2006	2005	Change from 2005
<b>Suspicious transaction reports pursuant to the Money Laundering Act (initial reports)</b>	<b>Banks</b>	Credit banks	2,882	2,787	
		Saving banks and state central banks	3,072	2,694	
		Credit unions and co-operatives	1,632	1,026	
		Deutsche Bundesbank and main branches	49	50	
		Other	508	105	
		<b>Total</b>	<b>8,143</b>	<b>6,662</b>	<b>22.2%</b>
	<b>Insurance companies</b>	Insurance companies	35	35	
		of which: life assurance policies	14	18	
		of which: report by insurance agent	---	2	
		of which: accident insurance policies	1	---	
		<b>Total</b>	<b>35</b>	<b>35</b>	<b>0.0%</b>
	<b>Financial service providers</b>	Financial transfer services	1,779	1,366	
		Currency services	2	7	
		Credit cards	4	4	
		Traveller`s cheques	---	---	
		Other	53	123	
		<b>Total</b>	<b>1,838</b>	<b>1,500</b>	<b>22.5%</b>
	<b>Investment companies</b>	<b>Total</b>	<b>1</b>	<b>2</b>	<b>-50.0%</b>
	<b>Financing companies</b>	Factoring	---	1	
		Leasing	1	1	
		Other	2	1	
		<b>Total</b>	<b>3</b>	<b>3</b>	<b>0.0%</b>

		2006	2005	Change from 2005
<b>Suspicious transaction reports pursuant to the Money Laundering Act (initial reports)</b>	Casinos			
	Total	4	6	-33.3%
	Government authorities (Sec. 13,16 of the Money Laundering Act)			
	Federal Ministry of Finance	---	1	
	BaFin (regulatory authority for financial services pursuant to the Credit Act)	4	1	
	BaFin (regulatory authority for insurance companies pursuant to the Insurance Law)	---	---	
	BaFin (regulatory authority for securities pursuant to the Securities and Exchange Law)	---	---	
	Regulatory bodies for the insurance sector (excluding BaFin)	---	---	
	Other authorities	4	7	
	Total	8	9	-11.1%
	Other parties required to report			
	Lawyers	3	11	
	Legal aid providers	---	---	
	Patent attorneys	---	---	
	Notaries	---	1	
	Qualified auditors	2	1	
	Certified accountants	---	1	
	Tax consultants	2	6	
	Agents in tax matters	---	---	
	Real-estate brokers	1	---	
	Other business persons	2	4	
	Asset managers	---	---	
	Other parties required to report (Sect. 3 (1) MLA)	3	---	
	Total	13	24	-45.8%
	Other reports filed pursuant to the Money Laundering Act			
	Total	6	---	
	<b>Total</b>	<b>10,051</b>	<b>8,241</b>	<b>22.0%</b>



### 2.1.2 Other reports of suspected money laundering

All over Germany, a total of **530** other initial reports of suspected money laundering were additionally filed in 2006. The number of these reports declined by **3.5%** compared to the total number of reports filed in 2005 (**549**). The number of reports filed by the tax authorities pursuant to Section 31 (b) of the Fiscal Code in 2006 (**335**) increased only slightly compared to the previous year (**330**).

The significant drop in connection with checks for cash made by the customs / Federal police from **62** to **nine** cases is due to the fact that these cases are not to be recorded in the "money laundering" data network any more.

**Table 2** "Other reports indicating money laundering activity" by reporting party

Other reports indicating money laundering activity	Number		Change from 2005
	2006	2005	
Private citizens	26	47	
Other reports	53	5	
Customs / Border Guard / police cash checks pursuant to the Customs Act (Sec. 12a-12c)	9	62	
Tax authorities (Sec. 31 of the Tax Law)	335	330	
Domestic law enforcement authorities	102	98	
Foreign law enforcement authorities	1	4	
Other government agencies (not defined in Sec. 13, 16 of the Money Laundering Act)	4	3	
<b>Total</b>	<b>530</b>	<b>549</b>	<b>-3.5%</b>

### 2.1.3 Distribution of suspicious transaction reports pursuant to the Money Laundering Act over the German states

The following table shows the distribution of suspicious transaction reports filed pursuant to the Money Laundering Act among the German states responsible for the clearing process. As in previous years, the majority of the suspicious transaction reports (about 65%) were filed in Bavaria (2,164), North Rhine-Westphalia (2,142), Baden-Württemberg (1,109) and Hessen (1,74).

In all of the German states, an increase compared to the previous year has been ascertained. High percentage increases are recorded in particular in Thuringia (70%), Saxony-Anhalt (58%), Brandenburg (55%) and Bremen (51%), however, all mentioned states are not on top of the list in terms of absolute figures. The biggest absolute increases are recorded in Bavaria (+468), North Rhine-Westphalia (+367) and Lower Saxony (+196).

Table 3: Suspicious transaction reports pursuant to the Money Laundering Act by state

Federal state	Number		Change from 2005
	2006	2005	
Baden-Württemberg	1,109	964	15.0%
Bavaria	2,164	1,696	27.6%
Berlin	573	533	7.5%
Brandenburg	198	128	54.7%
Bremen	131	87	50.6%
Hamburg	420	361	16.3%
Hessen	1,074	1,063	1.0%
Mecklenburg-Western Pomerania	98	89	10.1%
Lower Saxony	747	551	35.6%
North Rhine-Westphalia	2,142	1,775	20.7%
Rheinland-Palatinate	339	269	26.0%
Saarland	91	65	40.0%
Sachsen	298	212	40.6%
Saxony-Anhalt	171	108	58.3%
Schleswig-Holstein	336	246	36.6%
Thuringia	160	94	70.2%
<b>Total</b>	<b>10,051</b>	<b>8,241</b>	<b>22.0%</b>

### 2.1.4 Reports of possible criminal offences (from the perspective of the reporting parties)

The suspicious transaction reports pursuant to the Money Laundering Act and other reports indicating money laundering activity forwarded to the FIU in 2006 contained a total of **3,490** references to criminal offences. The listing of multiple offences in a single report was possible. Compared to 2005 (1,259 reports), this means an increase of **177%**.

The number of reports indicating possible fraud offences almost quadrupled with **2,789** listings compared to the previous year (**735** listings). Among the **2,789** listings were **1,913** suspicious transaction reports filed in connection with the "phishing" / "financial agents" phenomenon.<sup>1</sup>

The offence of "money laundering" will not be explicitly included in the following table for 2006 since it can always be assumed that this offence has been committed – except for reports filed in connection with the financing of terrorism.

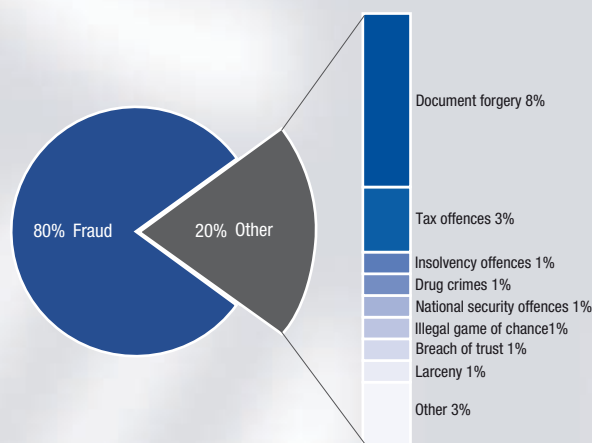
**Table 4: Reports of possible criminal offences from the perspective of the reporting parties (TOP 10)**

Possible criminal activity	Number		Change from 2005
	2006	2005	
Fraud	2,789	735	279.5%
Document forgery	273	111	145.9%
Tax offences	111	125	-11.2%
Insolvency	47	21	123.8%
Drug crimes	40	50	-20.0%
National security offences	33	31	6.5%
Illegal game of chance	33	6	450.0%
Breach of trust	33	26	26.9%
Larceny	29	7	314.3%
Extortion	6	3	100.0%
Other	96	144	-33.3%
<b>Total</b>	<b>3,490</b>	<b>1,259</b>	<b>177.2%</b>

<sup>1</sup> For further information, see item 3.3.4.

The following graph shows the ratio between the percentage of reports referring to fraud and the percentage of reports referring to other offences as compared with the total number of suspicious transaction reports with references to criminal offences. The percentage of approximately **80%** (**2,789** listings) of reports referring to fraud is even more distinct than in the previous year (**58%**). The total listings of all other offences amount to **701** during the period under review (2005: 524).

**Graph 2: Reports of possible criminal offences from the perspective of the reporting parties**



### 2.1.5 References to foreign involvement in suspicious transaction reports pursuant to the Money Laundering Act

The following is a description of transactions with references to countries of origin and destination for transferred assets, regardless of the frequency and amounts of such transactions. Where several countries were mentioned in one suspicious transaction report, they were listed, too.

### Transfer of assets to foreign countries

A considerable increase in the number of transfers of assets to Russia (+362 listings) and Ukraine (+156 listings) has been recorded. This increase can primarily be explained by the increasing number of suspicious transaction reports filed with regard to "financial agents".

A strikingly large decrease is recorded for transactions to Nigeria (-41%), after a recorded decrease of 22% in 2005 already. This is probably due to the numerous suspicious transaction reports filed in the previous years on completed fraud cases involving the so-called "Nigeria letters"<sup>2</sup>. During the period under review, hardly any such cases were the subject of suspicious transaction reports any more.

**Table 5: Suspicious transaction reports on transfers of assets to foreign countries (TOP 10)**

Countries	Number		Change from 2005
	2006	2005	
Russia	500	138	262.3%
Ukraine	213	57	273.7%
Turkey	112	100	12.0%
China	105	123	-14.6%
Nigeria	96	162	-40.7%
Spain	91	114	-20.2%
Netherlands	86	114	-24.6%
USA	84	100	-16.0%
France	78	80	-2.5%
Austria	77	53	45.3%
Other	1,530	1,542	-0.8%
<b>Total</b>	<b>2,972</b>	<b>2,583</b>	<b>15.1%</b>

### Transfer of assets from foreign countries

Particularly large increases in the number of reported suspicious transfers of assets from abroad were recorded for Spain (+ 53%) and Austria (+ 48%). In contrast to this, a disproportionate decrease to 79 from 128 listings (-38%) was recorded for the United Kingdom.

**Table 6: Suspicious transaction reports on transfers of assets from foreign countries (TOP 10)**

Countries	Number		Change from 2005
	2006	2005	
USA	168	186	-9.7%
Russia	139	123	13.0%
Kazakhstan	126	127	-0.8%
Switzerland	105	106	-0.9%
Spain	98	64	53.1%
Italy	82	88	-6.8%
France	81	77	5.2%
Great Britain	79	128	-38.3%
Austria	68	46	47.8%
Netherlands	58	60	-3.3%
Other	1,363	960	42.0%
<b>Total</b>	<b>2,367</b>	<b>1,965</b>	<b>20.5%</b>

<sup>2</sup> Fraudsters, most of them living in Nigeria, send letters in which they ask for assistance in the transfer of millions to foreign countries. Parties interested are promised high commissions. Prior to settling the business, the perpetrators demand payment of fees which are to be transferred mainly to Nigeria. The money paid in advance is lost since the perpetrators never intend to transact business but only aim at fraudulently receiving the fees.

### 2.1.6 Suspects

In 2006, **18,735** suspects in total<sup>3</sup> were listed. This means an increase of approximately 20% compared to the preceding year (2005: 15,621).

#### Nationality

The percentage of German suspects amounts to about 57% and thus remained almost unchanged (2005: 55%). Among the top ten, the number of Kazakh suspects increased most significantly, with a rise of 55% over the preceding year, from 140 references (2005) to 217 (2006). This is probably due to public reports according to which organised crime groups were transferring funds to Germany from Kazakhstan. Although the FIU was unable to verify these reports, they apparently had an effect on the filing of suspicious transaction reports.

In contrast to this, a decrease of 30% (to 214 from 304 listings) of the number of Polish suspects has been recorded. This could be due to measures focussing on the German-Polish border area, taken by the law enforcement agencies in 2005, which led to an increase of 122%.

Table 7: Nationalities (TOP 10)

Suspect nationality	Number		Change from 2005
	2006	2005	
German	8,049	6,809	18.2%
Turkish	681	690	-1.3%
Russian	608	500	21.6%
Chinese	247	207	19.3%
Italian	243	275	-11.6%
Kazakh	217	140	55.0%
Polish	214	304	-29.6%
Nigerian	200	170	17.6%
Iranian	197	174	13.2%
Serbian	164	134	22.4%
Other	3,285	3,054	7.6%
unknown / no entry	4,630	3,164	46.3%
<b>Total</b>	<b>18,735</b>	<b>15,621</b>	<b>19.9%</b>

<sup>3</sup> The figures for suspects are based on suspicious transaction reports pursuant to the Money Laundering Act and other reports.



## Residence

Of the suspects cited in suspicious transaction reports and other reports indicating money laundering activity, **12,124** individuals (approximately 65%) had their residence in the Federal Republic of Germany (2005: approximately 70%).

A considerable increase has been recorded for residences stated to be in Ukraine (+234%), Romania and Kazakhstan (+120% each) as well as Russia (+114%). The increase in the number of suspects having their residence in Ukraine and Russia can primarily be explained by suspicious transaction reports filed against "financial agents" or the final beneficiaries residing in those countries.

**Table 8: Country of residence (TOP 10)**

Countries	Number		Change from 2005
	2006	2005	
Germany	12,124	10,968	10.5%
Russia	494	231	113.9%
Kazakhstan	145	66	119.7%
Nigeria	131	92	42.4%
Italy	129	103	25.2%
Ukraine	117	35	234.3%
Switzerland	106	111	-4.5%
USA	101	65	55.4%
Romania	88	40	120.0%
Netherlands	87	84	3.6%
Other	1,799	1,054	70.7%
Unknown / no entry	3,414	2,772	23.2%
<b>Total</b>	<b>18.735</b>	<b>15.621</b>	<b>19.9%</b>

## Occupation

In respect of the **18,735** suspects mentioned in the suspicious transaction reports and other reports indicating money laundering activity, occupations were cited in **5,050** cases (2005: 4,001), which means an increase of approximately **26%** compared to 2005. This increase in the number of occupations cited (+ 1,049) suggests that parties required to report are becoming increasingly aware of the importance of the "know your customer (KYC)" principle in the process of establishing suspicion. The increase of approximately 44% for car dealers and approximately 41% for self-employed as well as freelance workers and employees is striking.

**Table 9: Suspects by occupation (TOP 10)**

Occupation	Number		Change from 2005
	2006	2005	
Corporate Director	757	660	14.7%
Freelance / independent	442	312	41.7%
Employee	402	285	41.1%
Student	298	296	0.7%
Unemployed	272	202	34.7%
Shareholder (partner)	272	216	25.9%
Pensioner	180	153	17.6%
Labourer	144	122	18.0%
Car Dealer	143	99	44.4%
Housewife	140	105	33.3%
other	2,000	1,551	28.9%
<b>Total</b>	<b>5,050</b>	<b>4,001</b>	<b>26.2%</b>

### 2.1.7 Corporate headquarters

During the year under review, **4,191** corporate headquarters were listed (2005: 3,647)<sup>4</sup>, **2,439** of them in Germany (2005: 1,950).

The repeated increase of reported companies in the "British Virgin Islands" offshore territory<sup>5</sup> to 44 from 24 (+ 83%) and the decrease of listed offices in the United Kingdom to 62 from 84 (- 26%) are striking here.

**Table 10: Corporate headquarters (TOP 10)**

Suspicious companies – Principal offices in:	Number		Change from 2005
	2006	2005	
Germany	2,439	1,950	25.1%
Switzerland	75	68	10.3%
Great Britain	62	84	-26.2%
USA	59	61	-3.3%
Netherlands	47	37	27.0%
British Virgin Islands	44	24	83.3%
Russia	43	32	34.4%
Austria	32	24	33.3%
Spain	28	24	16.7%
Italy	24	22	9.1%
Other	98	346	-71.7%
Unknown / no entry	1,240	975	27.2%
<b>Total</b>	<b>4,191</b>	<b>3,647</b>	<b>14.9%</b>

### 2.1.8 Business sectors

In **1,079** cases, information on the business sectors was given (2005: 840). This represents a **28%** increase compared to the preceding year. An increase has been recorded in all of the mentioned sectors, with the building and construction sector still being the business sector most frequently listed (**116**) by the parties required to report, followed by the car trade (**106**), export / import (**81**) and the real estate business (**62**).

The increase in the number of suspicious transaction reports filed in connection with lotteries and betting activities to 39 from 12 (+ **225%**) is striking, most of them are, however, believed to be based on clear fraud cases.

**Table 11: Business sectors (TOP 10)**

Business sector	Number		Change from 2005
	2006	2005	
Building and construction	116	75	54.7%
Motor vehicle dealers and agents	106	54	96.3%
Export / import	81	70	15.7%
Real-estate brokerage	62	35	77.1%
Associated companies	43	17	152.9%
Computer	42	18	133.3%
Lotteries and betting	39	12	225.0%
Corporate Consulting	37	27	37.0%
Telecommunication	34	27	25.9%
Assets managers / trust executors	30	21	42.9%
Other	489	469	4.3%
<b>Total</b>	<b>1,079</b>	<b>840</b>	<b>28.5%</b>

<sup>4</sup> The figures are based on suspicious transaction reports pursuant to the Money Laundering Act and other reports.

<sup>5</sup> Group of islands in the Caribbean (100 km east of Puerto Rico) consisting of Beef Island, Anegada, Virgin Gorda and Tortola.

## 2.1.9 Accounts

From the **12,535** accounts recorded in total<sup>6</sup> (2005: 11,306), the type of account was given in **5,988** of the cases (2005: 4,923). Private accounts (**1,679** listings), current accounts (**1,609**) and business accounts (**1,143**) are on top of the list. In 2005, the current accounts still represented the largest part with a third of all mentioned types of accounts. The increase in private accounts is believed to be due to the considerable increase in suspicious transaction reports in connection with "phishing" / "financial agents".

