fedpol.ch

Bundesamt für Polizei
Eidg. Justiz- und Polizeidepartement

Office fédéral de la police
Département fédéral de justice et police

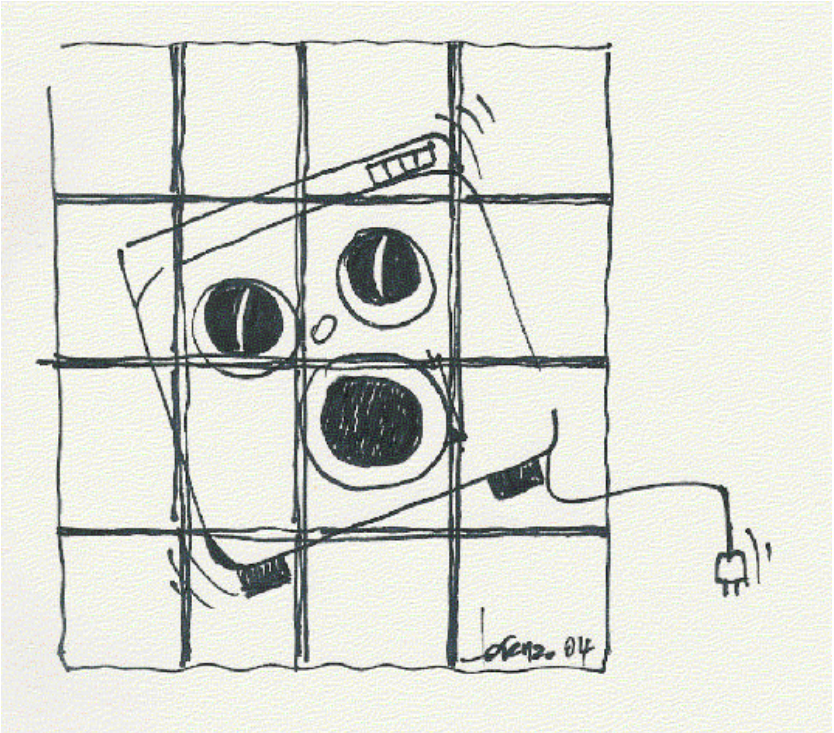
Ufficio federale di polizia
Dipartimento federale di giustizia e polizia

Federal Office of Police
Federal Department of Justice and Police

Money Laundering Reporting Office Switzerland

MROS

6th Annual Report



2003

Federal Department of Justice and Police
Federal Office of Police (fedpol)

MROS

6th Annual Report

March 2004

2003

Federal Department of Justice and Police
Federal Office of Police
Money Laundering Reporting Office Switzerland
3003 Berne

Tel.: (++41) 031 323 40 40
Fax: (++41) 031 323 39 39
email: mros.info@fedpol.admin.ch

Internet: http://www.fedpol.admin.ch

Table of contents

1. Introduction

The year 2003 was dramatic and hectic for MROS as far as its main task - the processing of suspicious activity reports from financial intermediaries - was concerned. Because of various developments at the national and international level, the campaign against money laundering and terrorist funding continued to have the highest priority.

At the international level, just two years after the events of 11 September 2001, the 40 recommendations as well as the eight special recommendations of the Financial Action Task Force (FATF) regarding the fight against the financing of terrorism went through a revision. This revision has a significant impact on Switzerland because national legislation must be adapted to the new standards.
In 2003, there were 84 member countries worldwide in the Egmont Group. Because MROS depends daily on an efficient exchange of information at the international level, the acceptance of new members into the Egmont Group means that the network of information sources has widened and this has proved useful in the processing of suspicious activity reports. The Egmont Group, therefore, also plays an important role in the fight against money laundering and terrorist financing.

At the national level, oversight authorities such as the Federal Banking Commission and the Money Laundering Control Authority drew up new regulations for financial intermediaries. The provisions in these regulations continue to make Switzerland a leader in the fight against money laundering and terrorist financing. This, in turn, improves the Swiss image even more as a financial centre with integrity.

As was the case in 2002, the number of reports of suspicious transactions in 2003 increased considerably, with MROS dealing with around one-third more reports than in the previous year. **Within only two years the volume of reports has doubled. As in 2002, the number of reports sent to the MROS by financial intermediaries from the non-banking sector was greater than those from the banking sector**. Nevertheless, the number of reports by banks increased compared to 2002. **Money transmitters** were at the top of the list of reporting financial intermediaries with more than 400 reports. In contrast, reports from lawyers, insurance companies and asset managers declined. MROS has noticed that the extent to which these financial intermediaries cooperate in the fight against money laundering, based on the number of reports they submitted, is not proportional to their presence on capital markets.

The amount of assets frozen because of reports of suspicious transactions speaks for itself: In 2003 the total amount of blocked assets came to slightly less than the 2002 figure. **Eight per cent of the reports filed in 2003 led to the freezing of more than CHF 1 million in assets**.

Because, in principle, no assets can be frozen on the basis of reports from money transmitters, these reports can be eliminated from the above calculation. This means that the ratio of reports to frozen assets increased to 18% for more than CHF 1 million.

In 2003, reports of suspicious transactions in connection with the possible **financing of terrorism** dropped sharply with only five reports filed. Since 11 September 2001, MROS has received a total of 115 reports related to suspected terrorist financing. Ninety-five of these 115 reports were filed with MROS in 2001, within only a few months of the events on 11 September. These 95 reports accounted for 99% of all the assets frozen on the basis of the 115 reports. It must be concluded from this that the Swiss mechanism used to combat terrorist financing has been successfully implemented.

The reports filed in the period under review cannot be categorised under a particular theme because the case typologies were extremely varied.Since the introduction of the Federal Banking Commission's money laundering regulation, MROS has received **more reports of *attempted* money laundering**. By requiring banks to report such cases, the Federal Banking Commission acted in anticipation of the new FATF recommendations.This development is highly gratifying as it means that the phenomenon of "financial tourism" can be curbed. Financial tourism is the term used to describe the situation whereby an individual travels from bank to bank with the aim of depositing incriminating assets. If one bank is not prepared to do business, then the individual goes to the next bank.

Unfortunately, the Nigerian swindler gangs were extremely active in 2003. For years MROS has been receiving reports concerning the so-called "**Nigerian Letters**" in which dubious letters promise the gullible individual vast sums of money in return for a high advance payment. The victims never receive the promised returns.

Since 1998 MROS has been storing information relevant to money laundering in its GEWA data base, which has become an important tool in establishing a link between older reports of suspicious transactions and more recent developments. The GEWA data base is, therefore, a valuable instrument in the analysis of reports and their subsequent processing by law enforcement agencies.
Under Art. 29, par. 2 of the Money Laundering Act (MLA), cantonal prosecutors as well as the Office of the Attorney General of Switzerland report all pending procedures relating to money laundering and terrorist financing to MROS. This information is also stored in the GEWA data base. It is highly gratifying that the reports of these authorities increased considerably in 2003. On the basis of this information, MROS was in a position to draw conclusions about the fate of the reports passed on to law enforcement agencies: Since 1998 a judgment or judicial decree has been passed on circa 30% of the cases forwarded to the law enforcement agencies. This has **helped to**

considerably reduce the number of pending cases in the hands of the law enforcement agencies.