**Table 12: Types of accounts**

Type of account	Number		Change from 2005
	2006	2005	
Private account	1,679	1,090	54.0%
Current account	1,609	1,585	1.5%
Business account	1,143	898	27.3%
Savings / investment account	776	647	19.9%
Deposit account	194	175	10.9%
Loan account	182	137	32.8%
Currency account	81	72	12.5%
Credit card account	78	104	-25.0%
Attorney trust account	71	50	42.0%
Bank deposit box / bank safe	67	68	-1.5%
Joint account	40	30	33.3%
Thrift account	18	17	5.9%
Time deposit account	17	14	21.4%
Fixed term deposit account	10	13	-23.1%
Trust account	8	8	0.0%
Direct account	6	1	500.0%
Aval credit account	5	13	-61.5%
Clearing account	4	1	300.0%
<b>Total</b>	<b>5,988</b>	<b>4,923</b>	<b>21.6%</b>

<sup>6</sup> The figures are based on suspicious transaction reports pursuant to the Money Laundering Act and other reports.

## 2.1.10 Grounds for suspicion

For a more precise recording of the grounds for suspicion for which the parties required to report filed an MLA report, the FIU defined a catalogue according to which the cases reported are assessed and stored in the FIU database.

This catalogue "grounds for suspicion" is divided into the following categories:

1. Unusual indication / link to other cases
2. Document / certificate / identification
3. Company
4. Type of transaction
5. Subject of transaction
6. Account opening / management
7. Product / customer
8. Financing of terrorism
9. Grounds for suspicion not specifiable

Each category comprises various grounds for suspicion that are used for storage in the FIU database. When several grounds were decisive for the generation of the suspicious transaction report from the point of view of the reporting party, they can all be listed.



**Table 13: Grounds for suspicion indicated by the parties required to report**

Category	Grounds for suspicion	Number
Special hints / links to known cases	Transfer fraud	1,674
	Link to known investigation	698
	Internet transactions	490
	Region involved	165
	Games of chance / bets	86
	Other (special) hints / links to known cases	75
	Fraudulent offers	68
	Direct debit fraud	46
	Press releases / Open source information	41
	Social security fraud	35
	BaFin circulars	3
	<b>Total</b>	<b>3,381</b>
	Document / certificate / identification	Document forgery
Smurfing		133
Other (document / certificate / identification)		31
Difficulties in / refusal of identification		26
<b>Total</b>		<b>432</b>
Company	Business activity	186
	Fictitious / letter-box company	83
	Other (company)	54
	Structure / network of companies	30
	Payment of commissions / bribes	17
	Persons involved / business partners	14
	Company foundation	13
	<b>Total</b>	<b>397</b>
Kind of business ("how")	Cash	2,455
	Non-Cash	827
	Credit	223
	Barter	191
	Capital investment	56
	Insurance	33
	Other (kind of business)	4
	<b>Total</b>	<b>3,789</b>

Category	Verdachtsgrund	Number
Business purpose ("what")	Cheque	390
	Vehicle	304
	Real Estate	232
	Building and construction	54
	Securities	38
	Precious metals	27
	Other (business purpose)	15
	Catering sector	13
	Counselling / brokerage	10
	Precious stones	6
	Electronics	6
	Services	6
	Expensive goods (other)	6
	Boats	5
	Art	4
	Licences / patents (rights)	1
	<b>Total</b>	<b>1,117</b>
Account opening / account keeping	Account use	3,204
	Transactions	1,242
	Economic background	1,063
	Economic authorisation	227
	Transfers through uneconomic / indirect channels	72
	Financial (transfer) transaction without required authorisation	27
	Other (account opening / keeping)	8
	E-money	1
		<b>Total</b>
Product / customer	Customer behaviour	786
	Safe deposit box	54
	Other (product / customer)	33
	Conditions	26
	Cash dispensers	26
	Type of account	24
	Persons in prominent political and / or economic positions	3
		<b>Total</b>
Financing of terrorism	Other (financing of terrorism)	28
	Matches with listed persons	21
	criminal association / organisation	10
		<b>Total</b>
No-specific grounds for suspicion	No specific grounds for suspicion	49
		<b>Total</b>
<b>Overall total</b>		<b>16,020</b>



Through the introduction of the new catalogue "grounds for suspicion", a comparison with the "general grounds for suspicion" published in previous years is possible to a limited extent only. From the FIU's perspective, the following trends identified in reporting year 2006 are worth mentioning:

#### Transfer fraud

In this category, **1,674** suspicious transaction reports are recorded which were filed in connection with the "phishing" as "financial agents" phenomenon. Since another **239** reports in connection with "phishing" and "financial agents" were not listed under "transfer fraud" but under "Internet transactions", "links to known investigation" or "fraudulent offers", the number of the relevant suspicious transaction reports totals **1,913** in 2006. Compared to 2005 (**346** reports), this means an increase by **1,567** reports.

#### Internet transactions

The suspicious transaction reports involving "Internet transactions" (**490** cases) increased considerably in 2006 (+ **280** cases). They cite less grounds for suspicion in respect of money laundering activities, but rather give information on possible fraud and tax offences.

#### Real estate

The number of suspicious transaction reports filed in connection with real estate transactions in 2006 increased to **232** compared to **183** in the preceding year. The investment of illegal assets in real estate for money laundering purposes represents a phenomenon that is becoming increasingly important. Consequently, by creating a "case collection" and by the "monitoring of suspicious transaction reports", the FIU attempts to present indicators which show typical concealment methods in connection with real estate transactions.

It seems to be worth mentioning in this context that almost all of the suspicious transaction reports – with only one exception – were filed by the account-keeping institutions not by the real estate brokers separately required to report pursuant to Section 3 (1) of the Money Laundering Act.

#### Fraudulent offers / document forgery / cheques

A total of **700** suspicious transaction reports were recorded under these grounds for suspicion, with a large part of them not subsumed under money laundering in the sense of Section 261 of the German Penal Code, but suspected fraud and document forgery (cheque fraud, cheque forgery etc.). As these reports distort the (statistical) situation reports on the money laundering phenomenon, the FIU will compile questions and issues in this regard in an effort to positively influence the reporting behaviour in the sense of the Money Laundering Act.

## 2.2 Results of processing

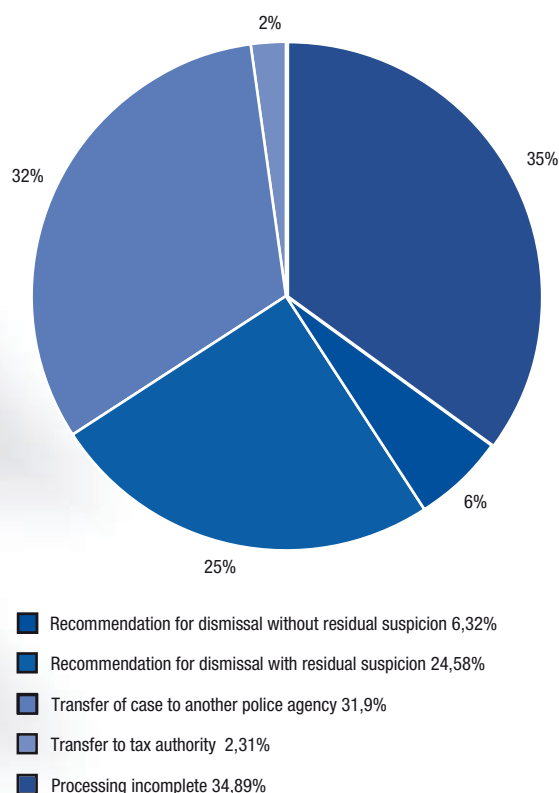
### 2.2.1 Status of report processing at the close of the reporting year

In 2006, police investigations (clearing) were closed without residual suspicion in approximately **6%** of the **10,051** suspicious transaction reports filed pursuant to the Money Laundering Act. In **25%** of all cases, investigations were closed despite the existence of residual suspicion from the police perspective. In approximately **35%** of all cases, processing by the clearing offices had not been completed by year's end.

In approximately **32%** of all cases, the suspicion of money laundering or a different criminal offence was supported to the extent that the cases were forwarded for further investigation to an appropriate police investigation office. In about another **2%** of all cases, the suspicion of tax offences was supported so that the cases were forwarded to the tax authorities.

Thus, like in 2005, the suspicion of a criminal offence was supported in about one third of all reports.

Graph 3: Results of processing by Money Laundering Clearing Offices of the State Criminal Police Offices (LKÄ)



## 2.2.2 Cases transferred to other specialised investigative agencies

Upon completion of processing by the Money Laundering clearing offices of the state criminal police offices, approximately one third of all suspicious transaction reports were forwarded to other specialised investigative agencies. In these cases, connections with the following types of crime were identifiable (multiple entries were possible in a given report):

**Table 14: Connections to types of crime identified by Clearing Offices in cases forwarded to other investigative agencies (TOP 10)**

Type of crime	Anzahl		Veränderung zum Vorjahr
	2006	2005	
Fraud	1,674	1,080	55.0%
Money Laundering	968	284	240.8%
Document forgery	156	110	41.8%
Tax offences	82	61	34.4%
Drug crimes	63	92	-31.5%
Breach of trust	59	44	34.1%
Insolvency offences	49	31	58.1%
Illegal employment	22	5	340.0%
Larceny	17	12	41.7%
Offences against custom laws	13	16	-18.8%
Other	329	189	74.1%
<b>Total</b>	<b>3,432</b>	<b>1,924</b>	<b>78.4%</b>

"Fraud" with about **49%** of the total number of cases was most frequently recorded as type of crime. It is also interesting to note that the number of cases forwarded by the clearing offices to other investigative agencies for suspected money laundering has increased. This is probably due to the increase in the number of reports relating to the "phishing" and "financial agent" phenomenon.

## 2.3 Summary and evaluation

### 2.3.1 Summary of report volume in 2006

- In 2006, a total of **10,051** suspicious transaction reports were filed pursuant to the Money Laundering Act. This marks a significant rise by **1,810** suspicious transaction reports compared to the previous year (+ **22%**).
- The number of other reports relating to money laundering (**530**) decreased by **3.5%** compared to the preceding year (**549**). The number of reports filed by the tax authorities in 2006 pursuant to Section **31b** of the Fiscal Code (**335**) increased only slightly compared to the previous year (**330**).
- The number of reports containing references to fraud offences almost quadrupled with **2,789** listings compared to the previous year (**735** listings). Among the **2,789** listings were **1,913** suspicious transaction reports filed in connection with the "phishing" / "financial agents" phenomenon.
- A sharp increase in listings involving suspicious money transfers to Russia (to **500** from **138**) and Ukraine (to **213** from **57**) was identified in 2006.
- This increased total number of suspicious transaction reports is believed to be the reason for the almost identical percentage increase in the listed occupations of the suspects, the principal corporate offices, the business sectors and the types of account.
- The following changes in the results of processing were identified as compared to the previous year:
  - Recommendation for dismissal without residual suspicion in **6%** of all cases (2005: **14%**).



- Recommendation for dismissal with residual suspicion in 25% of all cases (2005: 25%).
- Transfer of cases to other specialised offices in 32% of all cases (2005: 32%).
- Transfer of cases to tax authorities in 2% of all cases (2005: 3%)
- Processing not completed in 35% of all cases (2005: 26%)

### 2.3.2 Evaluation of report volume in 2006

- The reason for the considerable increase in the number of suspicious transaction reports mainly lies in the increase of reports filed in connection with the "phishing" and "financial agent" phenomenon (to **1,913** from 346 listings). Searches on the part of the financial transfer service providers, targeting in particular the "financial agents" phenomenon, uncovered a large number of cases which were reported in 2006. This aggressive move was accompanied by an intensified co-operation between the financial transfer service providers and the banks concerned, the banking associations and investigative authorities in Germany and abroad as well as by the provision of information and warnings. The following efforts made by the financial transfer service providers are listed as examples which did not only lead to an increase in the number of reports filed, but can be considered as effective measures for prevention and repression:
  - Regular provision of new information on "financial agents" to the partners.

- In suspicious transactions, the customers were advised on a form to be signed about the existing risk of being used as a "financial agent" and / or committing a crime.
- Persons involved are "barred" from further transactions, i.e. put on so-called "block lists" if a concrete suspicion is revealed.
- The enormous increase of transfers to Russia and Ukraine can be explained by the "phishing" / "financial agents" phenomenon. The financial agents mainly transferred the funds received in their accounts to these countries.
- The types of crime identified from the investigative results showed a remarkably high correlation with the offences cited by the reporting parties, with fraud offences (49%) still representing by far the largest part.



### 3 Monitoring of suspicious transaction reports

#### 3.1 Introduction

Pursuant to Section 5 subsection 1 (5) of the Money Laundering Act, the FIU has the task to monitor suspicious transactions reports filed in accordance with the Money Laundering Act and reports filed by the tax authorities pursuant to Sect. 31b of the Fiscal Code and to regularly inform parties required to report pursuant to this Act about money laundering typologies and methods.

By measures aiming at optimising structures and processes within the FIU, which were implemented on January 1<sup>st</sup> 2006, the monitoring of all suspicious transaction reports received has been re-structured and re-oriented.

The monitoring of suspicious transaction reports means a qualified analysis of all initial reports on money laundering and the financing of terrorism. This is done according to the following five categories:

##### a) "Noteworthy cases"

Cases classified as "noteworthy" are those filed in connection with individuals in prominent business, political or social positions, with media coverage or a high transaction volume (exceeding three million euros) but where no new typologies are identified.

The Financial Intelligence Unit obtains the current status of such cases from the criminal justice authorities with original jurisdiction and, if relevant, initiates or directly offers additional measures (for instance by sending enquiries to foreign FIUs).

##### b) "Monitoring of trends"

If the monitoring reveals new trends with regard to phenomena of money laundering that are relevant to analysis or investigation (such as an unusual accumulation of similar grounds for suspicion, facts of the case or the like), this trend is monitored for a limited period with a view to obtaining statistical figures. On this basis, research on the causes is made in dialogue with the parties involved in the case. The identification of new trends and a feedback are important especially for those required to report pursuant to the Money Laundering Act.

##### c) "Typology"

At the beginning, when the suspicious transaction report is filed, a search for possible money laundering typologies is feasible to a limited extent only, due to the early stage of the case.

However, if the suspicious transaction reports suggest new money laundering typologies at this early stage already, they are directly passed on to the FIU case collection with the note "cases to be checked"<sup>7</sup>.

If a case is classified as a new typology by the FIU case collection, the concealment method is analysed, processed and put down in writing and a feedback is provided to the parties required to report pursuant to the Money Laundering Act.

<sup>7</sup> The case collection firstly means compilation, analysis and storage of case descriptions, which show different modi operandi of concealment methods relating to money laundering/disposal of assets in the widest sense for cash flows and non-cash flows. Besides gathering information from the copies of the suspicious transaction reports that are centrally received by the FIU (independent of an investigation), case constellations are also taken into consideration that are integrated into investigations. The case collection also includes cases relating to the financing of terrorism.

#### **d) Indicators for the financing of terrorism**

The FIU forwards copies of the suspicious transaction reports containing information on the financing of terrorism to the financial investigation section of the State Security Division at the Bundeskriminalamt so that immediate contact can be made with the competent state security authority with original jurisdiction at the State Criminal Police Office concerned and the necessary urgent measures can be taken.

#### **e) No relevance to analysis**

Suspicious transaction reports that are not classifiable under the categories a) to d) are not submitted to any further analysis.

The following objectives are pursued with the monitoring of suspicious transaction reports:

- Prompt identification of new methods / typologies of money laundering and emerging trends, including research into the causes, and provision of a feedback to the addressees of the Money Laundering Act, especially the parties required to report
- Provision of information about noteworthy cases and cases to be checked in respect of typology for entry in the "FIU Case Collection" with a view to presenting new money laundering typologies
- Formulation of topics to be subjected to strategic and operational analysis
- Prompt development of strategies / concepts for optimising the suppression of money laundering and the financing of terrorism

The results of analysis are also compared with the information gathered from the follow-up responses submitted by the public prosecutor's offices pursuant to Section 11 (9) of the Money Laundering Act and from the international FIU information exchange and are thus supported by a broad basis of information.

Feedback about the results obtained is provided to those obligated by the Money Laundering Act through publication in the Annual Reports, holding specialist meetings on a case-by-case basis, presenting lectures at seminars and conferences of the reporting parties, during the meeting of the Working Party of Banks and Chambers organised annually by the FIU, and through the FIU Newsletters.

The following is a selection of "noteworthy cases", "trends" and new "methods / typologies" obtained from the suspicious transactions reports in accordance with the Money Laundering Act and reports filed by the tax authorities pursuant to Section 31b of the Fiscal Code during the period under review.



### 3.2 Noteworthy cases

In the previous FIU Annual Reports, the description of noteworthy cases was given much attention. Due to the fact that a large number of cases was published in the 4<sup>th</sup> Newsletter of the FIU, only a small selection of cases will be described in this Annual Report.

#### Case 1 Securities transaction

A German management consulting firm held a portfolio with the pertinent account with a German bank. Seven million shares worth about 77 million euros of a foreign company A were credited to this portfolio from another portfolio which the management consulting firm held with a foreign bank. The shares had just been quoted on the stock exchange a few days before and their value increased by of more than 1,000% since then.

Two weeks after the transfer of shares, the CEO of the management consulting firm arranged for the re-transfer of 6.5 million shares to the foreign bank, this time, however, to the portfolio of another firm B in Germany. The CEO, who also belonged to the management of firm B, stated that the shares were to be distributed to customers there. The remaining 500,000 shares in the portfolio of the management consulting firm in Germany were to be used as commission.

Essential characteristics of the case:

- Movement of funds probably originating from a violation of the Securities Trading Act (market manipulation).
- Use of German and foreign portfolios as transit / collective accounts and for re-transfers with a view to concealing the channels through which the funds are channelled.

#### Case 2 Internet providers

The services of a German Internet provider were offered and billed through a German company A, with the payment transactions being handled online from Switzerland by the managing director. The Internet provider kept a business account with a German bank and about 6.2 million euros were credited to this account from company A during the first half of 2006 which were re-transferred to different persons, stating the purpose of payment as "withdrawal".

The individuals were former partners of the Internet provider. According to the managing director, the company was sold to a Swiss holding company in June 2006 which had also made deposits to the business account since then.

Essential characteristics of the case:

- Billing of services through third persons
- Private withdrawals by former partners
- Sale of the company to a foreign holding company

### Case 3 Import / export companies

Payments from three import / export companies abroad, all domiciled in the British Virgin Islands, involving about 3.8 million euros, were received in the business account (current account) of a German import as well as export company. The funds always came from a bank in Lithuania.

The incoming payments were always transferred by the managing director to lorry and / or commercial vehicle dealers in Germany within the next few days. In return, the dealers allegedly supplied lorries to a large group of companies near Moscow.

Two re-transfers amounting to 220,000 euros were paid to the account of a company domiciled in the Seychelles, held with a bank in Latvia.

Essential characteristics of the case:

- Transfer of funds to business accounts in Germany through various foreign banks (transfers from Lithuania to companies domiciled in the British Virgin Islands).
- Re-transfer of the funds to dealers in Germany for the purchase of lorries on behalf of a group of companies in Russia.
- Re-transfers to Latvia and the Seychelles.



### 3.3 Monitoring of trends

Suspicious transaction reports that – given their similar characteristics, topics, modi operandi – either suggest new trends or could be relevant due to existing trends which are monitored for an initial period of three months.

#### 3.3.1 Internet auctions

In connection with eBay auctions, funds were transferred to private accounts in a large number of cases and were withdrawn cash immediately afterwards. The goods were offered to the buyers at excessive prices, as stolen goods or counterfeits of branded goods. In most of the cases, no goods were supplied at all.

In the first quarter of 2006, a total of 65 suspicious transaction reports of this type were filed pursuant to the Money Laundering Act. Since the pertinent financial transactions exclusively based on fraudulent acts, the monitoring of trends was discontinued. The suspicious transaction reports were merely recorded statistically so that statements on the number of similar fraud cases can be made.

#### 3.3.2 FIFA World Cup 2006

In the second quarter of 2006, the suspicious transaction reports were monitored with regard to references to the FIFA World Cup 2006 in Germany. Fraudulent activities were background of a total of seven suspicious transaction reports filed. In all of the cases, World Cup tickets had been sold via eBay at excessive prices. The profits achieved through the auctions were channelled to private accounts and were withdrawn immediately after receipt. The tickets have not been delivered. Monitoring was discontinued once the World Cup was over.

#### 3.3.3 Clear fraud cases

In the third quarter of 2006, suspicious transaction reports were often filed for clear fraud cases in which the customer of the reporting institution or the institution itself was the prejudiced party (e.g. "eBay frauds", investment fraud, account opening fraud, credit fraud, misappropriation by bank clerks). A monitoring of trends was thus set up in the 4<sup>th</sup> quarter of 2006 in order to obtain information on the reporting behaviour in these cases. During this period, 26 suspicious transaction reports based on clear fraud cases without reference to money laundering were filed.

Besides, 385 suspicious transaction reports exclusively referring to "phishing" were recorded, so that the number of clear fraud cases totalled 411 in the 4<sup>th</sup> quarter of 2006. Thus, out of the 2,577 suspicious transaction reports filed in the 4<sup>th</sup> quarter, almost every 6<sup>th</sup> report contained a clear as well as exclusive lead to a fraud case without any concrete money laundering indicators.

The FIU's indicator paper published in June 2006 already pointed out that the customer as well as the bank should file a fraud complaint in such cases to the local police or the public prosecutor's office.

### 3.3.4 "Phishing" / "financial agents"

Given the large number of cases revealed in 2005, the "phishing" and "financial agents" phenomenon was also subjected to monitoring of trends during the period under review. The following information was gathered:

#### Modus operandi

In recent years, "phishing" in connection with the recruitment of "financial agents" has more and more developed into a lucrative source of income for (Internet) criminals.

#### "Phishing"

By sending e-mails ("phishing mails") via the Internet with "links" to forged websites of alleged banks or Internet auctions, the perpetrators gain access to the account data of individuals and companies. Through the misuse of the account data obtained (e.g. through online transfers made from the victim's account to the accounts of others), considerable losses are caused.

#### "Financial Agents"

Persons who appear to be trustworthy, most of them from Eastern Europe, contact German bank customers directly by e-mail or through (newspaper) advertisements and offer them to act as "financial agents" (or financial couriers, financial managers, financial brokers). A commission of 5% to 10% of the sum is promised to the customers for the use of their private accounts to receive and pass on funds through financial transfer service providers. Usually, the funds were obtained illegally.

#### Offences and case examples

The phenomenon described is found in a number of offences. Some of them are described here as examples:

#### "Phishing"

##### Section 269 of the German Penal Code (falsification of legally relevant data)

With a view to deceiving their victims, the perpetrators create counterfeit e-mails as well as "phishing" websites, which are legally relevant data pursuant to Section 269 of the German Penal Code. At the storage stage already, but especially when sending the e-mails through the Internet, the perpetrator generates an electronic document which deceives another regarding its authenticity, causing him to react in a legally relevant way. This constitutes an offence pursuant to Section 269 of the German Penal Code (punishable with a prison sentence of up to five years or a fine).

##### Section 263 Penal Code (fraud)

The counterfeit e-mail feigns to contain a "link" that allegedly connects the victim to the website of his bank. The e-mail is, however, channelled to the website of the perpetrator. Trusting in the correctness of the website visited, the victim enters his account access data. The act of deception committed by the perpetrators causes the victim to dispose of assets erroneously, which has an asset-reducing effect. Once the perpetrators have gained access to the bank data, they use them for transferring an amount from the victim's account to a bank account known to them without further participation of the victim (financial loss).

This constitutes a case of accomplished fraud (punishable, if committed on a repetitive and gainful basis, with a prison sentence ranging between six months and ten years).



### **Section 263a of the Penal Code (computer fraud)**

The perpetrators cause damage to the assets of another by manipulating the results of data processing operations. This unauthorised use of data and / or the illegal manipulation of an authorised data processing operation constitutes an offence of computer fraud (punishable with a prison sentence of up to five years or a fine).

### **"Financial Agents"**

#### **Sections 261 (4) and 53 of the Penal Code – money laundering on a repetitive and gainful basis**

Case example:

A commission of 5% to 10% was offered to an individual by e-mail if this individual made his bank account available for transfers involving several thousands of euros. The money transferred was to be passed on to Eastern Europe through a financial transfer service provider shortly. In this way, the "financial agent" transferred a total of about 15,000 euros which came from computer frauds ("phishing"). The perpetrator was sentenced to a compounded sentence of one year and six months in prison, suspended on probation, for commercial money laundering in five cases.

Reasons for the judgement:

"The defendant denies having been aware that the money was illegal. This claim is refuted, however. He cannot be spared the accusation that he knew or at least wilfully accepted that the money transferred was illegal. In the light of globalisation, media reports and general knowledge, he must simply have known that only "black" money is handled in the described way. The defendant also acted on a repetitive and commercial basis since he intended to cover at least part of his living expenses with the proceeds."

### **Sections 263a and 27 of the Penal Code – aiding and abetting computer fraud**

Case example:

A commission of 10% was offered to an individual by e-mail if this individual receives transfers in his account from customers of a Russian company and then transfers the money to accounts in Moscow through a financial transfer service provider. The money originated from computer frauds ("phishing"). In this way, the recruited "financial agent" transferred about 14,000 euros in total.

The defendant was fined 1,200 euros (60 day rates of 20 euros each) for aiding and abetting computer fraud.

Reasons for the judgement:

"All in all, the defendant wilfully accepted that the transactions did not base on a legal business. In his statement, the defendant himself admitted to having had doubts in the matter. Apart from the fact that the defendant should have become extremely suspicious due to the unexplainably high profit compared to the minor activity, this remark shows that the defendant had definitely considered that his activities could have been illegal. His behaviour shows that he was prepared to put aside all his doubts in favour of the fast profit."



The "financial agent" may also be threatened with other legal consequences, such as:

- a claim under civil law for re-payment of the money,
- criminal proceedings for negligent money laundering (Section 261 (5) of the Penal Code) and
- administrative proceedings of the BaFin (Federal Association of Public Banks in Germany) for unauthorised financial transfer operations on a repetitive and gainful basis since, given the commission received for his activities, he is making financial transfers on a commercial basis. He is thus providing financial services that require written permission from the BaFin. The BaFin has already opened the first administrative proceedings against individual "financial agents".

The judgements so far passed still show a high level of heterogeneity both with regard to the assessment of the offence and the penalty imposed. Unanimity, however, has been reached regarding the culpability for activities as "financial agent".



### Number of cases

In 2006, **1,913** suspicious transaction reports were filed in connection with the "phishing" / "financial agents" phenomenon (2005: 346). This corresponds to a percentage of about **19%** of the total amount of suspicious transaction reports filed pursuant to the Money Laundering Act and represents an increase of about 450% compared to 2005.

**Table 15: Reports filed in connection with "phishing" and "financial agents" (quarterly figures for 2006)**

	1 <sup>st</sup> quarter	2 <sup>nd</sup> quarter	3 <sup>rd</sup> quarter	4 <sup>th</sup> quarter	over-all total
Phishing	263	517	483	385	<b>1.648</b>
Financial Agents	6	9	53	197	<b>265</b>
<b>Total</b>	<b>269</b>	<b>526</b>	<b>536</b>	<b>582</b>	<b>1.913</b>

The number of suspicious transaction reports filed pursuant to the Money Laundering Act on pure "phishing" cases, that are basically not relevant under the "money laundering" aspect, decreased considerably in the course of 2006 as a result of appropriate information policy (inter alia the "indicator paper" published by the FIU in July 2006) <sup>8</sup>. The parties required to report – prejudiced parties have been asked to report these cases of fraud to the competent local law enforcement authority. The filing of a suspicious transaction report under the MLA should be refrained from in these cases. If there is, however, information suggesting the further disposition of illegal assets (e.g. receiving accounts), a suspicious transaction report pursuant to the Money Laundering Act should be filed since promising leads for investigations into money laundering are on hand then.

### Prognosis for the future

Assuming that both the number of online accounts (about 33.3 millions at the end of 2005)<sup>9</sup> as well as the number of Internet transactions will increase, opportunities for "phishing" and "financial agent" activities will increase just the same. Against this background, a further increase in the number of cases is to be expected for 2007.

Please see chapter 4 ("Follow-up responses by public prosecutors' offices pursuant to Section 11 (9) of the Money Laundering Act) for further comments on judgements, penalty orders and charges relating to cases involving "financial agents".

<sup>8</sup> For further information, see item 6.3.1.

<sup>9</sup> Deutsche Bundesbank, Statistics on payment transactions in Germany, 2001-2005, updated to October 2006.

### 3.4 Typologies

Acts of money laundering primarily aim at hiding illegally obtained assets from the law enforcement authorities and as or the state. In the end, the perpetrator wants to have assets at his disposal that are explicable and apparently legal and do not provide any leads to a criminal background. The following is a list of typologies describing specific or new concealment methods:

#### a) Online payment systems

According to a suspicious transaction report filed by a German bank, an East European female opened a savings account and has since been receiving transfers in the five-digit range under a reference name. The female passed on most of the money through a financial transfer service provider. The money came from an e-money institution domiciled in London which also acts as financial service provider under British law. An account can be opened there to which money can be transferred either by credit card or bank transfer and is changed to digital currency (e-money). Cash payments are not possible.

If money is paid in with a credit card, this card must first be registered in the customers profile at the e-money institution. Afterwards, the credit card is verified and the amount charged is automatically credited to the customer account.

Money can be transferred by e-mail through the e-money institution. All data are encoded and protected against unauthorised access. This ensures anonymity and data security. Everyone who receives money by e-mail merely has to register with the e-money institution. He or she then opens a free account to which the money transferred is credited in digital currency. Subsequently, the e-money can be changed to real money and can be transferred to an account held with another bank.

#### b) Bearer bonds

Transfers amounting to approximately four million euros were credited to sub-accounts of a German real estate company which, according to the stated purpose of transfer, were to be invested in bearer bonds<sup>10</sup>. The senders of the transfers suggested private investors. The large sums of money received were collected and subsequently transferred to an account in Dubai. Investments in bearer bonds have not been recognised here, however, funds from gang-type as well as commercial frauds were transferred abroad through sub-accounts.

<sup>10</sup>A bearer bond is a deed in which a service is promised to its holder. The issuer is only obliged to render the service against handover of the bond. The name of the owner is not mentioned on the deed which means that whoever physically holds the document is the creditor. Bearer bonds are, for example, federal bonds, corporate bonds and mortgage bonds.



### c) Payment cards

Suspicious transaction reports contained references to Internet offers in which agents offered “prepaid cards” that are to provide opportunities for making payment transactions without identification. These “prepaid cards” allegedly work like credit cards but on a credit balance basis only, i.e. they only allow for payment in line with the amount credited to the card account beforehand.

These prepayments can be made throughout the world in whatever amount or via reference accounts held with banks in offshore territories.

Cards can be applied for at the providers through online registration (identification of the customer is not made). The card itself is issued anonymously, a card can be linked to an account through the card number. Since the cards in question are based on VISA standards, they can be used like credit cards throughout the world for withdrawals at cash dispensers for example, for payment anywhere VISA cards are accepted or on the Internet.

By means of these anonymous payment cards, illegally acquired assets can be transferred to a (reference) account in offshore territories and can then be re-channelled into the legal economy again through these payment cards.

With a view to describing the potential of misuse of payment cards for money laundering activities and raising the awareness of all agencies concerned, the FIU has been conducting a special analysis on “Possible Money Laundering Activities in Connection with Payment Cards” since August 2006. The results are to be published in one of the next FIU Newsletters.

### 3.5 Assessment

All methods and typologies of money laundering that have been identified have been included in the catalogue “Money Laundering Indicators” (see item 6.3.1.) which serves the parties required to report as an orientation.

The cases, trends and typologies identified through the monitoring clearly show that classification of cases as suspicious is not possible exclusively on the basis of a rigid catalogue of grounds for suspicion. Therefore, the FIU wishes to emphasise that a catalogue of indicators or search matrices do not absolve the parties required to report pursuant to the Money Laundering Act of their obligation to examine and decide on each case individually. The respective risk and threat analysis on the basis of an assessment of the bank-specific customer segment and the range of products offered are crucial for deciding on the significance of individual indicators.

Feedback about money laundering methods and typologies is provided to those obligated by the Money Laundering Act through publication in the annual reports as well as by holding discussions on a case-by-case basis, presenting lectures at seminars and conferences of the reporting parties, providing information to the meeting of the Working Party of Banks and Chambers organised annually by the FIU, and publishing information in the FIU Newsletter.

## 4 Follow-up responses by public prosecutors' offices pursuant to Section 11 (9) of the Money Laundering Act

### 4.1 Introduction

In criminal proceedings instituted on the basis of a suspicious transaction report pursuant to Section 11 (1) of the Money Laundering Act, the competent public prosecutor's office is obliged by Section 11 (9) of the Money Laundering Act to inform the FIU at the Bundeskriminalamt about the bringing of charges and the outcome of the criminal proceedings as defined in Section 482 (2) of the Code of Criminal Procedure.

The follow-up responses by the public prosecutors' offices are collected within the FIU, are being recorded in a database and analysed in terms of statistics and contents with a view to

- better assessing the significance of suspicious transaction reports for criminal prosecution,
- assessing the forensic added value of suspicious transaction reports and
- initiating / taking measures for an optimisation of the response reporting practice of the public prosecutors' offices.

### 4.2 Statistical analysis

In 2006, **3,018** follow-up responses by public prosecutors' offices pursuant to Section 11 (9) of the Money Laundering Act were recorded. Compared to 2005, this means an increase by **80%**. Given the total amount of 10,051 suspicious transaction reports filed, the number of follow-up responses still needs to be optimised.

The following development of the response reporting practice of the prosecutors' offices – compared to the number of the reports filed pursuant to the Money Laundering Act – has been ascertained since 2003:

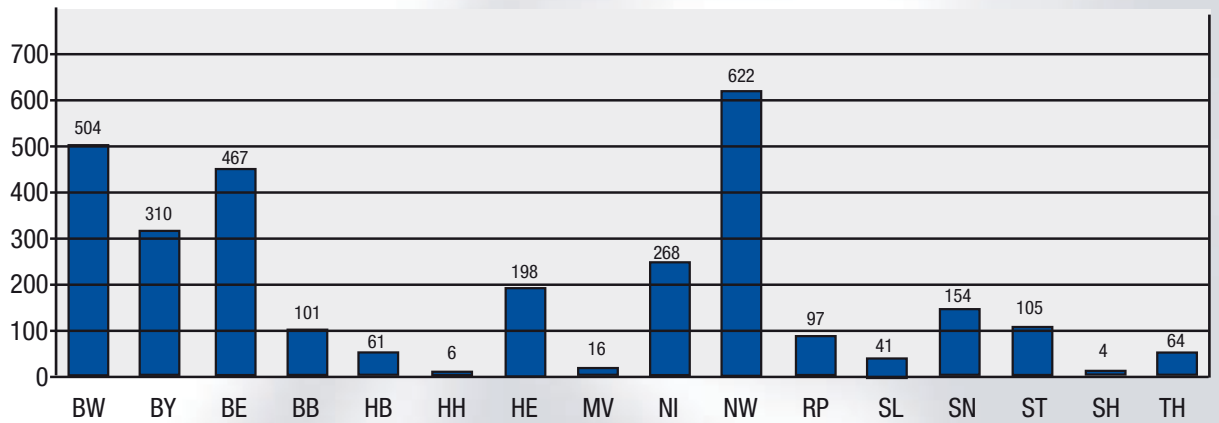
**Table 16: Follow-up responses pursuant to Section 11(9) of the Money Laundering Act (2003-2006)**

Year	Follow-up responses	suspicious transaction report	Difference
2003	13	6,017	6,004
2004	518	8,062	7,544
2005	1,680	8,241	6,561
2006	3,018	10,051	7,033

A direct comparison between the suspicious transaction reports filed during the calendar year and the follow-up responses received by the FIU cannot be easily made because the follow-up responses also refer to suspicious transaction reports filed in previous years, but due to insufficient information provided therein, cannot always be traced back. However, when the suspicious transaction reports filed under the Money Laundering Act are compared to the follow-up responses received over a period of four years, it can be summarised that no responses have been submitted to the FIU by the public prosecutors' offices for a considerable number of reports filed. Graph 4: Distribution of follow-up responses among the German states



**Graph 4: Distribution of follow-up response by German state**



As in the previous year, the federal states of Baden-Württemberg, North-Rhine Westphalia, Berlin and Bavaria are clearly at the top in respect of the number of follow-up responses from public prosecutors' offices pursuant to Section 11 (9) of the Money Laundering Act.

The considerable increase in the number of follow-up responses in the state of Hessen results from direct arrangements between the Frankfurt / Main Public Prosecutor General's Office and the FIU on the response reporting practice.

The FIU again received only a small number of follow-up responses from the German states of Hamburg and Schleswig-Holstein. This is due to the restrictive and narrow legal interpretation of Section 11 (9) of the Money Laundering Act in conjunction with Section 482 (2) of the Code of Criminal Procedure in conjunction with No. 11 (3) and No. 52 of the Directive on Reporting in Criminal Cases<sup>11</sup>. The German states of Hamburg and Schleswig-Holstein do not derive any reporting obligation for the public prosecutors' offices from the mentioned provisions.