MROS also noticed that the quality of the reporting has clearly improved. Doubtlessly this has had to do with the regular training of financial intermediaries in combating money laundering. MROS has actively supported the financial intermediaries by organising courses and talks at seminars. Its commitment was highly appreciated at these events.

On the international level, **MROS made new contacts with foreign money laundering reporting offices** and strengthened existing ones. In 2003 MROS met representatives from France, Belgium, Canada, Australia, Ukraine, Austria, Hungary and Liechtenstein and took these opportunities to exchange experiences and explain Swiss procedures to combat money laundering.
Finally we would like to point out that in May 2003 MROS moved into new offices in Nussbaumstrasse 29 in Bern.
Because of the constantly increasing work load, MROS increased the size of its staff from seven to eight.

Lorenzo Gerber
Deputy Head MROS
Bern, January 2004

2. Annual MROS statistics

2.1. General remarks

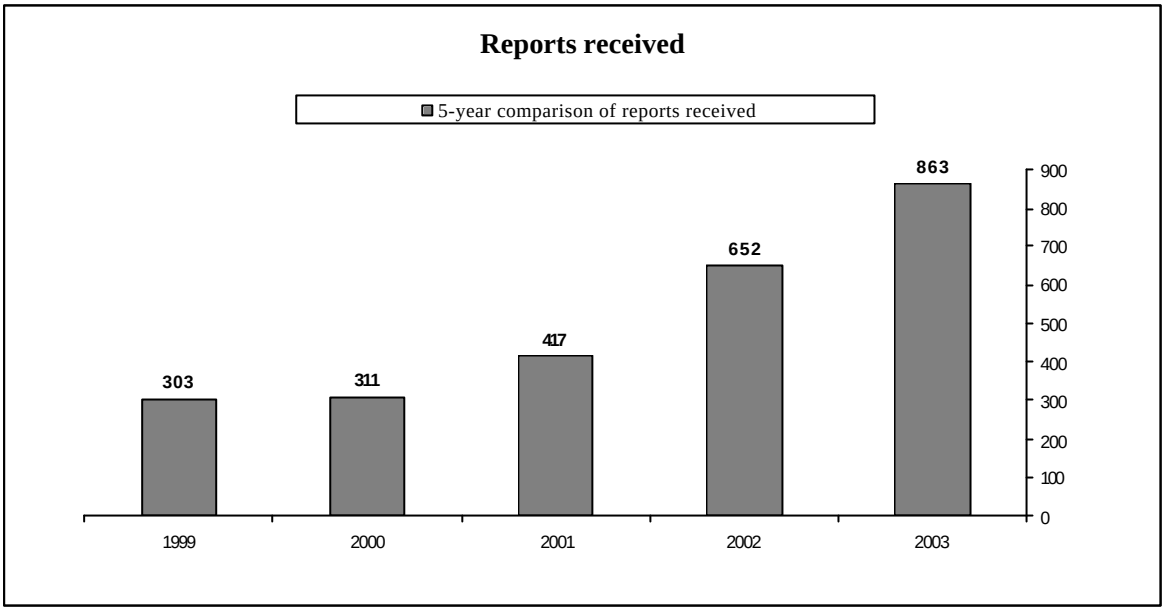
Statistically, three key figures stand out in the 2003 reporting year:

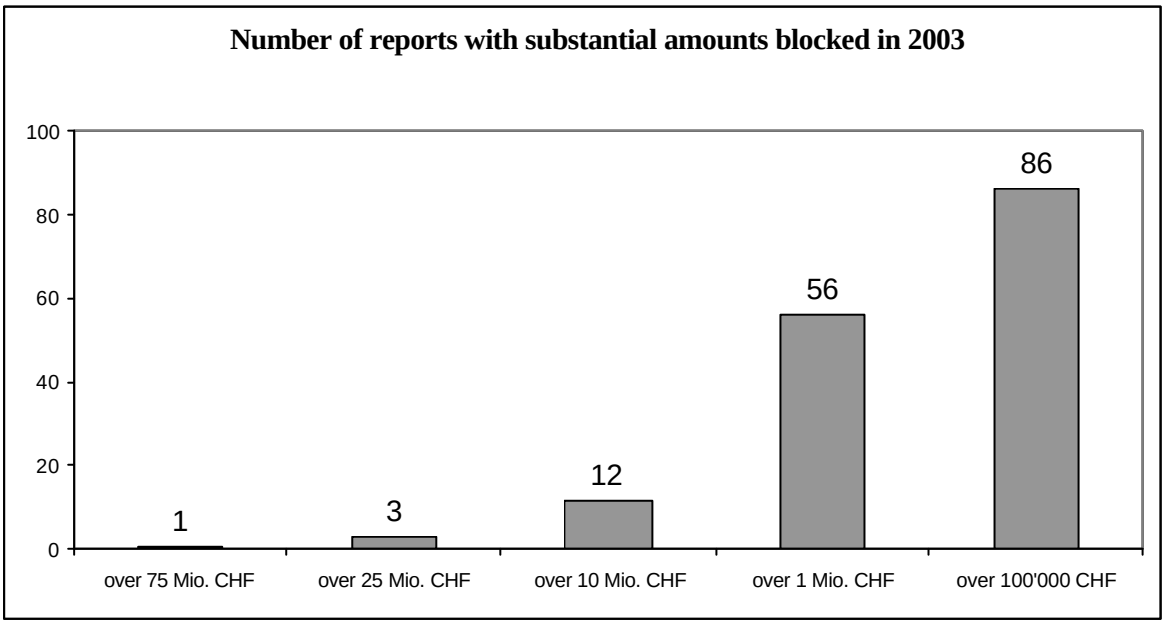
1. The **number of reports** increased by more than **32%**.
2. For the second consecutive year the reports from the **non-banking sector**, including money transmitters, increased. In 2003 this sector accounted for **65%** of the reports, in comparison to 35% from the banking sector.
3. The total **assets** involved **declined** again but in relation to the previous year only by around **7%**. In 2002, the drop in comparison to 2001 came to more than 75%.

The 32.4% increase in reports received in 2003 is again due primarily to the keener reporting habits (+64.6%) of financial intermediaries who provide services in the area of international financial transactions (money transmitters). If the statistics for 2003 are compared with the previous year, the number of reports from the banking sector (+11.4%), fiduciaries (+14.3%) and casinos (+100%) also increased. The other categories of financial intermediaries in the non-banking sector were either stagnant or even showed a decline in the number of reports to MROS.

In comparison with 2002, there was a slight drop of 2.4% to 76.6% in the number of reports passed on to law enforcement agencies. From this it can be assumed that the number of reports passed on from MROS to law enforcement agencies should more or less stabilise in the future. The reasons for this minimal decline are once again to be found in the increase in reports on financial transactions where the percentage of reports passed on came to a mere 61%. On the one hand, cases involving money transmitters are reported, which on first glance appear suspicious but on closer examination contain too little evidence to justify a judicial investigation. On the other hand it should be remembered that the stabilisation in the number of reports passed on is based on the increased quality of the reports which financial intermediaries send to MROS.

In the 2003 reporting period, the total of frozen assets linked with a report once again dropped but the figure of 7.5% was far less than in the previous year. The reasons for this lie, on the one hand, in the fact that, of the large number of reports from money transmitter cases, none included blocked assets. On the other hand, there are growing indications that six years after the Money Laundering Act came into force, Switzerland has become less attractive as a centre of money laundering activities.