This information gap makes well-founded statements on the significance of suspicious transactions reports for criminal prosecution and its forensic added value more difficult.

<sup>11</sup> Anordnung über Mitteilung in Strafsachen (Mistra).

With regard to the German states, the following trend has been observed for the last three years:

**Table 17: Follow-up responses pursuant to Section 11(9) of the Money Laundering Act – Comparison by year**

	Number 2004	Number 2005	Number 2006	Change from 2005
Baden-Württemberg	102	350	504	44.0%
Bavaria	36	296	310	4.7%
Berlin	128	292	467	59.9%
Brandenburg	69	42	101	140.0%
Bremen	4	30	61	103.0%
Hamburg	0	1	6	600.0%
Hessen	5	5	198	3960.0%
Mecklenburg-Western Pomerania	9	12	16	33.3%
Lower Saxony	24	91	268	194.5%
North Rhine-Westphalia	1	269	622	131.2%
Rheinland-Palatinate	63	86	97	12.8%
Saarland	16	22	41	86.4%
Saxony	24	96	154	60.4%
Saxony-Anhalt	29	54	105	94.4%
Schleswig-Holstein	1	2	4	100.0%
Thuringia	7	32	64	100.0%
<b>Total</b>	<b>518</b>	<b>1,680</b>	<b>3,018</b>	<b>79.6%</b>

This table shows a partly considerable absolute increase in the number of reported outcomes of proceedings for all German states. The following table shows the number of follow-up responses in relation to the suspicious transaction reports filed (pursuant to the Money Laundering Act) in the German states.

**Table 18: Comparison between "Number of suspicious transaction reports (STR) – number of follow-up responses"**

	2005			2006		
	STR	Follow-up-responses	%	STR	Follow-up-responses	%
BW	964	350	36.3	1,109	504	45.5
BY	1,696	296	17.5	2,164	310	14.3
BR	533	292	54.8	573	467	81.5
BB	128	42	32.8	198	101	51.0
HB	87	30	34.5	131	61	46.6
HH	361	1	0.3	420	6	1.4
HE	1,063	5	0.5	1,074	198	18.4
MV	89	12	13.5	98	16	16.3
NI	551	91	16.5	747	268	35.9
NW	1,775	269	15.2	2,142	622	29.0
RP	269	86	32.0	339	97	28.6
SL	65	22	33.9	91	41	45.1
SN	212	96	45.3	298	154	51.7
ST	108	54	50.0	171	105	61.4
SN	246	2	0.8	336	4	1.2
TH	94	32	34.0	160	64	40.0
<b>Total</b>	<b>8,241</b>	<b>1,680</b>	<b>20.4</b>	<b>10,051</b>	<b>3,018</b>	<b>30.0</b>

Although the comparison – as mentioned above – has to be interpreted with caution, a statement on some tendencies can be recognised: Considerable differences in the number of responses can be seen between the different German states, but an increase in the number of follow-up responses has been recorded for almost all of the German states.

### 4.3 Analysis of contents

#### 4.3.1 Follow-up responses not relevant to analysis

Of the 3,018 follow-up responses received in total, 2,616 (about 87%) were dismissal orders. In 2005, the rate of dismissals was about 77% only. This rise is mainly due to the considerable increase in follow-up responses received from the state of Hessen compared to the preceding year. 95% of them were dismissal orders.



The follow-up responses are divided as follows according to the decision taken:

- pursuant to Section 170 (2) of the Code of Criminal Procedure (insufficient suspicion) — 2,518
- pursuant to Section 154 (1) of the Code of Criminal Procedure (insignificant additional sanction) — 30
- pursuant to Section 153 (1) of the Code of Criminal Procedure (non-prosecution of petty offences) — 29
- pursuant to Section 205 of the Code of Criminal Procedure (discontinued provisionally) — 25
- pursuant to Section 152 (2) of the Code of Criminal Procedure (lacking initial suspicion) — 14

In most of the cases, dismissal orders pursuant to section 170 (2) of the Code of Criminal Procedure were issued without residual suspicion, 16 cases were dismissed with residual suspicion.

Dismissals pursuant to Section 154 (1) of the Code of Criminal Procedure were mainly explained by the fact that sentences for different offences were being anticipated so that penalties for the money laundering charges would have been of little significance.

Regarding the cases dismissed in accordance with Section 153 (1) of the Code of Criminal Procedure, the public prosecutors' offices considered the guilt of the perpetrator to be of a minor nature and did not see a public interest for prosecution.

Dismissals pursuant to Section 205 of the Code of Criminal Procedure concerned cases in which the proceedings had to be discontinued provisionally due to the anticipated absence of the accused (mostly due to a permanent stay abroad).

In 14 cases, the public prosecutors' offices – after appropriate examination – refrained from initiating proceedings due to lacking initial suspicion pursuant to Section 152 (2) of the Code of Criminal Procedure.

All the above-mentioned dismissals were not classified as being relevant to analysis since, apart from the reasons given on the basis of the Code of Criminal Procedure, no other significant information was provided.

The following table shows the absolute and percentage distribution of dismissals by German state. We wish to again point out that the numbers exclusively refer to the follow-up responses submitted to the FIU by the public prosecutors' offices and not to the absolute number of suspicious transaction reports filed.

**Table 19: Dismissal rates by German state**

	Total number of follow-up responses	Number of dismissals thereof	Dismissal rate
BW	504	470	93%
BY	310	230	74%
BE	467	384	82%
BB	101	81	80%
HB	61	59	97%
HH	6	2	67%
HE	198	189	95%
MV	16	14	88%
NI	268	237	88%
NW	622	527	85%
RP	97	94	97%
SL	41	34	83%
SN	154	141	92%
ST	105	93	89%
SH	4	1	25%
TH	64	60	94%
<b>Total</b>	<b>3,018</b>	<b>2,616</b>	<b>87%</b>

### 4.3.2 Follow-up responses relevant to analysis

In contrast to the 2,616 follow-up responses that are not relevant to analysis, 402 responses were classified as relevant to analysis, i.e. in connection with the investigations initiated on the basis of the suspicious transaction reports, either a bill of indictment, a penalty order or a judgement have been forwarded. In addition, cases have been included which resulted in the initiation of further investigations within the scope of the intelligence gathering process, or in which the suspicious transaction reports were integrated into ongoing investigations.

The 402 responses relevant to analysis have been classified as follows:

#### Judgements, bills of indictment and penalty orders

90 follow-up responses (22%) referred to an indictment, a penalty order or a judgement. 15 of them could not be assigned to specific transaction reports as the information provided was incomplete or the personal details had been deleted from the central FIU database due to the time limits on data storage. In 47 follow-up responses the persons reported acted as "financial agents". The other 43 indictments, penalty orders and judgements are classified as follows:

#### 22 indictments:

- eleven for fraud only
- five for money laundering only
- three for illegal organisation of games of chance
- one for money laundering coinciding with violation of the German Banking Act (KWG)
- one for currency counterfeiting
- one for tax evasion

#### 16 penalty orders:

- nine for fraud
- three for money laundering
- one for money laundering coinciding with violation of the German Banking Act (KWG)
- one for withholding of wages or salaries
- one for illegal organisation of games of chance
- one for false affirmation in lieu of an oath coinciding with aiding and abetting non-payment of contributions

#### Five judgements:

- two for money laundering
- one for violation of the Narcotic Drugs Act
- one for an embargo violation
- one for protection racketeering

#### Integration into pending proceedings

In 74 cases (18%), the information obtained in connection with proceedings initiated on the basis of a suspicious transaction report was integrated into pending investigative proceedings that had previously been initiated for another offence. Eight follow-up responses belonging to this group could not be assigned to the original suspicious transaction report.

#### Initiation of new proceedings

In 238 cases (60%), a new investigation was initiated on suspicion of other offences on the basis of the information obtained from the money laundering investigation. The investigation initiated on suspicion of money laundering was then discontinued pursuant to Section 170 (2) of the Code of Criminal Procedure. 28 follow-up responses belonging to this group could not be assigned to the original suspicious transaction report.

### 4.3.3 Reference to a certain type of crime

The following references to the various types of crime were revealed during the analysis of all follow-up responses by public prosecutors' offices which were relevant to analysis:

**Table 20: Types of crime mentioned in follow-up responses pursuant to Section 11 ( 9) of the Money Laundering Act**

Types of crime	Number
Fraud (also computer fraud, investment fraud, fraudulently obtaining services, breach of trust)	188
Money laundering (also in connection with violation of the Credit Act)	70
Tax offences	35
Document forgery (also in connection with fraud)	17
Insolvency offences	9
Illegal games of chance	7
Theft / misappropriation	5
Other	71
<b>Summe aller erkannten Deliktsbereiche</b>	<b>402</b>

If multiple offences were listed in the follow-up responses, the main type of crime was counted. The share of 47% of the follow-up responses classified as relevant to analysis again confirms for 2006 that cases based on (suspicion of ) fraud are often the subject of suspicious transaction reports filed pursuant to the Money Laundering Act. About 14% of these cases were classified as belonging to the "phishing" phenomenon (computer fraud). Actually, the percentage regarding the follow-up responses on "phishing" is probably much higher, however, the information contained in the follow-up responses by the public prosecutors' offices, is often not exact enough to allow a definitive assignment.

### 4.3.4 "Phishing" and / or activity as "Financial Agent"

A total of 180 follow-up responses by public prosecutors' offices has been assigned to suspicious transaction reports filed for "phishing" or activities as "financial agent". With regard to the 1,913 suspicious transaction reports filed in 2006 in connection with "phishing" and / or "financial agents" (see item 3.3), the number of follow-up responses received on this phenomenon appears to be low. However, the total number of dismissal orders regarding this phenomenon is not definitely quantifiable, as many of the follow-up responses by the public prosecutors' offices did not cite the reasons for dismissal.

In 16 cases, the investigations were in the end conducted for computer fraud (Section 263a of the Penal Code), in another 16 cases for money laundering or violation of the German Banking Act, or they were transferred to another competent agency.

Of the 90 indictments, penalty orders and judgements, the above-mentioned 47 exclusively concerned charges of illegal activities as "financial agents".

#### 12 indictments:

- five for money laundering only
- four for money laundering coinciding with violation of the German Banking Act (KWG)
- two for money laundering in connection with computer fraud



### 32 penalty orders:

- 19 for negligent money laundering
- six for money laundering coinciding with violation of the German Banking Act (KWG)
- three for computer fraud coinciding with violation of the German Banking Act (KWG)
- two for money laundering coinciding with computer fraud and violation of the German Banking Act (KWG)
- two exclusively for violation of the German Banking Act

The penalty orders involved fines between 300 and 3,800 euros.

### Three judgements:

- two passed for negligent money laundering (prison sentences of six months suspended on probation as well as a fine)
- one for money laundering in connection with document forgery (fine)

### Assessment:

The analysis of the judgements, indictments and penalty orders shows that the "financial agents" involved are accused of having been aware of or having at least wilfully accepted that the monies transferred were illegal assets – especially in view of the fact that the "phishing" phenomenon linked with the recruitment of "financial agents" has meanwhile received broad media coverage. The courts and public prosecutors' offices mainly found that the person involved should have recognised from the overall circumstances that the (job) offers cannot be serious.

Besides, some courts and public prosecutors' offices regarded these activities as violation of the German Banking Act. The transfer of funds is a financial transaction that also laymen can easily recognise as a classical task of banks or licensed financial transfer service providers. The accused should have recognised a private individuals that any such financial transaction must not be conducted without authorisation. If in doubt, they could or should have enquired with the BaFin with a view to clarifying authorisation issues.

For this reason, several courts found that activities as "financial agents" are illegal financial transactions pursuant to Section 54 subsection 1 (2) and subsection 2 in conjunction with Section 32 subsection 1 and Section 1 subsection 1a (6) of the German Banking Act and the BaFin initiated administrative proceedings against some of the individuals identified as "financial agents".

It can be seen from the partly different reasons given for the judgements that the law enforcement authorities and the courts do not yet have a standardised legal opinion with regard to the criminally relevant behaviour of "financial agents". "Financial agents" who make their accounts available for financial transactions must always face fines or prison sentences. In addition, "financial agents" have to expect civil law claims by the prejudiced parties or banks for re-payment of the money transferred (passed on) illegally.

#### 4.4 Use of the form "Reporting pursuant to Section 11 (9) of the Money Laundering Act, Sections 482 and 475 of the Code of Criminal Procedure"

The FIU published an optimised form for follow-up responses pursuant to Section 11 (9) of the Money Laundering Act in its Annual Report for 2005. In a joint letter of the Federal Ministry of the Interior and the Federal Ministry of Justice, sent to the state justice departments in March 2006, it was suggested to use this form "Reporting pursuant to Section 11(9) of the Money Laundering Act, Sections 482 and 475 of

the Code of Criminal Procedure” with a view to simplifying and standardising procedures.

Of the 3,018 follow-up responses submitted in 2006, the respective form was used in four cases only. Some public prosecutors’ offices used individually developed forms which vary considerably not only from one state to another but also from public prosecutor’s office to public prosecutor’s office within the individual German states.

The follow-up reports which were not good enough for analysis or could not be assigned to specific suspicious transaction reports showed that they regularly did not contain the information required for adequate recording or content-related analysis. For example, when dismissal orders were passed for suspected money laundering, information was lacking as to whether investigations were continued by another public prosecutor’s office for other offences. So far, only a very small number of follow-up responses on the results of such follow-up proceedings were transmitted to the FIU by the then competent public prosecutors’ offices.

According to some of the public prosecutors’ offices that were approached and asked about the potential for optimisation of the follow-up responses, the following aspects are, inter alia, considered a hindrance to a comprehensive response on the basis of the sample form, despite their understanding for the FIU’s task handling:

- The guiding principle is not the FIU’s need for information but only the statutory obligation (Section 11 (9) of the Money Laundering Act in conjunction with Section 482 (2) of the Code of Criminal Procedure).
- The public prosecutors’ offices’ heavy workload / overload
- Data protection-related restrictions when transmitting personal details

The form was already designed in a way that the follow-up responses can be used not only for informing the FIU about the outcome of proceedings but also for informing the reporting party (pursuant to Section 475 of the Code of Criminal Procedure) and the police authority involved (pursuant to Section 482 of the Code of Criminal Procedure). Above all the parties required to report pursuant to the Money Laundering Act have vividly criticised for years that they rarely receive case-specific follow-up responses from the public prosecutors’ offices although this would be of great importance for the continuous adjustment of the monitoring and research systems in use and consequently for the improvement of the reporting behaviour.

#### 4.5 Summary and Outlook

The increase in the number of follow-up responses pursuant to Section 11 (9) of the Money Laundering Act by approximately 80% is seen as a positive development. The FIU took extensive measures in 2005 and 2006 with a view to improving the response reporting practice of the public prosecutors’ offices. The considerable increase reached as a result of the measures taken to raise the involved parties’ awareness facilitated a more detailed and more conclusive analysis.

The quality of the follow-up responses has improved as well. There is, however, potential for optimisation regarding the completeness of the data. In 2007 as well, the FIU will approach the public prosecutors’ offices concerned with a view to further optimising the response reporting practice in respect of quality and quantity. The use of the standardised response form plays an important role in this regard. In 2006, the use of this form unfortunately did not find general acceptance.



## 5 Financing of terrorism

### 5.1 General remarks

With the amendment of the Money Laundering Act in August 2002 and the incorporation of reporting obligations in cases of suspected "financing of terrorism", suspicious transaction reports pursuant to the Money Laundering Act in the field of police state security proved to be successful as an important instrument for the suppression of international terrorism. Although a decrease is recorded for the reporting year 2006, the information gleaned from the suspicious transaction reports represent valuable leads for the suppression of international terrorism. Within the framework of the police clearing process and investigations initiated by public prosecutors' offices, they provide insights into personal relationships and other structures that could not have been gained without such reports. On the basis of the suspicious transaction reports it is also possible to trace and locate suspects potentially linked to state security-related cases.

The suspicious transaction reports filed pursuant to the Money Laundering Act are checked by the state criminal police offices for any relevance to state security matters and, if any such references have been revealed, are forwarded to the State Security Division of the Bundeskriminalamt which has the function of a central office and therefore receives the reports for analysis purposes and identifying possible typologies. One of the results is the "Indicator Paper" (see item 6.3.1), prepared in 2006, which contains criteria suggesting the financing of terrorism in the field of politically motivated crimes committed by foreign nationals.

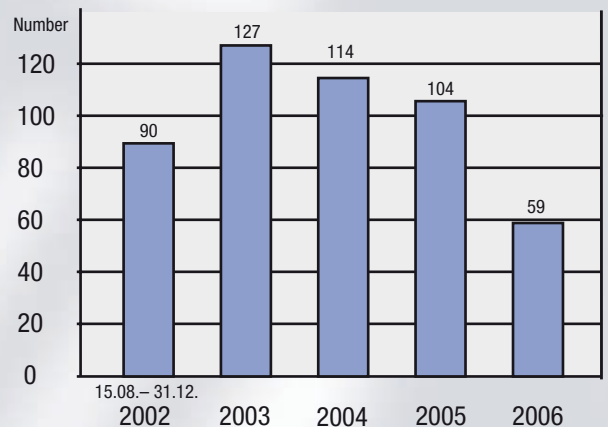
The FIU supports efforts to collect financial information of relevance to national security from the relevant agencies at national and international level. The FIU obtains this information from suspicious transaction reports filed pursuant to the Money Laundering Act and through correspondence exchanged with other FIUs.

### 5.2 The national situation

#### 5.2.1 Quantitative development of suspicious transaction reports pursuant to the Money Laundering Act relating to the financing of terrorism

The following statistics comprise suspicious transaction reports filed by the reporting parties on suspicion of financing of terrorism. Compared to the previous year, the number of suspicious transaction reports dropped to 59 from 104.

Graph 5: Suspicious transaction reports indicating suspected involvement in the financing of terrorism



On the whole, a decline in the number of suspicious transaction reports regarding suspected involvement in the financing of terrorism to 59 in 2006 from 127 in 2003 has been recorded since the enactment of Section 11 (1) sentence 2 of the Money Laundering Act in August 2002.

Table 21: Statistical distribution of suspicious transaction reports relating to the “financing of terrorism”

	15.08.- 31.12.02	2003	2004	2005	2006
<b>Total number of suspicious transaction reports (STRs) Filed pursuant to the Money Laundering Act (MLA)</b>	2,271	6,602	8,062	8,241	<b>10,051</b>
<b>STRs checked by the State Security Section at the BKA (statistically recorded for the first time in 2005)</b>	---	---	---	358	<b>376</b>
				4.3%	<b>3.7%</b>
<b>Total number of STRs filed by parties required to report indicating suspected involvement in the financing of terrorism</b>	90	127	114	104	<b>59</b>
Percentage of total number of STRs	4%	2%	1.4%	1.3%	<b>0.6%</b>
<b>Cases with (suspected) list match</b>	49	83	68	58	<b>21</b>
Percentage of STRs indicating suspected involvement in the financing of terrorism	54.4%	65.4%	59.6%	55.7%	<b>35.6%</b>
Percentage of total number of STRs	2.2%	1.3%	0.8%	0.7%	<b>0.2%</b>
<b>Cases without list match (other cases)</b>	41	44	46	46	<b>38</b>
Percentage of STRs indicating suspected involvement in the financing of terrorism	45.6%	34.6%	40.4%	44.3%	<b>64.4%</b>
Percentage of total number of STRs	1.8%	0.7%	0.6%	0.6%	<b>0.4%</b>

Of the 59 suspicious transaction reports indicating suspected involvement in the financing of terrorism submitted in 2006, 21 reports were filed on the grounds of possible matches with embargo lists issued by the UN and the EU (EU Regulations No. 881/2002 and No. 2580/2001)<sup>12</sup>. No match with listed persons was found.

The remaining 38 reports filed cited other grounds for suspicion, such as unusual account transactions or transaction amounts or other suspicious behaviour. This reflects a decrease of 17% compared to the previous year.

The decrease in the number of reports filed for suspected financing of terrorism is therefore mainly based on the smaller number of reports filed in respect of possible list matches.

In calendar year 2006, the FIU received only nine follow-up responses by public prosecutors' offices pursuant to Section 11 (9) of the Money Laundering Act as compared with the 59 suspicious transaction reports in total filed under the Money Laundering Act for suspected financing of terrorism. The respective investigations were discontinued for lack of sufficient suspicion pursuant to Section 170 (2) of the Code of Criminal Procedure. The Bundeskriminalamt did not receive any follow-up responses on the outcome of the other 50 cases. In 2006, the State Security Division at the Bundeskriminalamt reviewed 376 requests for information from state criminal police offices based on suspicious transaction reports in cases in which possible involvement in the financing of terrorism could not be excluded. In 51 cases, this involvement was confirmed. Eight of these cases were based on suspicious transaction reports pursuant to the Money Laundering Act relating to the “financing of terrorism”.

<sup>12</sup>With the support of the State Security Division of the Bundeskriminalamt, the FIU compiled information on the procedures and the legal consequences in case of a match and published this information in its 4th Newsletter for use of the parties required to report.



This shows the importance of suspicious transaction reports for the suppression of international terrorism, evident in the following example:

**Case:**

Two suspicious transaction reports were filed by a party required to report since the recipient of the money was an organisation listed in EU regulation No. 881/2002. Initial investigations brought to light that only part of this organisation is listed in country A. The investigation initiated by the competent public prosecutor's office on the basis of the two suspicious transaction reports was discontinued pursuant to Section 182 (2) of the Code of Criminal Procedure. A new investigation was initiated on suspicion of violation of Section 129 of the German Penal Code (formation of a terrorist organisation). The investigations are still in progress.

### 5.2.2 Quality of suspicious transaction reports pursuant to the Money Laundering Act relating to the financing of terrorism

As in previous years, the number of reports with possible matches between the relevant lists and the individual or organisation in question has declined, the increasing knowledge among the parties required to report about the fact that only the EU regulations No. 881/2002 and 2580/2001 are legally binding in Germany could be the reason for this decrease.

The fact that leads suggesting possible matches with the OFAC List<sup>13</sup> have become increasingly rare confirms of this assumption.

In addition, more routine in handling cases concerning possible list matches could be the reason for the sharp drop in this year's figures.

<sup>13</sup> List issued by the U.S. Department of the Treasury - Office of Foreign Assets Control.

The difficulties that parties required to report have experienced in an effort to identify potential involvement in terrorism on the basis of observations of account activity and transactions alone, as described in the previous FIU Annual Reports, continue to exist.

The analysis of all suspicious transaction reports for cases with relevance to state security also provides an insight into the financing of terrorism phenomenon. The fact that reports are filed for suspected involvement in "financing of terrorism" suggests a basic awareness of this phenomenon. In addition, the reporting behaviour exhibited in 2006 documents is the basic functional viability of the monitoring systems. This is exemplified by the following suspicious transaction reports:

**Case:**

A financial transfer service provider filed a suspicious transaction report pursuant to the Money Laundering Act concerning a German national of Lebanese origin because the economic background of considerable payments to and from the Middle East and Sub-Saharan Africa could not be explained. The person reported, who, according to police information, is a Hizballah supporter, was mentioned in another suspicious transaction report filed by a different party in connection with a real estate business.

This case proves that individual suspicious transaction reports also offer possible investigative leads in respect of other economic activities of a person recorded under the state security aspect.





**Case:**

A computer search yielded a standing order that a customer had placed several years ago in favour of the Al Aqsa e.V. association. A suspicious transaction report was filed thereupon. The Al Aqsa e.V. association was banned by the Federal Ministry of the Interior, following final confirmation by the Federal Administrative Court on December 3<sup>rd</sup> 2004, for its links to the terrorist organisation Hamas.

The following is another example that documents the awareness of the parties required to report, also in view of cases involving the suspicion of financing of terrorism.

**Case:**

A case relating to suspected terrorist financing was revealed through a suspicious transaction report in connection with an association whose objective, besides charity work, was also the furthering of religion. Considerable donations were received in the association's account from country A, part of which were transferred to a German limited liability company and from there onward to an account in country B. The security authorities in country A enquired about the association and its executive officers in connection with police investigations. Information was obtained that this association is not only registered in Germany but also active in country A. The investigations in Germany and in country A are still in progress, so it remains to be seen whether the suspicion of terrorist financing will be corroborated.

### 5.2.3 Preparation of an indicator paper

With the amendments to the Money Laundering Act that came into effect in 2002, "suspected financing of terrorism" was included in Section 11 of the Money Laundering Act as reporting obligation for institutions.

The catalogue of "indicators of the financing of terrorism in the field of politically motivated crimes committed by foreign nationals", which was prepared on the basis of the experience gathered by the security authorities, was provided to the parties concerned after agreement with the competent national authorities such as the Federal Ministry of the Interior, the Customs Criminal Investigation Office, the Federal Agency for Supervision of the Financial Services Sector as well as bodies of the credit sector, with a view to using it for research and monitoring.

The suspicious transaction reports filed pursuant to the Money Laundering Act in the second half of 2006 do not show a significant change in the reporting behaviour of the parties required to report. Thus, the list of indicators supplemented by the terrorist financing criteria seems to have had little effect so far. It is believed, however, that introduction and use of the indicators have not yet been implemented by all parties required to report under the Money Laundering Act throughout Germany.

It should not be disregarded in this context that the formulation of indicators is very difficult due to the manifold ways of acquiring money, depending on many aspects, and that they are close to the previous money laundering indicators.

Experience shows that attacks can be committed with limited financial means and from legal sources. It was impossible so far to identify the financial transfers required for this purpose on the basis of the existing criteria. The parties required to report should therefore show particular awareness here.



The problems in recognising terrorist financing that are encountered all over the world repeatedly show the importance of detailed information on the personal situation of the account holder as well as the person transferring the funds so that a suspicion can be generated taking all indicators into account. Thus, the "know your customer" (KYC) principle will always play by far the most important role combating the financing of terrorism.

The following case is described as an example:

**Case:**

Two almost simultaneous cash deposits made by two different persons at a branch of a German bank for transfer to an account held with a foreign bank in Vienna, attracted the attention of the law enforcement authorities only because both deposit slips showed the same script. According to the competent clearing office, the two individuals had not been properly identified. However, it was found out that one of the persons who made the deposits is a PKK activist.

This case clearly shows that relevant persons could have been identified at an early stage and that suspicious transaction reports could have been filed if the KYC principle had been applied and due identification had been made. For the above-mentioned reasons, the development and adjustment of suitable indicators will continue to be an important issue for national and international bodies suppressing the financing of terrorism. The FIU will ensure that the indicators are permanently adjusted to the current situation, supported by the authorities specialised in the suppression of terrorism.

#### **5.2.4 Current trends concerning measures relating to the freezing of assets pursuant to EU regulations No. 2580/2001 and No. 881/2002**

In general, the UN / EU sanction lists with the related measures are a suitable means for suppressing the financing of terrorism. The measures adopted under international law inter alia aim at freezing the financial resources of the person listed. The efforts made to obtain full personal details on persons to be listed in order to achieve clear identification contribute to the success of this measure.

In its ruling dated 12 December 2006 on the listing of the People's Modjahedin-E-Khalq (MEK) the European Court of Justice found that defence rights, the obligation to give reasons and the right to effective legal protection, had been violated.

The ruling says that no sufficient reasons for initial or follow-up decisions regarding the listing had been given. The offences they are charged with had not been sufficiently communicated to the People's Modjahedin prior to the indictment. Due to the insufficient stating of reasons, the plaintiffs were unable to properly take action before the court. The court has not made a substantive decision on the legitimacy of the MEK listing. The court also saw the necessity to improve the "listing" and "de-listing" procedures. The ruling of the European Court of Justice obliged the European bodies to develop and implement these procedures in line with the criteria formulated by the court. This has been done in the respective Council decision dated 28 June 2007.

## 5.3 The international situation

### 5.3.1 FIU correspondence

At international level, the FIU Germany plays a co-ordinating role with regard to requests for information from and to foreign FIUs, thereby supporting national and international authorities in an effort to combat the financing of terrorism. Of the 718 cases in which the FIU exchanged correspondence, 427 were subjected to more thorough checks by the State Security Division of the Bundeskriminalamt.<sup>14</sup> In 38 cases, a reference to state security was established, seven enquiries were confirmed as relevant.

The comparatively small number of cases relating to state security matters is believed to be due to the fact that most of the foreign FIUs are not attached to the law enforcement authorities and their assessment of cases under state-security aspects is probably much more difficult.

#### Case:

A foreign FIU enquired about several individuals listed in EU sanction list No. 881/2002 and detained in Germany. The purpose of the enquiry was to receive further information to that already available and to be informed of possible links of the individuals to the requesting country. The requested information has indeed been passed on to the foreign FIU.

#### Case:

A foreign FIU enquired about a German company that had come to notice in the past as a supplier of radio-active test sources to countries outside Europe. The initially presumed state-security links have been ruled out. This case, however, proves that also in this very sensitive

field of trading in radioactive substances and technology, especially in view of its current political importance in the world, suspicious transaction reports are a feasible tool for reconstructing economic operations that could also be of state-security relevance.

#### Case:

In connection with a request for information on suspicious financial transactions carried out by a German national, it was established that this person had already come to notice to the German security authorities for his contacts with the Al Qaeda command structure. Due to this enquiry, this person's current whereabouts and the corresponding contacts have been revealed. Although this person was not a terrorist, the enquiry proves that potential perpetrators can be quickly located and linked to contact persons.

Through the exchange of information among international FIUs, information of relevance to state security can be acquired which, in the interest of a comprehensive case research, can have a considerable added value for investigations conducted in Germany.

In the field of combating the financing of terrorism, the FIU Germany performs an important co-ordinating function by enriching information by police intelligence on a timely basis, evaluating such information and – to the extent legally permissible – forwarding it to the relevant agencies. In this sense, the global alliance of FIUs also facilitates efficient and timely co-operation with foreign corresponding agencies.

<sup>14</sup>The forwarding of enquiries received from abroad to our State Security Division is not possible when the requesting FIU has not given its consent to the release of the information. The 718 cases of correspondence also comprise enquiries from national law enforcement authorities in which checks relating to state security information can be made or initiated by the requesting national authority itself.

### 5.3.2 EU study – state of implementation of the nine FATF special recommendations

As early as in late 2004 already, the EU Commission had decided, in connection with the "EU Counter Terrorist Financing Strategy", to conduct a study on the state of implementation of the nine special recommendations of the Financial Action Task Force (FATF) in the individual EU member states. The EU commission commenced the announced assessment in 2006. The collection and analysis of data is made by external experts tasked by the Commission.

In order to establish the state of implementation in Germany, EU experts conducted an interview in August 2006 with representatives of the Federal Ministry of the Interior, the Federal Ministry of Finance, the Federal Agency for Supervision of the Financial Services Sector and the Bundeskriminalamt.

The *nine special recommendations* implemented after 11 September 2001 are based on the experience gained from the financial investigations conducted in the member states in connection with the suppression of the financing of terrorism. They contain guidelines, control mechanisms and procedures that are to ensure a uniform concept and joint and effective action in the FATF member states.

In Germany, these special recommendations have been fully implemented by both EU regulations that are legally binding as well as the introduction of legal provisions, inter alia in the Money Laundering Act.

### 5.3.3 Typologies

Within the context of international co-operation, information and practical experience gained from cases involving the use of the financial sector to finance terrorist activity is exchanged, assessed on the basis of characteristic indicators of the use of the financial sector for the purposes of terrorism and summarised in the form of typologies. At national level, this was inter alia implemented in the above-mentioned indicator paper.

The State Security Division at the BKA plays an active role in the described national and international typology work by collecting and analysing information from the relevant criminal investigations and comparing it with current international trends.

In this context, the question of how terrorists generate, transfer and finally use the financial resources they need, was discussed on the basis of concrete case studies during the last FATF typology meeting in Shanghai in November 2006.

The variety of different financing sources and possibilities of transaction renders the preparation of a practicable list of indicators for early detection of terrorist financing difficult.

The case examples presented during the meeting therefore show the necessity and importance of intensive and constructive co-operation between the national FIU and the respective national private sector (banks, financial transfer service providers, insurance companies etc.). According to the reports presented by the participants, the co-operation between the parties required to report pursuant to the Money Laundering Act and the FIU Germany is functioning well.

An international list of *indicators for early detection of the financing of terrorism*, to be prepared by the FATF, has been announced for the next meetings.

## 5.4 Summary and Outlook

Since August 2002, suspicious transaction reports pursuant to the Money Laundering Act have been filed and analysed also under the aspect of the possible financing of terrorist activities and violent crimes. This has proved to be an effective instrument especially from the viewpoint of a holistic approach to the suppression of international terrorism.

Although the percentage of suspicious transaction reports filed pursuant to the Money Laundering Act and relevant to state security is very small in relation to the total number of suspicious transaction reports, the investigative leads and structural information gained on terrorist organisations are considered advantageous for the German security authorities.

The fact alone that 51 suspicious transaction reports with references to politically motivated crime were filtered out shows the complementary significance of the instrument of suspicious transaction reports filed under the Money Laundering Act for combating the financing of terrorism. The investigations and analyses made in these cases as well as the resulting new structural information and modi operandi used by terrorists form an important and useful part in this field.



## 6 National co-operation

### 6.1 The FIU as central office

In Germany, a large number of agencies are involved in the suppression of money laundering and the financing of terrorism. The following parties are mentioned as examples here:

Investigation authorities of the Federation and the states (especially the joint financial investigation teams of the police and the customs at the Bundeskriminalamt and the state criminal police offices), the public prosecutors' offices, the customs and financial authorities (such as the tax investigation services), other security authorities (such as the Federal Intelligence Office, the Federal Office and the state offices for the Protection of the Constitution, regulatory authorities (such as the Federal Association of Public Banks in Germany), professional associations (e.g. for accountants, lawyers and tax advisors), umbrella organisations (such as the Union of German Insurance Companies, the Central Credit Committee), the parties required to report under the Money Laundering Act (in particular all institutions as defined in Section 1 (4) of the Money Laundering Act and all business sectors mentioned in Section 3 (1) of the Money Laundering Act), all companies engaged in the prevention of money laundering, providers of special research and monitoring software, training and further training institutions, research institutions (such as Max-Planck-Institute), commissioned business consultants and Ministries of the Federation and the states (above all home affairs, finance and justice).

The Central Office for Suspicious Transaction Reports at the BKA is in contact with all the above-mentioned agencies and often acts as contact in connection with change processes and / or their initiation or optimisation measures for suppressing the phenomena of money laundering and financing of terrorism. On the one hand, this position results from its competence as national central unit for suspicious

transaction reports and, on the other hand, from its role as contact for foreign FIUs. Consequently, international efforts and trends both with respect to the permanently changing offender behaviour and initiatives relating to international suppression strategies can be incorporated in national developments.

The following measures taken by the FIU during the 2006 reporting year are mentioned as examples for its efforts to constantly develop its competence:

**FIU staff members attended on-the-job training** in compliance sections of banks and with security authorities in order to learn about the processes and problems in the handling of the respective tasks and to include this experience in the work of the FIU. Naturally, this has helped to establish or improve personal contacts with important reporting parties and the security authorities.

In addition, at a large number of the above-mentioned parties, FIU staff members held **lectures** on the responsibilities, processes, legal aspects, problem fields, as well as chances and limits when combating money laundering and financing of terrorism. In connection with their activities, the lecturers of the Central Office for Suspicious Transaction Reports were often approached with questions or problems by the participants. This led to an insight into current public opinion on the one hand and the identification of weak points on the other hand.

The Central Office for Suspicious Transaction Reports also offers a **telephone hotline** for special questions by national and international agencies engaged in the prevention and suppression of money laundering and the financing of terrorism.

The following problems are described below as examples which have been recognised by the FIU and conveyed to the competent authorities:<sup>15</sup>

- Under what conditions can accounts be kept active for tactical reasons during the covert investigation stage although a suspicious transaction report has been filed and the account is to be closed?
- Do the offences on which the investigation is based have to be explicitly stated in requests for information on and release of account data?

In carrying out its task as central office and contact for all questions involving the suppression and prevention of money laundering, the FIU welcomes – like in the past – an open and constructive dialogue which is to be continued with all agencies involved.

The following are some outstanding measures taken by the Central Unit for Suspicious Transaction Reports as well as examples of the co-operation with agencies that are significantly engaged in the suppression of money laundering and the financing of terrorism.