Reports received
5-year comparison of reports received
303
311
417
652
863
900
800
700
600
500
400
300
200
100
0
1999
2000
2001
2002
2003


Number of reports with substantial amounts blocked in 2003
100
80
60
40
20
0
1
3
12
56
86
over 75 Mio. CHF
over 25 Mio. CHF
over 10 Mio. CHF
over 1 Mio. CHF
over 100'000 CHF

2.2. The search for terrorist funds

In the 2003 reporting period MROS received five reports in connection with suspected terrorist funding. The total amount of money involved came to nearly CHF 154,000 in comparison with 2001 and 2002 when CHF 37 million and CHF 1.61 million respectively were involved. Four reports concerned individuals who were on the lists issued by the Bush administration. The fifth report was based on the "Taliban regulations" of the State Secretariat for Economic Affairs (seco). MROS passed on all five reports to the Office of the Attorney General of Switzerland.

The following shows in detail the five reports in connection with suspected terrorist funding:

a) Home canton of reporting financial intermediaries

	No. of reports	**%**
ZH	3	60%
BE	1	20%
GE	1	20%
Total	5	100%

b) Type of financial intermediary

	No. of reports	**%**
Banks	3	60%
Money transmitters	1	20%
Insurance companies	1	20%
Total	5	100%

c) Type of bank filing the report

	No. of reports	**%**
Trade bank	2	67%
Major bank	1	33%
Total	3	100%

d) Nationality and domicile of client

Country	Nationality		Domicile	
Switzerland	2	40%	5	100%
Italy	2	40%	0	0%
Pakistan	1	20%	0	0%
Total	5	100%	5	100%

e) Nationality and domicile of beneficial owner

Country	Nationality		Domicile	
Switzerland	1	20%	5	100%
Italy	2	40%	0	0%
Pakistan	1	20%	0	0%
Somalia	1	20%	0	0%
Total	5	100%	5	100%

2.3. Detailed statistics

2.3.1 Overview of MROS statistics 2003

Business year summary (1.1.2003 - 31.12.2003)

Number of reports	2003 Absolute	2003 Relative	+/-	2002 Absolute	2002 Relative
Total received	**863**	100.0%	32.4%	652	100.0%
Passed on to law enforcement agencies	661	76.6%	28.3%	515	79.0%
Not passed on	202	23.4%	47.4%	137	21.0%
Pending	0	0.0%	0.0%	0	0.0%
Type of financial intermediary					
Money transmitter	461	53.4%	64.6%	280	42.9%
Bank	302	35.0%	11.4%	271	41.6%
Fiduciary	48	5.6%	14.3%	42	6.4%
Asset manager / Investment advisor	21	2.5%	-12.5%	24	3.7%
Attorney	9	1.0%	-25.0%	12	1.8%
Insurance	8	0.9%	-11.1%	9	1.4%
Other	5	0.6%	-37.5%	8	1.2%
Casino	8	0.9%	100.0%	4	0.6%
Currency exchange	0	0.0%	-100.0%	1	0.2%
Credit card	1	0.1%	0.0%	1	0.2%
Securities trader	0	0.0%	0.0%	0	0.0%
Amounts involved in CHF					
(Total effective assets at time of report)					
Overall total	616'266'457	100.0%	-7.5%	666'468'023	100.0%
Total involved in reports passed on	614'741'199	99.8%	-4.9%	646'733'344	97.0%
Total involved in reports not passed on	1'525'258	0.2%	-92.3%	19'734'679	3.0%
Average report value (total)	714'098			1'022'190	
Average report value (passed on)	930'017			1'255'793	
Average report value (not passed on)	7'551			144'049	

2.3.2 Monthly statistics of incoming reports

What the graph represents

The graph shows the monthly distribution of incoming reports in 2002 und 2003.

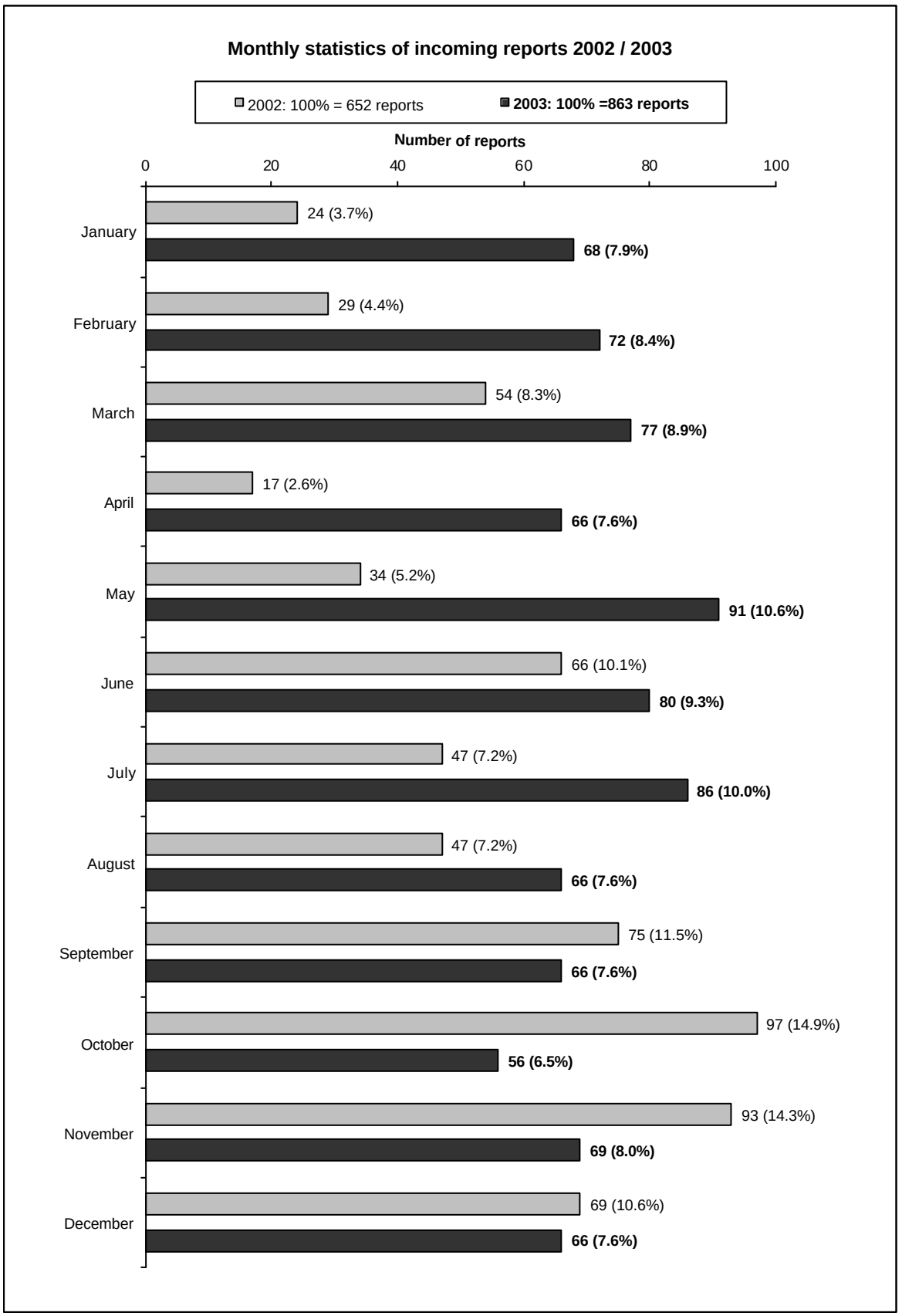
Graph analysis

In 2003, MROS processed an average of nearly 72 reports a month compared with a monthly figure of 54.3 reports in 2002. This is an average increase of 32.4%.