## 6.2 National investigative agencies

### Co-operation at the operational level

In their function as clearing offices for suspicious transaction reports, the Joint Police as Customs Financial Investigation Groups of the state criminal police offices as well as the state security agencies and the tax investigation offices (in respect of reports filed pursuant to Section 31b of the Fiscal Code) are the main co-operation partners of the FIU. In 2006 again, co-operation in the field of information exchange with foreign FIUs was a focal point of co-operation with the national investigative authorities. This information exchange is also conducted for other local investigative authorities (police, prosecutors, customs etc.) in cases in which they have a need to know as the investigative agencies with original jurisdiction.

Prior to making an enquiry abroad, the FIU routinely makes initial checks on the facts submitted in order to be able to give advice to the national investigative authorities in respect of an optimal procedure. In this context, the following aspects are, inter alia, important:

- Checks on whether the information required can be obtained from the foreign FIU at all or whether a different authority (e.g. Interpol) in the country concerned should be addressed.
- Consideration of the legal provisions valid in the country from which the information is needed: For what offences have the national proceedings been initiated? Are these offences punishable as a predicate offence of money laundering under the corresponding foreign laws? Tax evasion, for example, is not a predicate offence of money laundering in all countries.

<sup>15</sup>Note: The examples only serve to make clear the kind of issues discussed with the FIU. Thus, the FIU refrains from replying to the questions in its Annual Report.



The successful work of the FIU Germany as a national central office was evident in 2006 in a substantial number of cases in which pending investigations in the individual German states were enriched with valuable information or new investigations were initiated in Germany on the basis of information obtained from foreign FIUs. In this context, the advantage of the German police FIU as a "bridgehead", especially between the (primarily) administrative FIUs abroad and police agencies in Germany, was clearly demonstrated once again.

In response to requests for information both to and from foreign FIUs, it was possible to initiate measures such as seizures of assets or to combine investigative complexes for the national investigative agencies within a very short period of time.

The FIU Germany processed a larger number of cases in which individuals of political, economic or social prominence were involved and which therefore required a high level of sensitivity. In many of these cases, it was determined that information from the financial sector obtained from foreign sources had not been transmitted through other information channels and was therefore not available to national investigative agencies.

The role of the FIU as an information "broker" for national investigative agencies is outlined below in the description of a case that attracted extraordinary (media) interest:

**Case:**

An insolvent valuables transport company had embezzled customer funds for years and transferred a part of them abroad and misused them for its own interests. Due to the large customer base, the withdrawal of customer funds was not noticed at first since it was compensated by the daily receipts from other customers. The outstanding receivables finally totalled a three-digit million amount. The competent investigative authorities asked the FIU Germany for assistance in order to establish where the funds coming from this complex had gone. 43 FIUs throughout the world were contacted and seven of them held information relevant to the case. As a result, assets in the medium single-digit million range have been recovered abroad by way of legal assistance requests.

This case underscores the added value generated for the national investigative authorities by the involvement of the FIU.





### Co-operation at the strategic level

In 2006, in addition to operational information, the FIU also conveyed the results of strategic analysis to the national investigative authorities. Important products for the work of the FIU were inter alia posted in a secure police information portal to which national investigative authorities have access.

Especially the Joint Police as Customs Financial Investigation Groups at the state criminal police offices and at the Bundeskriminalamt were again actively involved in the working areas of the FIU in the 2006 reporting year. Worthy of note in this context, for example, is their participation

- in the FIU's bank and professional associations group,
- in updating as well as preparing the *Indicator Paper on Money Laundering and the Financing of Terrorism* and
- in compiling the procedures for filing reports pursuant to Section 31b of the Fiscal Code.

The FIU also provided support to national investigative authorities (police, customs, tax investigation offices etc.) in the form of presentations at special courses and at conferences in the field of financial investigation.

### 6.3 Parties required to report pursuant to the Money Laundering Act

The co-operation between the parties required to report under the Money Laundering Act and the FIU, set up in 2002, is functioning well now. The FIU is often routinely contacted as central office for money laundering-specific problems or for clarifying details.

The most important examples of co-operation with parties required to report pursuant to the Money Laundering Act in 2006 are described in greater detail in the following sections.

#### 6.3.1 The FIU's new catalogue of indicators

The FIU Germany elaborated an up-dated indicator paper for the banks, financial service providers and insurance companies required to file suspicious transaction reports pursuant to the Money Laundering Act, .

This indicator paper was published in the password-secure section of the FIU on the BKA website in July 2006 and was also published in an FIU Newsletter. The BaFin distributed this Newsletter to all agencies concerned in Circular 07 2006 – GW on August 2<sup>nd</sup> 2006.

In addition to the indicators of money laundering, a catalogue of indicators suggesting financing of terrorism in the field of politically motivated crimes committed by foreign nationals was prepared on the basis of information provided by the state security units at the state criminal police offices and the Customs Criminal Investigation Office in co-operation with the State Security Division of the BKA.

This indicator paper is intended to serve the parties required to report as a tool for recognising cases of relevance to money laundering and possible involvement in the financing of terrorism. When stating the reasons for filing a suspicious transaction report, reference was and is sometimes made to the relevant indicators published.



The primary purpose of the catalogue is to heighten awareness among the groups of reporting parties cited above. It was not intended to prepare an exhaustive (check) list of relevant indicators which is neither feasible nor would reflect the constantly changing realities. Those required to report will remain obliged to review each case individually when taking decisions regarding the filing of a suspicious transaction report.

Besides, the indicator paper prepared by the FIU specifically for the occupational groups specified in Section 3 (1), No. 1 and 2 of the Money Laundering Act ("new parties required to report") remains to be valid. It has also been included in the 3<sup>rd</sup> Newsletter with a view to completely presenting all indicator papers prepared by the FIU.

The new indicator paper does not contain descriptions of exemplary cases. These descriptions are published regularly in the Newsletters as products of the FIU's case collection activity. In February 2007 for example, the FIU published several cases in its 4<sup>th</sup> Newsletter which in addition to the indicators reflect current problems as well as typologies.

A large number of agencies involved in the suppression of money laundering contributed to the process of compiling this indicator paper by providing constructive suggestions and thus helped prepare a paper that is fit for practical use. Despite partly heterogeneous interests and expectations, almost all aspects have been included in the indicator paper or acceptable compromises have been found.

The entities involved in this process were, inter alia, the state criminal police offices, the Central Office of the German Customs Investigation Service, the Federal Agency for Supervision of the Financial Services Sector (BaFin), the Central Credit Committee and its affiliated associations, the Union of German Insurance Companies, as well as some banks and credit institutions.

### 6.3.2 The FIU Newsletter

In a timely manner, the FIU Newsletter informs all parties required to report pursuant to the Money Laundering Act about current developments in the field of suppression of money laundering and thus contributes to a progressive optimisation of task handling. The expectations attached to the Newsletter to support further improvement in communication between the FIU and the parties required to report have been fulfilled.

Since April 2005, four FIU Newsletters have been published in the password-secure section of the BKA's website. While the 3<sup>rd</sup> Newsletter, published in July 2006, exclusively dealt with the indicator paper, cases with specific *modi operandi* of money laundering and suspected cases of financing of terrorism were additionally described in the 4<sup>th</sup> Newsletter. Furthermore, information is provided on the current legal situation and the procedures that have to be applied by the parties required to report if a hit is received on suspected terrorist financing following an identified match with persons and companies on the EU sanction lists.

### 6.3.3 The Conference of Banks and Professional Associations

In June 2006, the FIU hosted the annual conference of representatives of bank associations, professional associations, money laundering experts from major German banks, the state criminal police offices, the Central Office of the Customs Investigation Service and other experts of the BKA. The conference focused on the following subjects:

- Key figures of the FIU's 2005 Annual Report
- New methods of money laundering and current trends
- Current status of the "electronic suspicious transaction report" (eVA) project with a presentation of the technical concept
- Current status of the *Catalogue of Indicators of money laundering and financing of terrorism*

The following topics were also discussed:

- Presentation of the re-orientation of the monitoring of suspicious transaction reports implemented at the beginning of 2006
- Detailed statements on the trend monitoring conducted by the FIU in 2006 (e.g. "phishing", "FIFA World Cup 2006", "Internet auctions", "financial agents")
- Transmission of account details in electronic form in reply to requests for information by public prosecutors' offices
- Problems and procedures involving matches with EU sanction lists in respect of suspected financing of terrorism

According to the participants, this conference has proved its value as a platform for the mutual exchange of information and experience by banks, banking associations, professional associations and law enforcement authorities. Some of the participants also expressed their wish for an even more intensive information exchange in this circle.



### 6.3.4 "Other business persons"

Under the Money Laundering Act (Section 3 (1) sentence 2), "other business persons" are those who carry out a trade and are not subject to the identification obligation pursuant to Section 2 of the Money Laundering Act, i.e. no institutions as mentioned in Section 1 of the Money Laundering Act and no lawyers, patent attorneys, notaries, tax consultants, agents in tax matters, qualified auditors, certified accountants, real estate brokers or gambling casinos.

No suspicious transaction reports were submitted by "other business persons" in 2002 and 2003, four reports each were filed in 2004 and 2005 and only two reports were received in 2006. Consequently, only ten reports in total have been filed by "other business persons" since August 2002. Given the size of this group of parties required to report and the presumed potential of money laundering in this field, there appears to be a considerable need for information and awareness with regard to this phenomenon.

The federal and state authorities are competent for implementing the Money Laundering Act in the field of the "other business persons" (Section 16 (4) of the Money Laundering Act). It is, however, often problematic to bindingly determine the authority that has supervisory function at regional and local level. A central supervisory authority – like the Federal Agency for the Supervision of Financial Services for the institutions – does not exist in the field of "other business persons".

This unsatisfactory reporting volume and problems involving the determination of the supervisory authorities in this field prompted the FIU to contact two umbrella organisations representing "other business persons", the National Association of German Manual Trades (ZDH) and the German Federation of Chambers of Commerce and Industry (DIHK). With a view on improving knowledge of the relevant regulations and raising the awareness to the money laundering phenomenon among the "other business persons", the FIU published a "letter to sensitise" these parties on the BKA website (see appendix 2), in which information is inter alia provided on the relevant regulations and, on the basis of concrete cases, awareness is raised to the potential involvement in money laundering activities (linked with the risk of being punished for participation in such activities).



## 6.4 Reports made pursuant to Section 31b of the Fiscal Code

Besides the copies of the suspicious transaction reports made pursuant to the Money Laundering Act, the FIU also includes all reports made on suspicion of money laundering pursuant to Section 31b of the Fiscal Code as an information basis when handling its tasks.

As early as 30 October 2002, the Federal Ministry of Finance (file no. VII B 7 - Wk 5023 - 1023/02), in agreement with the Federal Ministry of the Interior, decreed that the fiscal authorities have to report to the law enforcement authorities, pursuant to Section 31b of the Fiscal Code, any facts that suggest an offence punished in accordance with Section 261 of the Penal Code. It is not explicitly stated that copies of the suspicious transaction reports have to be passed on to the Bundeskriminalamt. However, this results from the legal arguments and the sense and purpose of Section 5 of the Money Laundering Act, which came into effect after the Fourth Financial Market Promotion Act and thus after Section 31b of the Fiscal Code.

This soon resulted in the above-mentioned decree to apply Section 31b of the Fiscal Code in which the procedure stipulated therein was declared binding.

Due to a large number of transmission errors and enquiries the FIU received from fiscal authorities regarding the channelling of reports pursuant to Section 31b of the Fiscal Code, the FIU compiled the channelling rules to be applied nation-wide. Since very different methods are applied in the federal states, the FIU repeatedly described feasible reporting channels in its Newsletters (No. 2 – 4), in line with proposals for nation-wide standardisation.

## 6.5 Case collection

Before the FIU was set up at the BKA, information regarding the concealment of illegal assets was hardly subjected to a structured collection and analysis. This concerned both investigations based on suspicious transaction reports pursuant to the Money Laundering Act as well as investigations concerning other crimes (e.g. predicate offences of money laundering). The FIU considers the pooling of this information as one of its main tasks as central police office.

The case collection consists of a constant collection, structured compilation and content analysis of cases with special methods of money laundering and as or unusual asset disposal as well as transactions which could serve the purpose of financing terrorism. By publishing case constellations, the FIU is meeting its statutory obligation as stipulated in Section 5 of the Money Laundering Act, which is "to regularly inform parties required to report pursuant to the Money Laundering Act about money laundering typologies and methods" (early warning function).

The case constellations are based on information actively obtained from the German law enforcement authorities and on the FIU's monitoring of suspicious transaction reports. With a view on gaining the best possible overview of the identified methods of money laundering and the financing of terrorism, the FIU asked all agencies concerned to continue to commit themselves proactively in the future by providing new case constellations.

## 6.6 Internet presentation of the FIU

Since its establishment in August 2002, the FIU has been very active in its public relations work with a view on communicating its essential working results to all agencies involved in the prevention and suppression of money laundering and the financing of terrorism and, thus paving the way for a permanent dialogue.

This is the main purpose of the information published by the FIU on the website of the Bundeskriminalamt, briefly described below. Please see appendix 3 for a graphic description of the structure and the path of the Internet offer:

### **"Publications" (password-secured)**

Some information offers are published on the Internet in the password-secure section. This access restriction is considered necessary because the contents could be misused for instructions to commit money laundering offences and the perpetrators could circumvent the information published in a targeted manner by altering their behaviour. The access data were exclusively transmitted to the money laundering officers via the respective associations and can be obtained from the FIU or the competent associations. The money laundering officers have to prove their appointment to the association and as or the FIU.

### **Form "Suspicious transaction report" pursuant to Section 11 of the Money Laundering Act**

A sample form along with instructions for use and the contact data for the relevant agencies has been posted as a downloadable file since April 2005. It would be very desirable to have suspicious transaction reports submitted on the standardised form to the relevant agencies, with copies sent (by fax) to the BKA (FIU). The use of this standardised form would enhance the efficiency of the process for all parties involved.

### **Form "Follow-up responses pursuant to Section 11 (9) of the Money Laundering Act"**

In order to be able to reliably assign these responses to the original suspicious transaction report and to facilitate further analysis, the form "follow-up responses by public prosecutors' offices pursuant to Section 11(9) of the Money Laundering Act" was developed and published on the Internet. Although there is no obligation to use it, the form ensures that the minimum standards are fulfilled in respect of completeness and depth of information of the relevant data, thus producing a better overall picture of the "judicial success" of the suspicious transaction reports filed in Germany.

### **FIU Newsletter – Money laundering and terrorist financing indicators**

All four issues of the Newsletter published so far have been posted on the Internet, some of them with translations into English. The third Newsletter is identical with the indicator paper.

### **"Publications" (without access restriction)**

#### **Annual reports of the FIU**

The FIU has published all annual reports prepared so far (2002-2006) on its website. Apart from the 2003 Annual Report, all reports are also available in English.

#### **Internet information for new parties required to report**

This FIU Internet portal is primarily meant for the additional occupational groups tasked with reporting obligations when the Money Laundering Act was amended in 2002 – lawyers, legal advisors (if they are members of a chamber of lawyers), patent attorneys, notaries, auditors, tax consultants, agents in tax matters, certified accountants). However, the information published also offers interesting background information to other parties required to report.

#### **Internet information for "Other business persons"**

In order to improve the reporting behaviour, the FIU published a letter on its website especially for "other business persons" pursuant to the Money Laundering Act which aims at raising awareness (see also appendix 2).

### **Publications by the Financial Action Task Force (FATF)**

The FIU had the Bundessprachenamt (Federal Office of Languages) translate the FATF reports on money laundering typologies for the years 2002 to 2005 into German and published them on its website. Since 2006, the FATF has only prepared project reports on the following subjects:

- Report on trade-based money laundering 06/2006
- Report on the misuse of corporate vehicles, including trust and company service providers 10/2006
- Report on new payment methods 10/2006

The above-mentioned reports are available (in English) on the FIU's website.



## 6.7 The "electronic suspicious transaction report (eVA)" project

### 6.7.1 Preliminary remarks

Law enforcement authorities face an increasing workload as a result of the progressive rise in the number of suspicious transaction reports. This applies to information processing but also, and in particular, to the recording and evaluation of information received. In light of this increased workload, reporting parties have also expressed the need for greater efficiency as well as a reduction of the costs of filing suspicious transaction reports.

In order to achieve the desired improvements, the required as well as recommended contents of suspicious transaction reports have been specified in a standard model report form, which was made available as a WORD-based form in April 2005.

In mid 2005, the Federal Ministry of the Interior ordered the BKA to perform a feasibility study and a cost-benefits assessment for the purpose of determining whether an electronic suspicious transaction report (Project "eVA") could be realised as an Internet-capable service on the basis of the "BundOnline 2005" e-government initiative.<sup>16</sup>

The objectives of the "eVA" project and the tentative results of the study are described below:

### 6.7.2 Objectives

- A high level of acceptance among parties required to report
- Elimination of media barriers in order to achieve (partially) automated processing in police systems
- Improvement in the quality of suspicious transaction reports through structured, comprehensive transmission of information in order to create a better basis for police investigation and analysis and to avoid time-consuming follow-up and post-processing work.
- Acceleration of the reporting process, in order to provide for more rapid response, especially in "deadline" and "rush" cases.
- Better protection of received data to ensure confidentiality, integrity<sup>17</sup>, and authenticity<sup>18</sup>
- Assurance of the amenability of the entire process to auditing
- Use of recognised standards and procedures that have proven effective in actual practice and about which all parties involved are well informed and able to adopt the technical processes involved without the need for time-consuming tests.

The basic technical concept developed by the BKA on the basis of these objectives was presented to representatives of the credit sector, the financial service provider sector and the financial investigation offices of the state criminal police offices for review and approval on the occasion of a final workshop in late October 2005.

<sup>16</sup> See also <http://www.wmsbundonline.de/>

<sup>17</sup> Integrity refers to the degree to which data are protected against manipulation by third parties.

<sup>18</sup> Authenticity is the degree of assurance that the identity of an individual conforms to the identity claimed by the individual.



### 6.7.3 Recommendation

The eVA concept in its current form provides for two new channels for the electronic transmission of suspicious transaction reports. The first of these options involves the use of an online form to transmit reports and attachments (e.g. account complexes or lists of account transactions) electronically to the state criminal police offices and the FIU. The content of the online form corresponds for the most part to that of the existing model form, but also provides additional options intended to facilitate the entry of data. This mode of transmission is particularly well suited to the needs of reporting parties who file relatively low numbers of reports (business persons, lawyers etc.)

A second alternative is the direct transmission of suspicious transaction report data from the data-processing systems operated by the reporting parties. This option would be used by reporting parties with high reporting volumes (e.g. large banks) and corresponding research and monitoring software.