In 2003, a total of 863 reports were filed – a 32.4% increase over the 2002 reporting period.

In the first half of 2003 the average number of reports was almost 76 a month, while in the second half of the year the monthly average was slightly more than 68.

The slight drop in reports received in the second half of the year can be explained mainly by tighter business practices during the summer by a big dealer in financial transactions in the money transmitter sector. In the first half of the year, 56% of all reports came from this sector. In the second half of the year, the figure was 51%. Not including the reports from the money transmitter sector, the average number of reports filed monthly with the MROS was 33.5.


Monthly statistics of incoming reports 2002 / 2003
2002: 100% = 652 reports
2003: 100% =863 reports
Number of reports
0
20
40
60
80
100
January
24 (3.7%)
68 (7.9%)
February
29 (4.4%)
72 (8.4%)
March
54 (8.3%)
77 (8.9%)
April
17 (2.6%)
66 (7.6%)
May
34 (5.2%)
91 (10.6%)
June
66 (10.1%)
80 (9.3%)
July
47 (7.2%)
86 (10.0%)
August
47 (7.2%)
66 (7.6%)
September
75 (11.5%)
66 (7.6%)
October
97 (14.9%)
56 (6.5%)
November
93 (14.3%)
69 (8.0%)
December
69 (10.6%)
66 (7.6%)

2.3.3 Home canton of reporting financial intermediaries

What the graph represents

This graph shows in which cantons the reporting financial intermediaries who filed reports to MROS are based, as opposed to the graph „Law enforcement agencies involved“ (Graph 2.3.13), which indicates to which law enforcement agencies the reports were passed on.

Graph analysis

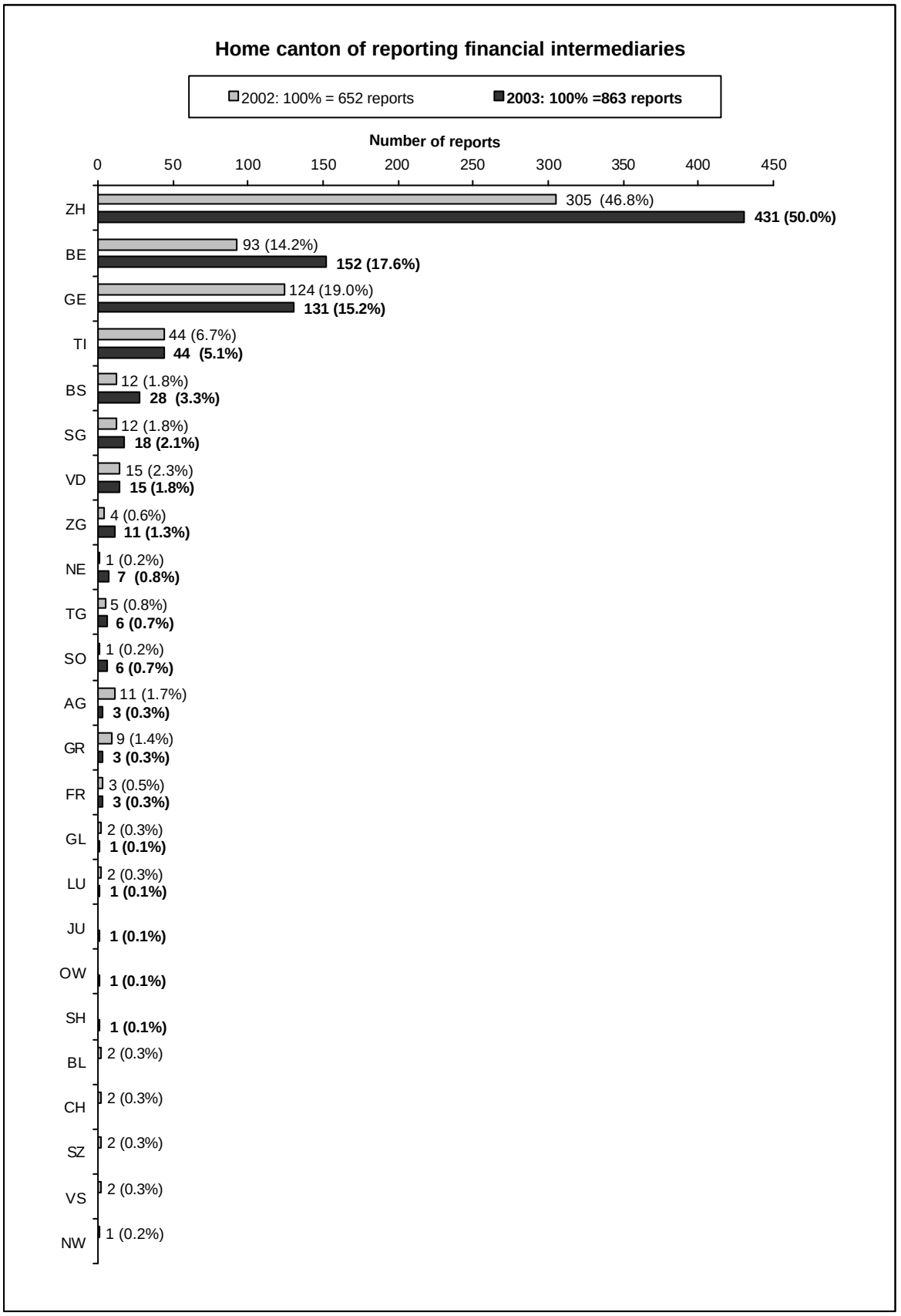
Another increase in reports from Zurich; Bern overtakes Geneva

As in previous years most of the reports (87.9%) in 2003 came from financial intermediaries in the cantons of Zurich, Bern, Geneva and Ticino. The canton of Zurich recorded another increase over the previous year. Half of all reports sent to MROS came from this canton. Canton Bern filed 152 reports giving it an overall share of 17.6% of the reports. For the first time, it moved into second place ahead of Canton Geneva, which filed 131 reports for a 15.2% share. The number of reports from Canton Ticino remained unchanged at 44. This notable shift towards cantons Zurich and Bern can be explained by the centralisation within companies of compliance sectors into so called competence centers in the cities of Zurich and Bern.

Only the half cantons of Appenzell Inner Rhoden and Ausser Rhoden and Canton Uri did not file reports to MROS in 2003.

Legend

AG	Aargau	GR	Grisons	TG	Thurgau
AI	Appenzell Inner Rhoden	JU	Jura	TI	Ticino
AR	Appenzell Ausser Rhoden	LU	Lucerne	UR	Uri
BE	Berne	NE	Neuchatel	VD	Vaud
BL	Basel-Land	NW	Nidwalden	VS	Valais
BS	Basel-Stadt	OW	Obwalden	ZG	Zug
CH	Money Laundering Control Authority	SG	St. Gallen	ZH	Zurich
FR	Fribourg	SH	Schaffhausen		
GE	Geneva	SO	Solothurn		
GL	Glarus	SZ	Schwyz		


Home canton of reporting financial intermediaries
2002: 100% = 652 reports
2003: 100% =863 reports
Number of reports
0
50
100
150
200
250
300
350
400
450
ZH
305 (46.8%)
431 (50.0%)
BE
93 (14.2%)
152 (17.6%)
GE
124 (19.0%)
131 (15.2%)
TI
44 (6.7%)
44 (5.1%)
BS
12 (1.8%)
28 (3.3%)
SG
12 (1.8%)
18 (2.1%)
VD
15 (2.3%)
15 (1.8%)
ZG
4 (0.6%)
11 (1.3%)
NE
1 (0.2%)
7 (0.8%)
TG
5 (0.8%)
6 (0.7%)
SO
1 (0.2%)
6 (0.7%)
AG
11 (1.7%)
3 (0.3%)
GR
9 (1.4%)
3 (0.3%)
FR
3 (0.5%)
3 (0.3%)
GL
2 (0.3%)
1 (0.1%)
LU
2 (0.3%)
1 (0.1%)
JU
1 (0.1%)
OW
1 (0.1%)
SH
1 (0.1%)
BL
2 (0.3%)
CH
2 (0.3%)
SZ
2 (0.3%)
VS
2 (0.3%)
NW
1 (0.2%)

2.3.4 Location of suspicious business connection

What the graph represents

The graph shows in which cantons the financial intermediary managed accounts or had business connections, which they reported to MROS in 2003. This is meant to be a complement to the previous *graph 2.3.3 showing the geographical origin (headquarters) of the reporting financial intermediary*.

Graph analysis

The place where a reporting financial intermediary has its headquarters is not a definite indication of the location of the account or business mentioned in the report.

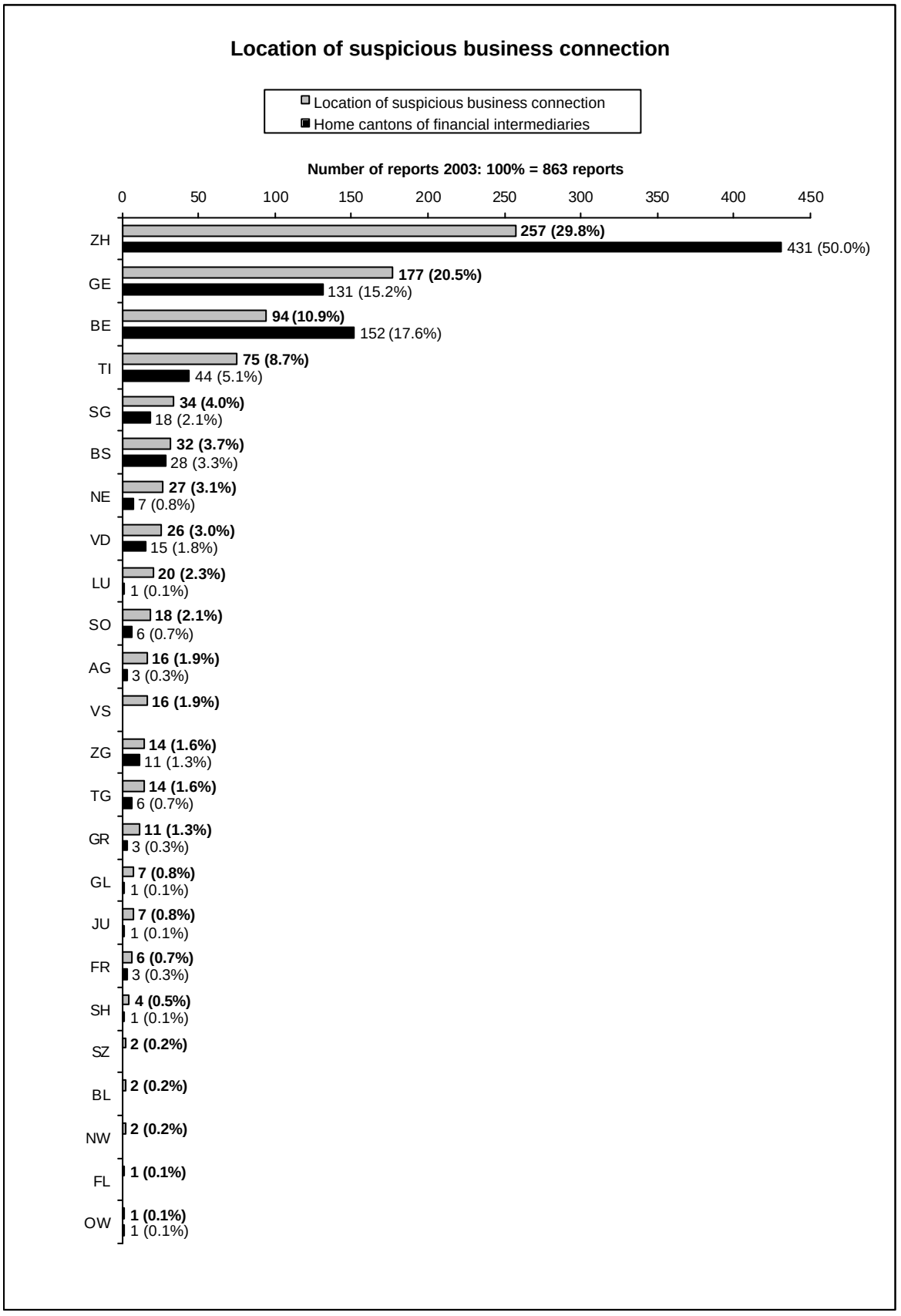
It is mainly the major banks and so-called money transmitters that have established regional competence centers to submit reports of suspicious activities although they do not involve only the home canton of the financial intermediary. This can lead to a distorted picture of the geographical distribution of money laundering cases in Switzerland. A direct comparison with the statistics of the law enforcement agencies involved (2.3.13) is not possible because, for one thing, not all cases are passed on and, for another, as a result of federal jurisdiction in certain cases the location of the account or business alone no longer determines which judicial authority is responsible.

In the case of cantons Zurich and Bern, it can be seen that 50% and 17.6% respectively of the reports sent to MROS come from these cantons, although only in 29.8% or 10.9% of the cases did the reported business connection take place in the canton itself. The cantons of Geneva and Ticino had precisely the reverse situation.

As expected, the trends shown in these statistics, which appeared for the first time in the 2002 annual report, were confirmed in 2003.