User authentication would be ensured by a user management system which is accessible only via a programmed component of the eVA system, ensuring authenticity of the reporting party.

### 6.7.4 Tentative summary

The study prepared in close consultation with potential users and recipients clearly indicates that timely implementation of an electronic reporting system (eVA) as an Internet-capable service for both state and federal authorities should be recommended as a consolidated system on a cost-sharing basis. The feedback provided in the workshops attended by representatives of the reporting parties and the state criminal police offices gives reason to expect that the concept in its current form would be widely accepted.

As the cost-benefits assessment<sup>19</sup> indicates, the required investment in the system would not only pay for itself but would provide other benefits as well. Law-enforcement authorities could expect a marked improvement in the quality of data provided for the purposes of investigation and analysis. The eVA will also result in a significant increase in the speed and efficiency of report processing. Thus the electronic suspicious transaction report could contribute substantially to a rigorous and effective campaign against money laundering and the financing of terrorism.

The Federal Ministry of the Interior and the police expert bodies have meanwhile approved the eVA project. Besides, the Federal Government included eVA as a top service in the eGovernment – Initiative 2.0<sup>20</sup>.

### 6.7.3 Further steps

A project group has been established at the Bundeskriminalamt that started to elaborate a refined concept under participation of the federal states and industry in spring 2007. On behalf of the associations, pilot participants are being determined for this purpose. Subsequently, the refined concept has to be re-submitted for approval to the police bodies. Afterwards, the development of the necessary technical components and the pilot phase can be started.

<sup>19</sup>The assessment was performed with the assistance of an external consultant on the basis of information provided by the Co-ordination and Consulting Office of the Federal Government for Information Technology (KBSt).

<sup>20</sup>See also [://www.wmsbundonline.de/](http://www.wmsbundonline.de/) for further information on the eGovernment initiative of the Federal Government.



## 6.8 Status of implementation of the "Third EU Money Laundering Directive"

Directive 2005/60/EC, issued on October 26<sup>th</sup> 2005 by the European Parliament and the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Third EU Money Laundering Directive), took effect on December 15<sup>th</sup> 2005.

The Directive is to be incorporated into national law by December 15<sup>th</sup> 2007. It contains primarily provisions designed to prevent money laundering and the financing of terrorism. Directive 2006/70/EC, issued by the Commission on 01 August 2006, which contains implementing rules for directive 2005/60/EC, has to be observed in this regard. They refer to the definition of "politically exposed persons" and the determination of technical criteria for simplified customer due diligence procedures and exemption from customer due diligence procedures in cases where financial transactions are carried out occasionally or to a very limited extent only. Like the Second EU Money Laundering Directive, the third one also contains a large number of issues affecting both the competence of the Ministry of the Interior and that of the Federal Ministries of Finance, of Justice and of Economics and Technology. These issues are currently discussed between the relevant departments and comprised in a bill drafted for an amendment to the Money Laundering Suppression Act. Once completed, this bill will be forwarded – in accordance with the prescribed participation process – to the federal states and the chambers and associations concerned (banks, the credit sector and professional organisations representing "freelance occupations").

The bill mainly focuses on the following:

- Provisions governing internal risk-management measures to prevent money laundering ("customer due diligence measures") in consideration of new money laundering trends and typologies. The risk-oriented approach pursued in this context clearly shows that the danger of money laundering and the financing of terrorism is not equally high in all case constellations. The Third EU Money Laundering Directive allows of eased customer due diligence if the transactions pose only a little money laundering or terrorist financing risk but provides for increased diligence in cases in which a higher risk is evident. Consequently, the bill mainly aims at developing simplified and increased customer due diligence measures. It is important to ensure, however, that reporting parties can meet these stricter requirements without unreasonable effort or cost.

- Improved integrity and transparency standards to prevent money laundering and the financing of terrorism. As regards the transparency of legal entities, the Financial Action Task Force on Money Laundering (FATF) recommends that the countries take appropriate action with a view to preventing the misuse of legal entities by money launderers. It has to be ensured that adequate, correct and up-to-date information is available on the beneficial owners and the control structures and that the competent authorities can obtain or retrieve this information in good time. The third EU Money Laundering Directive takes up this recommendation and introduces the concept of the beneficial owners in connection with identification obligations for legal entities.
- Expansion of the instruments developed for the suppression of money laundering to encompass the suppression of financing of terrorism as well. The reporting obligation specified in Article 22 of the Third EU Money Laundering Directive as well as the other requirements are expanded to include transactions which support the financing of terrorism or would do so if actually carried out. The inclusion of this phenomenon is intended to ensure that all available information can be used in the fight against the financing of terrorism. In effect, this reflects the intent of FAFT Recommendation 16, in particular.

The FIU commented to the Federal Ministry of the Interior on the amendment proposals of relevance to the FIU and will provide advice during the further law-making process. All changes that will result from the new Money Laundering Act will be made available to the parties required to report as soon as possible and in a form suitable for use.



## 7 International co-operation

### 7.1 Exchange of intelligence with other FIUs

Pursuant to Section 5 (2) of the Money Laundering Act, the German FIU at the Bundeskriminalamt works closely together with the central agencies of other countries responsible for the prevention and prosecution of money laundering and the financing of terrorism.

During the year under review, the intelligence exchanged in connection with this central office function with the corresponding foreign offices was again the essential basis for the initiation of new, or the provision of support to pending, investigations in the various fields of crime in Germany.

All in all, the FIU corresponded with foreign FIUs in 718 cases in 2006. This represents an increase of approximately 9% over the preceding year. The rate of increase from 2004 to 2005 was approximately 8%.

The following table contains a list of the twenty countries with which the FIU Germany corresponded most frequently.

Table 22: Exchange of intelligence with foreign FIUs (TOP 20)

Country	Number		Change from 2005
	2006	2005	
Netherlands	101	16	531%
Luxembourg	71	68	4%
Switzerland	59	53	11%
Belgium	58	82	-29%
France	37	32	16%
Russia	27	31	-13%
Bulgaria	24	29	-17%
Liechtenstein	21	14	50%
Spain	20	18	11%
Finland	16	7	129%
Hungary	14	19	-26%
Poland	14	19	-26%
Portugal	13	10	30%
Croatia	12	18	-33%
Austria	11	9	22%
Ukraine	10	12	-17%
Slovakia	8	10	-20%
Jersey	8	5	60%
Great Britain	8	5	60%
USA	6	15	-60%
Other	180	185	-3%
<b>Total</b>	<b>718</b>	<b>657</b>	<b>9%</b>

In 2006, the FIU Germany co-operated with the corresponding offices in 62 countries all over the world. As last year, the contacts were focused primarily on co-operation with FIUs in the major European finance centres, in a few eastern European countries and Germany's neighbour countries.

The enormous increase in correspondence exchanged with the Netherlands is due to an extensive investigation complex with numerous references to Germany conducted by the Dutch authorities. This illustrates that the statistical development is also influenced by chance.

The detailed analysis of all information obtained through the national and international exchange of correspondence resulted in specific links to intelligence held by German law enforcement authorities in 108 cases of correspondence.

As in previous years, a considerable percentage (33%) of the cases were noted to have links to fraud. The next important links are those to money laundering (17% of the cases) and to drugs (5%).

In 182 requests for information submitted by foreign FIUs, concrete suspicious circumstances in respect of specific types of crime or crime phenomena were already indicated. Here, too, fraud cases (41% of the requests) head the list, followed by money laundering (14% of the requests) and drug cases (13% of the requests).

## 7.2 Noteworthy cases in the context of international FIU correspondence

Further to the statistical data provided above, the following are two examples of noteworthy cases handled by the FIU in 2006:

### Case: Purchase of valuable real estate

A suspicious transaction report was filed by a German bank in 2005 concerning a German national. The person reported obviously acted on behalf of a foreign national, using funds for the purchase of real estate in Germany that had been transferred to German accounts from abroad. The economic background of the assets transferred from abroad was unknown. On the basis of the suspicious transaction report, an investigation for suspected money laundering was initiated into this German national.

The initial clearing process led to establishing that this German national was financing a valuable real estate in Germany and was preparing the purchase of a business involving several millions of euros on behalf of a foreign national. Regarding this foreign national, there were indications that he was a former office holder responsible in particular for the privatisation of state-owned company shares. It could not be excluded that the assets invested in Germany were embezzled state funds.

In the course of the investigations conducted at the FIU, a considerable discrepancy was established between the receipts obtained from the management of the real estate on the one hand and the liabilities for financing the loan as well as additional operating expenses on the other hand. The resulting gaps in coverage were compensated by considerable payments from foreign letter-box companies whose economic background was completely unclear. The accused was in positions of responsibility in almost all of the foreign letter-box companies. The amount of assets transferred to Germany did not correspond to the accused person's known financial situation.

With the help of the accused, the foreign national purchased the above-mentioned business in Germany. The funds transferred to Germany for this purchase came from the same foreign letter-box companies as those previously used for financing the above-mentioned real estate. Besides the money transfers in connection with real estates, further sums in the seven-digit euro range were transferred to Germany.

The investigations have brought to light that the suspected financial backer of these operations was the above-mentioned foreign national who used the accused person's network of companies and accounts in Germany and abroad. The investigations in respect of the predicate offence(s) also revealed that this foreign national was already under investigation abroad for suspected abuse of official authority and embezzlement of state funds.

In the end, the investigations have corroborated the suspicion that the accused, due to

- his central positions within the companies active in Germany and abroad,
- his acting "in the foreground" towards the German credit institutions involved,
- his extensive powers to draw on the business and private accounts of this foreign national,
- his business activities on behalf of this foreign national, and
- the international cash flows handled through his accounts,

concealed the assets coming from the illegal (predicate) offences of this foreign national through an international network of accounts and companies, involving offshore companies, trustees and brokers, fictitious and cover contracts as well as investments in real estates in Germany in the sense of Section 261 of the Penal Code and thus jeopardised the tracing of the origin of the money.

#### **Case: Concealment of embezzled gambling funds**

In connection with a clearing process, the FIU took over investigations into beneficial owners of a network of German companies for suspected money laundering.

There was suspicion that considerable amounts of money were obtained from private individuals by professional fraud as well as breach of trust in connection with the organisation of games of chance (Lotto, participation in games of chance through the Internet) without using these funds for the intended purpose, i.e. the participation in games of chance.

The analysis of investigations (some of them initiated on the basis of suspicious transaction reports) led to the identification of the persons responsible who operate the required structure of companies and as or organisations abroad. The complex structure of this organisation has been established through the FIU's partner services abroad.

The modus operandi is characterised by

- soliciting of new customers through call centres that are partly self-managed or controlled
- collection of customer funds through the respective companies
- cash withdrawals and money transfers also through financial transfer service providers
- difficulties for the customers to check whether the games of chance have actually been carried out.

### 7.3 Egmont Group

The annual plenary meeting of the Egmont Group took place in Limassol, Cyprus, from June 12<sup>th</sup> to 16<sup>th</sup> 2006. The conference was attended by representatives of 79 FIUs, observers of FIUs with applicant status and delegates from, inter alia, the United Nations, the World Bank and the International Monetary Fund. The FIU Germany was represented by its head.

A priority subject of the meeting was the formalisation of the structure and working methods of the Egmont Group. The essential suggestions on this subject had been elaborated by the "Transition Sub-Committee (TSC)" of the Egmont Group in which also Germany participated.

Based on these working results, the following resolutions were adopted:

- The future permanent secretariat of the Egmont Group will be seated in Canada (Toronto) and will take up its work with four staff members at first.
- The budget will be financed by a basic contribution to be made by each FIU, supplemented by a country-specific contribution that depends on the gross national product of the respective country. Besides, minimum and maximum contributions are defined.
- The work of the "Transition Sub-Committee" has been completed. This body will thus be dissolved.
- With a view to formulating the agreed contents of the so-called Charter MoU as a future formal basis of the Egmont Group and assisting as accompanying the establishment of a permanent secretariat in Canada, an "Implementation Sub-Committee" with two working groups will be set up.

Other topics:

- The head of the FIU Liechtenstein has been elected as new chairman of the "Operational Working Group (OpWG)". This working group serves as a platform within the Egmont Group for exchanging information on current international case constellations focussing on "new typologies".
- The FIU France and the FIU Cyprus have been elected into the Egmont Committee as new representatives for Europe for two years.
- No new FIU was admitted to membership in the Egmont Group at the conference.

### 7.4 Memorandum of Understanding (MoU)

Following the two MoUs concluded with the FIU Poland and the FIU Russia in 2005, it was now possible to conclude a MoU with the FIU Canada (FINTRAC). Under Canadian law, it is a prerequisite for the FIU Canada that such a memorandum is signed before personal data can be exchanged with other FIUs.

An MoU with the FIU Australia (AUSTRAC) is being prepared. Due to the – meanwhile realised – reform of the Australian law on the suppression of money laundering and the financing of terrorism, there have been delays in formulating the text of the memorandum since it had to be adjusted to the new legal situation. In the meantime, a draft has been forwarded which is currently being checked.

The FIU Japan (JFIO) has also approached the BKA with the request for conclusion of an MoU. The FIU Germany has sent a text proposal to the FIU Japan. This draft has not yet been signed by the FIU Japan. This appears to be due to the efforts to convert the currently administrative FIU into a police FIU and the relating legal adjustments.

## 7.5 FATF

In 2006, the FATF elaborated and published typology reports on the following subjects:

### **"Report on new payment methods", 10/2006**

This report analyses new payment methods – such as prepaid cards, Internet payment systems, payment via mobiles – and the related risk of misuse for purposes of money laundering and the financing of terrorism.

### **"Report on the misuse of corporate vehicles, including trust and company service providers", 10/2006**

This report analyses the misuse of corporate structures as constellations for the purpose of money laundering and the financing of terrorism. The focus of the study is the concealment of the actual beneficial owners as the most significant feature of misuse.

### **"Report on trade based money laundering", 06/2006**

This typology report analyses the possibilities of concealing illegal assets and asset transfers through commercial businesses, among other things through incorrect information on prices, quantity and quality of imports and exports.

The English originals of the reports can be viewed on the website of the FATF and the FIU at the BKA.

Under participation of about 150 persons (among them staff members of the FIU Germany) from 33 countries and 15 international organisations and institutions, the FATF / EAG Joint Experts Meeting on Typologies dealt with the following topics in Shanghai from November 28<sup>th</sup> to 30<sup>th</sup> 2006:

Topic 1: Money laundering in the real estate business

Topic 2: Money laundering by means of value added tax carousel fraud in the EU

Topic 3: Financing of terrorism

Topic 4: Legalisation of profits from drug trafficking

All in all, as in the past, the typology meeting was characterised by very open and constructive discussions. In respect of the FATF's typology work it should be generally noted that topics 2 and 4 rather focus on the specific aspects of the predicate offences (VAT carousel fraud, drug trafficking) than on money laundering. The typology reports on topics 1 to 4 are planned to be completed in 2007.



## 8 Summary and Outlook

Compared to the previous year, a considerable increase in the number of suspicious transaction reports filed pursuant to the Money Laundering Act was identified in 2006. In this context, the "phishing as financial agents" phenomenon again played a central role. This is proved by the meanwhile distinctive awareness to this phenomenon both on the part of those obliged to report and the law enforcement authorities. The quality of the reports improved very positively again.

The quality of the follow-up responses has improved as well. There is, however, still potential for optimisation concerning the completeness of the data. In 2007 as well, the FIU will approach the public prosecutors' offices concerned with a view to further optimising the response reporting practice in respect of quality and quantity. The use of the standardised response form plays an important role in this regard.

In connection with the meanwhile established activities of the FIU in the field of co-operation with the parties required to report (through the Working Party of Banks and Chambers, Newsletters, lectures, hotline, training visits etc.), the publication of the jointly elaborated indicator paper and the awareness-raising measures for "other business persons" (Section 3 (1) of the Money Laundering Act) seem to be worth mentioning.

The "electronic suspicious transaction report" (eVA) project passed important stages of development during the year under review due to the approval by the Federal Ministry of the Interior and the expert committees and its inclusion in the eGovernment – Initiative 2.0 of the Federal Government.

At international level, the organisational developments of the Egmont Group were also successfully supported by the co-operation of the FIU Germany. The conclusion of all these measures can be expected in 2007.

The international correspondence exchanged by the FIU in 2006 again resulted in a considerable added value for the German law enforcement authorities.

Besides continuing with the ongoing projects, initiatives, analyses, and investigations, the focal points of activities for the FIU in 2007 are above all the professional assistance provided to the law amendments necessary for implementing the 3<sup>rd</sup> EU Money Laundering Directive, the furthering of the eVA project and the intensive monitoring of the "financial agents" phenomenon.