Legend

AG	Aargau	GR	Grisons	TG	Thurgau
AI	Appenzell Inner Rhoden	JU	Jura	TI	Ticino
AR	Appenzell Ausser Rhoden	LU	Lucerne	UR	Uri
BE	Berne	NE	Neuchatel	VD	Vaud
BL	Basel-Land	NW	Nidwalden	VS	Valais
BS	Basel-Stadt	OW	Obwalden	ZG	Zug
CH	Money Laundering Control Authority	SG	St. Gallen	ZH	Zurich
FR	Fribourg	SH	Schaffhausen		
GE	Geneva	SO	Solothurn		
GL	Glarus	SZ	Schwyz		


Location of suspicious business connection
Location of suspicious business connection
Home cantons of financial intermediaries
Number of reports 2003: 100% = 863 reports
0
50
100
150
200
250
300
350
400
450
ZH
257 (29.8%)
431 (50.0%)
GE
177 (20.5%)
131 (15.2%)
BE
94 (10.9%)
152 (17.6%)
TI
75 (8.7%)
44 (5.1%)
SG
34 (4.0%)
18 (2.1%)
BS
32 (3.7%)
28 (3.3%)
NE
27 (3.1%)
7 (0.8%)
VD
26 (3.0%)
15 (1.8%)
LU
20 (2.3%)
1 (0.1%)
SO
18 (2.1%)
6 (0.7%)
AG
16 (1.9%)
3 (0.3%)
VS
16 (1.9%)
ZG
14 (1.6%)
11 (1.3%)
TG
14 (1.6%)
6 (0.7%)
GR
11 (1.3%)
3 (0.3%)
GL
7 (0.8%)
1 (0.1%)
JU
7 (0.8%)
1 (0.1%)
FR
6 (0.7%)
3 (0.3%)
SH
4 (0.5%)
1 (0.1%)
SZ
2 (0.2%)
BL
2 (0.2%)
NW
2 (0.2%)
FL
1 (0.1%)
OW
1 (0.1%)
1 (0.1%)

2.3.5 Financial intermediaries according to category

What the graph represents

This graph illustrates which category of financial intermediary filed how many reports.

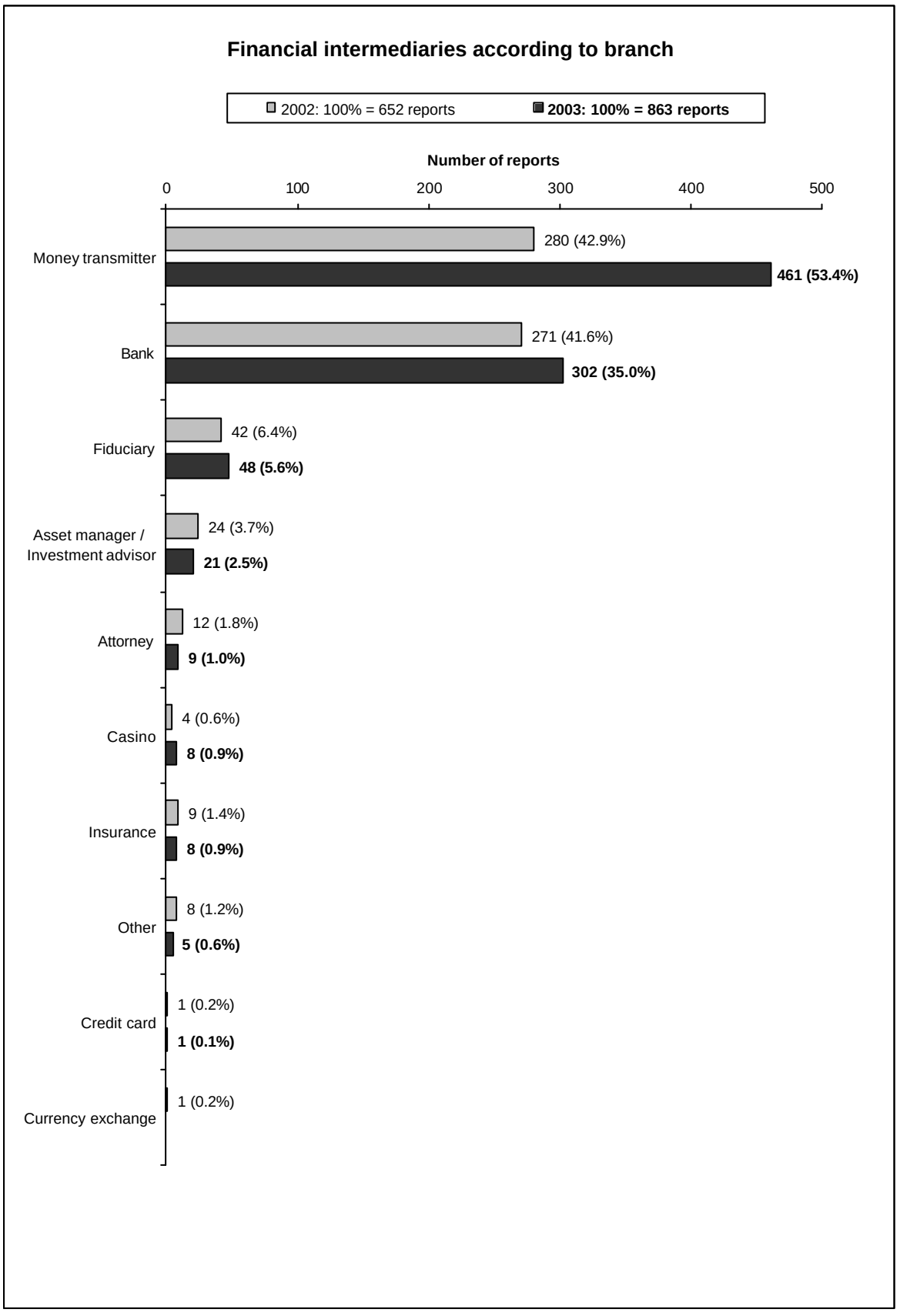
Graph analysis

Sectoral shift confirmed: another increase in reporting by the money transmitter sector stands in contrast to a proportionate decline in reports by the banking and remaining non-banking sector.

For the second year running since the introduction of the Money Laundering Act, banks did not file the most reports in a reporting year. Again it was the financial intermediaries from the money transmitter sector with 53.4% of reports. Although not as great as the 400% increase between 2001 and 2002, there was a 64.6% increase in reports in 2003. This can be explained by the stricter reporting practices of money transmitters. In addition, they also made more frequent use of the reporting option under Art. 305ter, par. 2 of the Swiss Penal Code and reported transactions they had refused.

In view of the sectoral shift, the banking sector showed a relative decline in reports compared with 2002. But if one looks at the absolute figures, there was an increase of reports filed by the banking sector in 2003 to 302 compared with 271 in 2002.

In the rest of the non-banking sector (excluding money transmitters), the total number of reports accounted for 11.6% of all reports compared with 25.6% and 15.5% for the 2001 and 2002 reporting periods respectively. Absolute figures show a slight drop of 1% in this sector from the previous year. Looking back it is somewhat surprising that insurance companies and attorneys who act as financial intermediaries file so few reports of suspicious activities to MROS.


Financial intermediaries according to branch
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
100
200
300
400
500
Money transmitter
280 (42.9%)
461 (53.4%)
Bank
271 (41.6%)
302 (35.0%)
Fiduciary
42 (6.4%)
48 (5.6%)
Asset manager / Investment advisor
24 (3.7%)
21 (2.5%)
Attorney
12 (1.8%)
9 (1.0%)
Casino
4 (0.6%)
8 (0.9%)
Insurance
9 (1.4%)
8 (0.9%)
Other
8 (1.2%)
5 (0.6%)
Credit card
1 (0.2%)
1 (0.1%)
Currency exchange
1 (0.2%)

2.3.6 Type of bank reporting

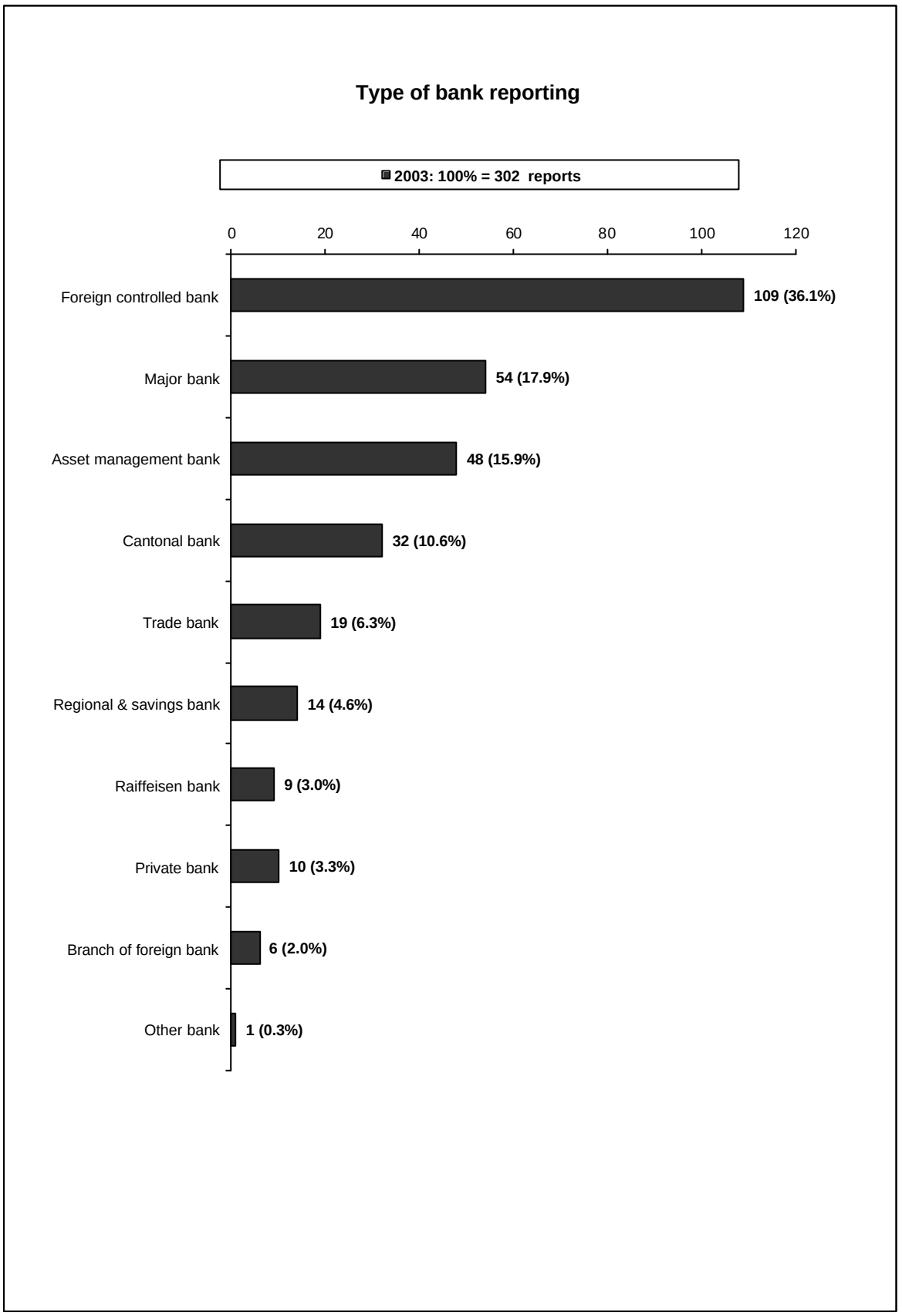
What the graph represents

This graph shows what type of bank submitted reports in 2003 and how many.

Graph analysis

Please note that these statistics can no longer be used freely for comparisons with previous reporting periods because, since 1 January 2003, the statistics have been based on the categories and their definitions according to the reference list of the Swiss National Bank.

In 2003, the financial institutions in the category foreign controlled banks submitted the most reports with 36.1% of the total. In second place were the major banks with 17.9% and in third place were the asset management banks with 15.9%. Reports by the cantonal banks accounted for 10.6% of the total.


Type of bank reporting
2003: 100% = 302 reports
0
20
40
60
80
100
120
Foreign controlled bank
109 (36.1%)
Major bank
54 (17.9%)
Asset management bank
48 (15.9%)
Cantonal bank
32 (10.6%)
Trade bank
19 (6.3%)
Regional & savings bank
14 (4.6%)
Raiffeisen bank
9 (3.0%)
Private bank
10 (3.3%)
Branch of foreign bank
6 (2.0%)
Other bank
1 (0.3%)

2.3.7 Factors arousing suspicion

What the graph represents

This graph shows what suspicions prompted a financial intermediary to file a report.

Graph analysis

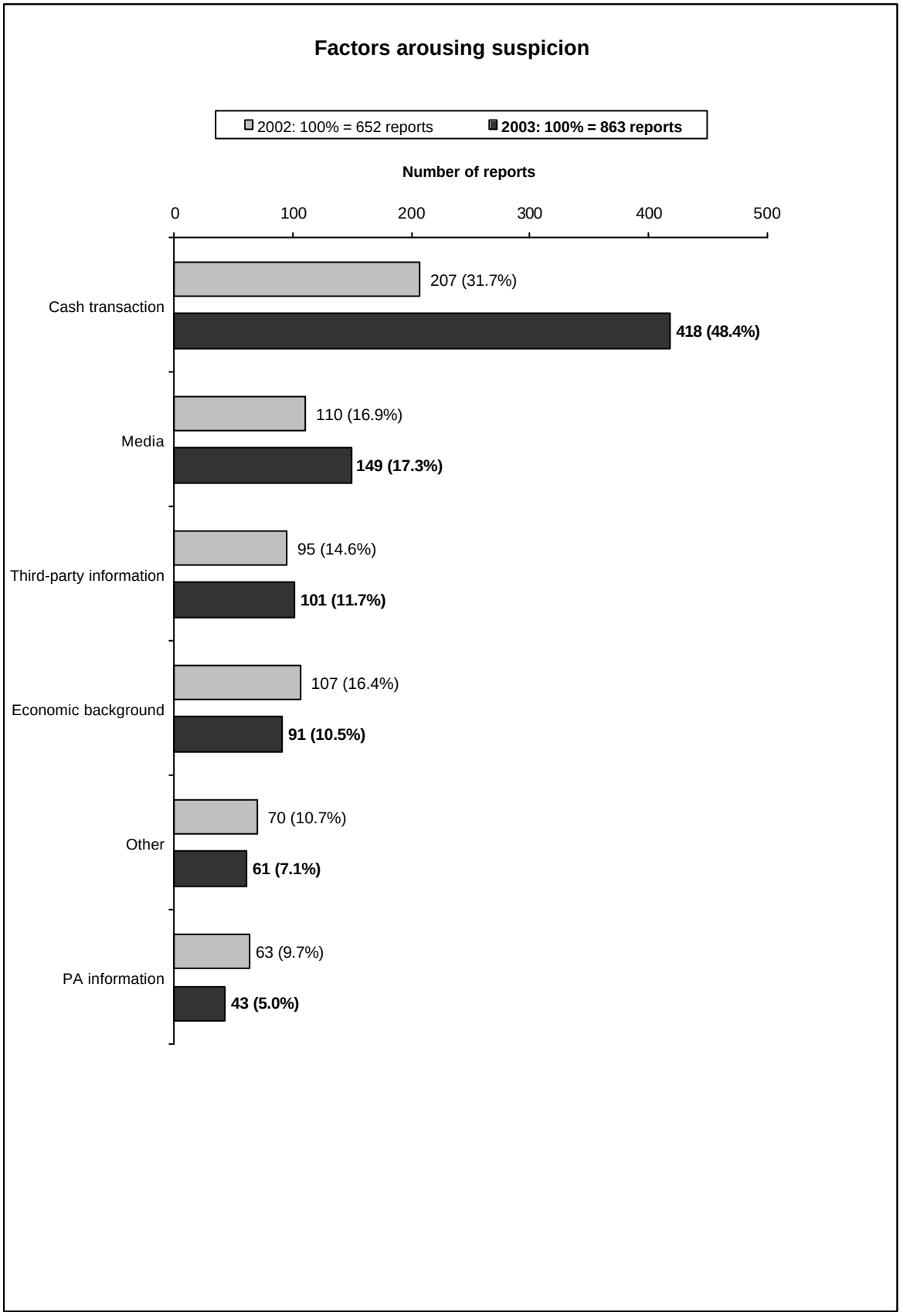
Financial intermediaries are making a critical analysis of their business relations.