**9 Appendices**

**Appendix 1:** List of Egmont Group members

**Appendix 2:** Letter by the FIU to raise the awareness of "other business persons" ("sensitisation letter")

**Appendix 3:** Internet presentation of the FIU Germany on the website of the BKA

Appendix 1: List of Egmont Group members (Part 1)<sup>21</sup>

Country	FIU Name	Type	Location
Albania	DBLKPP	Admin	Ministry of Finance
Andorra	UPB	Admin	Independent
Anguilla	MLRA	Admin	Independent
Antigua & Barbuda	ONDCP	Admin / Police	Independent
Argentina	UIF	Admin	Ministry of Justice (Indep)
Armenia		Admin	
Aruba	MOT-Aruba	Admin	Ministry of Finance
Australia	AUSTRAC	Admin	Attorney General's Dept.
Austria	A-FIU	Police	Ministry of Internal Affairs
Bahamas	FIU	Admin	Independent
Bahrain	AMLU	Police	Anti-Economic Crimes Directorate
Barbados	FIU	Admin	Office of the Attorney General
Belarus		Admin	
Belgium	CTIF-CFI	Admin	Independent
Belize	FIU	Admin / Police / Judicial	Independent
Bermuda	BPSFIU	Police	Police
Bolivia	UIF-Bolivia	Admin	Superintendancy of Banks
Bosnia & Herzegovina		Police	
Brazil	COAF	Admin	Ministry of Finance
Bulgaria	FIA	Admin	Ministry of Finance
BVI	Financial Investigation Agency	Police	Financial Services Commission
Canada	FINTRAC / CANAFE	Admin	Independent
Cayman Islands	CAYFIN	Admin / Police	Atty General
Chile	CDE	Judicial	Presidential Office
Colombia	UIAF	Admin	Ministry of Finance
Cook Islands	CIFIU	Admin	Independent
Costa Rica	CICAD / UAF	Admin	Presidential Office
Croatia	AMLĐ	Admin	Ministry of Finance
Cyprus	MO.K.A.S.	Judicial	Attorney General's Office
Czech Republic	FAU-CR	Admin	Ministry of Finance
Denmark	HVIDVASK	Judicial / Police	Public Prosecutor's Office
Dominica	FIU	Police	Independent
Dominican Rep.	UIF-Dom Rep	Admin	Superintendancy of Bank
Egypt	EMLCU	Admin	Independent
El Salvador	UIF-El Salvador	Admin	Attorney General's Office
Estonia	FIU	Police	Estonian National Police
Finland	RAP	Police	Police

<sup>21</sup> **Highlighted:** FIUs that joined the Egmont Group in 2007

Appendix 1: List of Egmont Group members (Part 2)<sup>21</sup>

Country	FIU Name	Type	Location
France	TRACFIN	Admin	Ministry of Finance
Georgia	FMS	Admin	Independent
Germany	FIU	Police	Federal Criminal Police Office
Gibraltar	GCID GFU	Customs / Police	
Greece	Committee / Art 7	Admin	Independent
Grenada	FIU	Police	Independent
Guatemala	IVE	Admin	Superintendency of Banks of Guatemala
Guernsey	FIS	Customs / Police	Independent Service Authority
Honduras		Admin	
Hong Kong	JFIU	Customs / Police	Police Headquarters
Hungary	ORFK	Police	National Police Directorate
Iceland	RLS	Police	National Icelandic Police
India		Admin	
Indonesia	PPATK	Admin	Independent
Ireland	MLIU	Police	An Garda Síógana
Isle of Man	FCU-IOM	Police	Police
Israel	IMPA	Admin	Ministry of Justice
Italy	UIC (S.A.R.)	Admin	Central Bank
Japan	JAFIO	Police	Police
Jersey	FCU-Jersey	Customs / Police	Police
Korea (South)	KoFIU	Admin	Ministry of Finance / Economy
Latvia	KD	Admin	Prosecutor's Office
Lebanon	SICCFIN	Admin	Central Bank
Liechtenstein	EFFI	Admin	Ministry of Finance
Lithuania	MDP prie VRM	Police	Ministry of the Interior
Luxembourg	CRF	Judicial	Prosecutor's Office
Macedonia	MLPD	Admin	Ministry of Finance
Malaysia	FIU / UPW	Admin	Central Bank of Malaysia
Malta	FIAU	Admin	Independent
Marshall Isles	DFIU	Admin	Banking Commission
Mauritius	FIU	Admin	Independent
Mexico	DGAIO / UIF	Admin	Ministry of Finance
Monaco	SICCFIN	Admin	Ministry of Finance
Montenegro		Admin	
Netherlands	MOT	Police	Ministry of Justice

<sup>21</sup> **Highlighted:** FIUs that joined the Egmont Group in 2007

Country	FIU Name	Type	Location
New Zealand	NZ Police	Police	Police
Nigeria		Admin	
Niue		Admin	
NL Antilles	MOT-AN	Admin	Ministry of Finance
Norway	ØKOKRIM	Police / Judicial	Police
Panama	UAF-Panama	Admin	National Security Council
Paraguay	UAF-Paraguay	Admin	Presidential Office
Peru		Admin	
Philippines		Admin	
Poland	GIF	Admin	Ministry of Finance
Portugal	FIU	Police	Police
Qatar		Admin	
Romania	ONPCSB	Admin	Independent
Russia	FMC	Admin	Independent
San Marino		Admin	
Serbia	FCPML	Admin	Independent
Singapore	STRO	Police	Police
Slovakia	OFiS ÚFP	Police	Ministry of Interior
Slovenia	OMLP	Admin	Ministry of Finance
South Africa	FIC	Police	Independent
Spain	SEPBLAC	Admin	Central Bank
St Vincent & the Grenadines	FIU	Admin	Independent
St. Kitts & Nevis	FIU	Admin	Independent
Sweden	NFIS	Police	Police
Switzerland	MROS	Admin	Federal Office of Police
Syria		Admin	
Taiwan	MLPC	Law Enforcement	Ministry of Justice
Thailand	AMLO	Police / Admin	Independent
Turkey	MSK - FCIB	Admin	Ministry of Finance
UAE	AMLSCU	Admin	Central Bank
Ukraine	SDFM	Admin	Ministry of Finance
United Kingdom	FID / NCIS	Police	Police
United States	FinCEN	Admin	Ministry of Finance
Vanuatu	FIU	Admin	State Law Office
Venezuela	UNIF	Admin	Superintendancy of Banks

## Appendix 2: Letter by the FIU to raise the awareness of "other business persons" ("Sensitisation letter")

### Suppression of money laundering – a task for the whole of society

#### Overview of the tasks of the FIU Germany – the Central Office for Suspicious Transaction Reports – and obligations of the "other business persons" pursuant to the Money Laundering Act

Following the attacks on the World Trade Center on September 11<sup>th</sup> 2001, a number of new legal regulations and guidelines were adopted which are to place increasingly strict limits on the perpetrators' fields of activities. Consequently, a Central Office for Suspicious Transaction Reports, known as FIU (Financial Intelligence Unit) at international level, has been set up at the Bundeskriminalamt. Pursuant to Section 5 of the Money Laundering Act, it has the following tasks:

- Collection and analysis of information and comparison with that provided by other national agencies (Section 11 of the Money Laundering Act)
- Provision of relevant information to the law enforcement authorities of the Federation and the German states
- Statistical recording of suspicious transaction reports
- Publication of an annual report
- Provision of information to the reporting parties about the identified typologies and methods of money laundering
- Co-operation with the central offices of other countries that are responsible for preventing and prosecuting money laundering and the financing of terrorism

When the Money Laundering Act was amended on August 15<sup>th</sup> 2002, new occupational groups, such as lawyers, auditors and real estate brokers, were added to those obliged under the Money Laundering Act and especially the identification obligation in cases of suspicion (involving money laundering and the financing of terrorism) and the reporting obligation in cases of suspicion involving money laundering were introduced for "other business persons". In connection with the 3<sup>th</sup> EU Money Laundering Directive (which is to be implemented in national law by the end of 2007), further adjustments could become necessary which may also affect the group of the "other business persons".

In 2005, the "other business persons" filed only 21 of all the 8,241 suspicious transaction reports. This suggests that, as far as the "other business persons" are concerned, there is still much need for further information about their obligations pursuant to the Money Laundering Act. The following catalogue of questions and answers is to serve the purpose of eliminating any existing uncertainties.

#### What does "other business persons" mean?

According to the Section 3 (1) sentence 2 of the Money Laundering Act, "other business persons" are those who carry out a trade and are not subject to the identification obligation pursuant to Section 2 of the Money Laundering Act, i.e. no institutions as defined in to Section 1 of the Money Laundering Act and no lawyers, patent lawyers, notaries, tax consultants, agents in tax matters, qualified auditors, certified accountants, real estate brokers or gambling casinos. Consequently, they include all legal or natural persons who carry out a trade and who are not explicitly mentioned in the Money Laundering Act.

### **What obligations do the "other business persons" have under the Money Laundering Act?**

Their obligations include in particular

- customer identification when accepting cash amounts of EUR 15,000 or more and in cases of suspected money laundering or suspected financing of terrorism
- retention identification documents
- filing of a suspicious transaction report in case of suspected money laundering

### **When does a suspicious transaction report has to be filed?**

Facts suggesting that a financial transaction serves the purpose of money laundering or would serve this purpose if actually carried out have to be reported immediately to the competent law enforcement authorities by the "other business persons", with a copy to be sent to the Bundeskriminalamt, Financial Investigation Unit (Central Office for Suspicious Transaction Reports).

### **Who is the first point of contact for the reporting parties and to whom do the reporting parties have to address the suspicious transaction reports?**

The "other business persons" in the sense of the Money Laundering Act address their suspicious transaction reports to the competent law enforcement authorities and send (or fax) a copy to the Bundeskriminalamt – Financial Intelligence Unit (see Section 11 (1) of the Money Laundering Act. The law enforcement authority to be contacted by "other business persons" usually is the criminal police office of the respective German state. The contact details of the agencies responsible for suspicious transaction reports filed pursuant to the Money Laundering Act can be obtained from the Financial Intelligence Unit at the BKA or directly through the central phone numbers of the respective state criminal police offices.

### **Does the customer get a copy of the suspicious transaction report or does he know who filed the STR?**

In order not to jeopardise the success of investigations that might be initiated, the customer does not receive any information from the public prosecutor's office or the state criminal police office on suspicious transaction reports filed. The same applies to so-called "petitioner enquiries" (enquiries from citizens about data stored with authorities) where it is impossible to obtain information on the party who filed the report.

### **Is the party filing the report threatened with any (liability-related) legal consequences by the customer?**

Pursuant to Section 12 of the Money Laundering Act, the person filing the report cannot be held responsible, unless the report has been made in a deliberately or grossly negligently false manner.

### **Is the reporting party allowed to inform the customer about the STR filed?**

No. Pursuant to Section 11 (5) of the Money Laundering Act, the reporting party may not inform the customer about the STR or any investigation initiated on the basis of this STR.

**Is there also a reporting obligation if a customer is exclusively staying abroad?**

Yes. The suppression of money laundering must be seen in the context of the fight against internationally organised crime. This means that, as a rule, it is irrelevant whether the customer exclusively or mainly stays abroad.

**What are the penal consequences of money laundering pursuant to Section 261 of the German Penal Code?  
Does the reporting party have any chance to avoid penal consequences in an advanced state of customer relations?**

Money laundering that constitutes an offence pursuant to Section 261 of the German Penal Code is punished with imprisonment ranging between 3 months and 5 years. Aggravated cases may be punished with imprisonment ranging between 6 months and 10 years.

Pursuant to Section 261 (9) of the German Penal Code, the criminal offence of money laundering as well as disguising illegal assets allows of so-called "active repentance". Consequently, pursuant to Section 261 of the Penal Code, no punishment shall be imposed on anyone who voluntarily reports a case of money laundering to the law enforcement authorities or causes the items to be seized (items such as cash or book money, valuables, securities, real estates, company shares, objects and all kinds of claims and rights).

**For what kind of predicate offences can the concealment or the disguising of the origin or the acceptance of assets from the predicate offence constitute an offence of money laundering and require the filing of a suspicious transaction report?**

The individual underlying offences in which the filing of a suspicious transaction report may be necessary are defined in Section 261 (1) of the German Penal Code. Since the list of predicate offences is long, it can be assumed, when in doubt, that any significant criminal activity is included in this list.

**What measures have to be taken in order to comply with the identification obligation under the Money Laundering Act?**

The identification obligation of the "other business persons" results from Section 3 (1) in conjunction with Section 2 (1),(2) and (3) and Section 6 of the Money Laundering Act. Pursuant to Section 8 of the Money Laundering Act, they are also obliged to seek information about the economic beneficiary and to establish his or her name and address.

In particular, this means the following:

- When accepting money worth 15,000 euros or more, the party presenting himself or herself has to be identified. This also applies to persons authorised to accept money by these enterprises and individuals, as far as they are carrying out their trade or business. Identification in the sense of the Money Laundering Act means to establish the name of the customer on the basis of a valid identity document, the date and place of birth, the nationality and the address (as far as recorded in the document) and to record the kind and the number of the document and the issuing authority. This can be done by copying the identity document, for example.
- Besides, customer identification is needed where facts are detected which suggest that the planned transaction serves the purpose of money laundering pursuant to Section 261 or the financing of a terrorist organisation pursuant to Section 129a in conjunction with Section 129b of the Penal Code or would serve such purposes if actually carried out (regardless of the sum involved).



- The parties required to report shall seek information from the person to be identified as to whether he/she enters into business for his or her own account. If the customer declares that he or she does not act on his or her own account, the party required to report shall establish, on the basis of the information supplied by him or her, the name and address of the person in question who enters into business.
- The identification shall be recorded and the records shall be retained for 6 years. The retention period shall begin at the end of the calendar year in which the information was obtained.

#### **Does a compliance officer for money laundering have to be named?**

Pursuant to Section 14 (1) No. 8 - 2nd alternative -, in conjunction with Section 14 (2) of the Money Laundering Act, "other business persons" shall design a compliance officer within their enterprise and take safeguards against their being misused for purposes of money laundering if they regularly conduct business in the sense of Section 3 (1) No. 2 and 3 of the Money Laundering Act.

Pursuant to Section 14 (4) of the Money Laundering Act, the competent authority pursuant to Section 16 of the Money Laundering Act may, however, make exemptions.

#### **What prerequisites does a compliance officer have to fulfil, what duties does he have and how is he integrated in the enterprise?**

Pursuant to section 14 (2) No. 1 of the Money Laundering Act, the compliance officer acts as contact for the prosecution authorities and the Bundeskriminalamt – Financial Intelligence Unit.

In order for the compliance officer to handle his tasks effectively, he must have the required expert knowledge, in addition to the necessary physical resources and time.

He should hold a position within the enterprise that allows him to emphatically represent all issues relating to the suppression of money laundering. It is considered obligatory that the compliance officer has power of attorney or sole representation right.

#### **Conclusion**

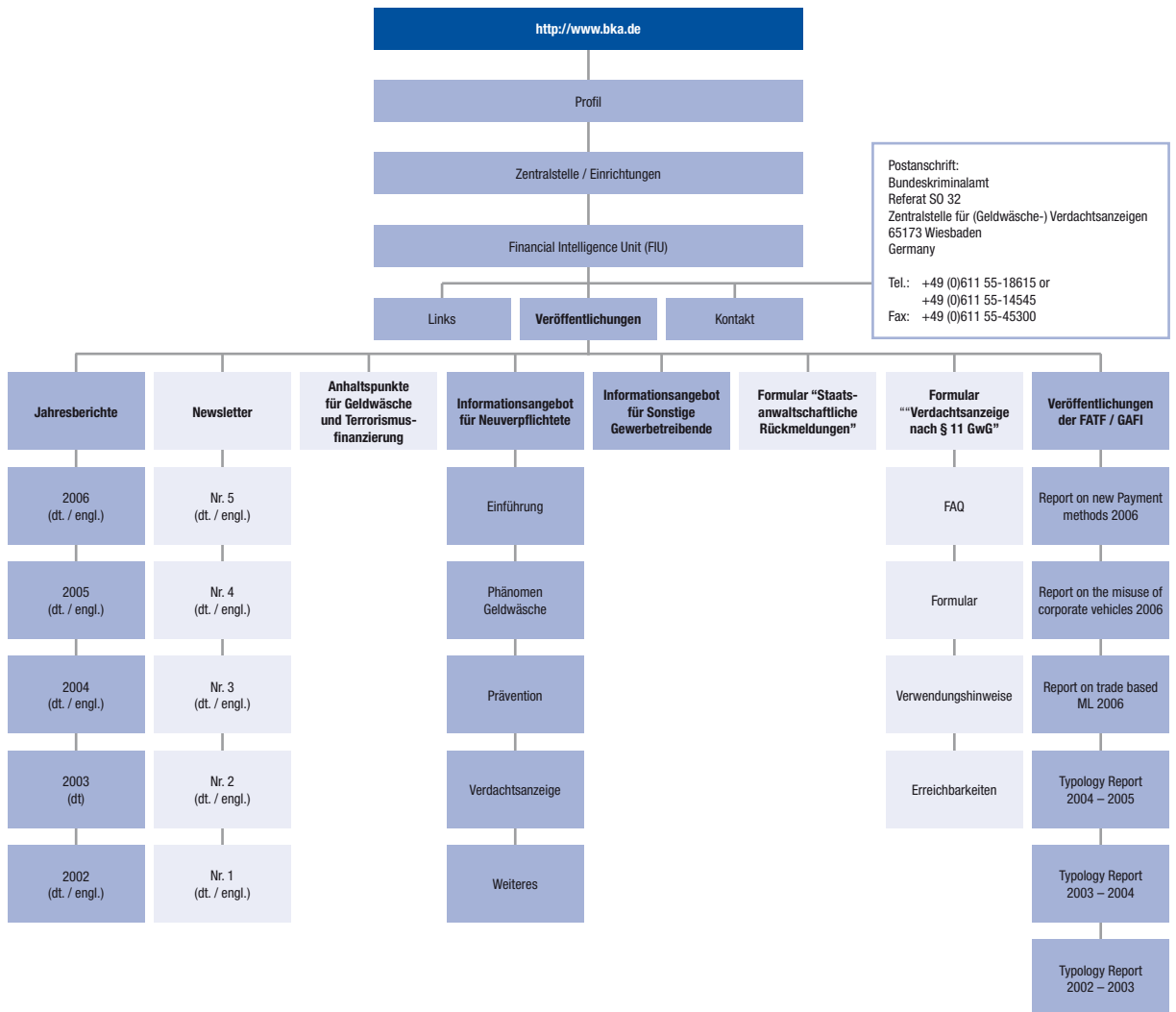
The legal obligations of identification and reporting pursuant to the Money Laundering Act are an additional administrative burden for the "other business persons". However, seen from the macroeconomic aspect, they also ensure economic competition in addition to serving the suppression of subversive organisations, because enterprises that are "subsidised" by assets deriving from illegal activities can easily force others from the market and thus distort competition considerably.

Without the assistance of the occupational groups required to report pursuant to the Money Laundering Act, the law enforcement authorities can take sustained action to a limited extent only. The law enforcement authorities especially depend on the help of the "other business persons" in their efforts to efficiently combat money laundering and to thus guarantee a well functioning competition.

Additional information can be retrieved from the Financial Investigation Unit at the Bundeskriminalamt and from its website.

**Bundeskriminalamt**  
**Referat SO 32 - FIU**  
**Zentralstelle für Verdachtsanzeigen**  
**65173 Wiesbaden**  
**Germany**  
**Tel.: +49-(0)611-55 14545**  
**Tel.: +49-(0)611-55 18615**  
**Fax: +49-(0)611-55 45300**  
**E-Mail: [FIU@bka.bund.de](mailto:FIU@bka.bund.de)**  
**Weitere Informationen unter: [www.bka.de](http://www.bka.de)**  
> Profile > Zentralstelle / Einrichtungen > FIU

Appendix 3: Internet presentation of the FIU Germany on the website of the BKA<sup>22</sup>



<sup>22</sup> The blocks highlighted in light-blue indicate content intended exclusively for money laundering officers. These sources are accordingly password-secured.

**2006 ANNUAL REPORT**  
FIU GERMANY



Bundeskriminalamt