Corresponding to the continued increase in the number of reports from the money transmitter sector, suspicious cash transactions were once again clearly at the top in the 2003 reporting period.

Excluding the money transmitter cases, the media was again the main source of most reports.

Legend

Economic background	The economic background of a transaction is either unclear or cannot be satisfactorily explained by the customer.
PA information	Law enforcement agencies initiate proceedings against an individual connected with the financial intermediary's client.
Media	The financial intermediary finds out from media reports that one of the people involved in the financial transaction is connected with illegal activities.
Third-party information	Financial intermediaries receive information from outside sources or from within a business about clients who could pose problems.
Various	Included in this category are topics which were listed separately in previous MROS statistics such as check transactions, forgery, high-risk countries, currency exchange, securities, smurfing, life insurance, non-cash cashier transactions, fiduciary transactions, loan transactions, transitory accounts, precious metals, opening of accounts.


Factors arousing suspicion
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
100
200
300
400
500
Cash transaction
207 (31.7%)
418 (48.4%)
Media
110 (16.9%)
149 (17.3%)
Third-party information
95 (14.6%)
101 (11.7%)
Economic background
107 (16.4%)
91 (10.5%)
Other
70 (10.7%)
61 (7.1%)
PA information
63 (9.7%)
43 (5.0%)

2.3.8 Nature of predicate offence

What the graph represents

This graph shows what predicate offence was suspected when MROS passed on a report to law enforcement agencies.

It should be noted that the classification is based solely on the findings of the financial intermediary and MROS. Once a report is passed on to a law enforcement agency and proceedings are initiated, the predicate offence is then given a definite label.

The category *not classifiable* includes cases in which a variety of possible predicate offences are suspected. The heading *no suspicion* includes those cases to which no obvious predicate offence can be attributed, although the analysis of the transaction or of the economic background cannot exclude the criminal origin of the money.

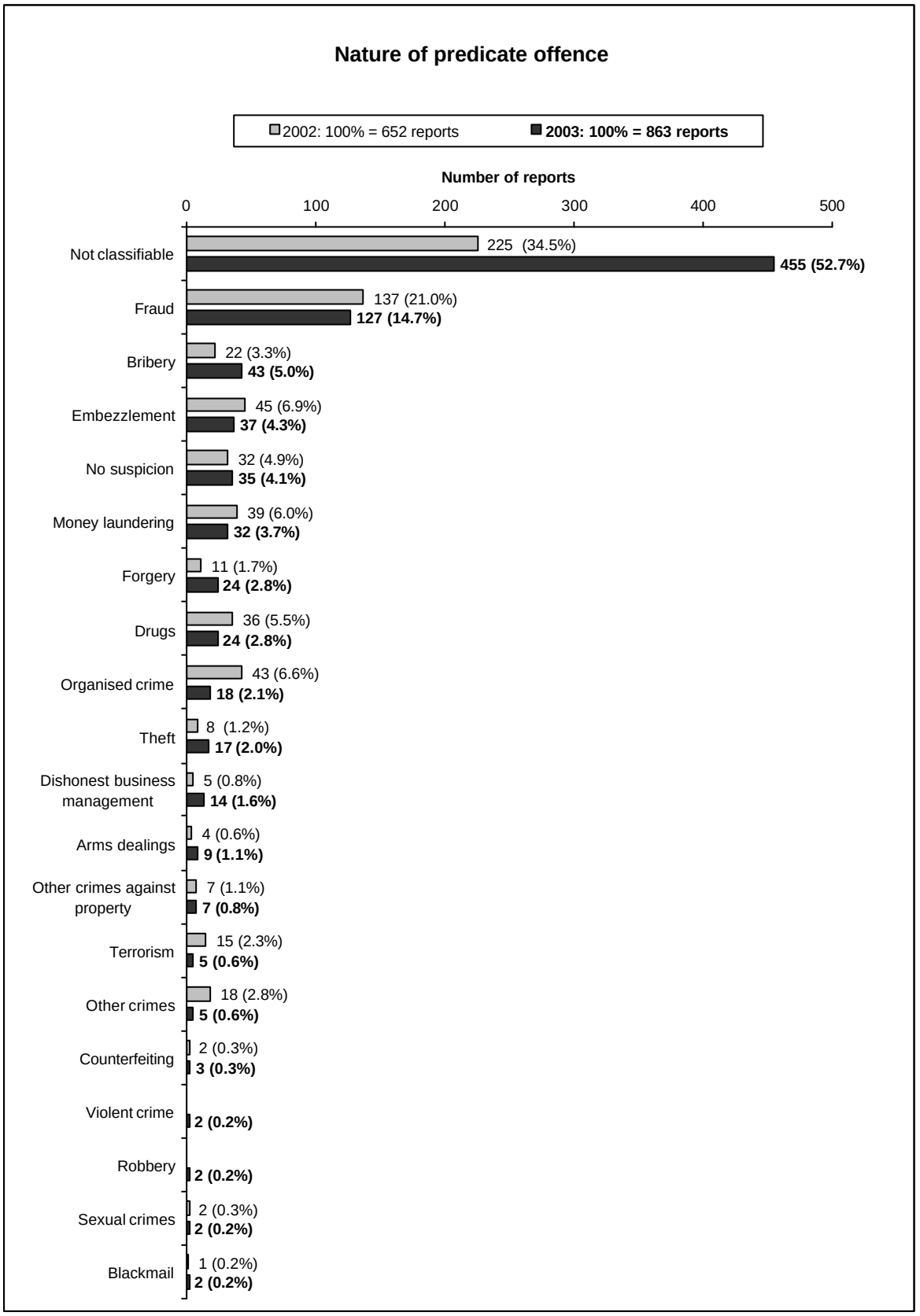
Graph analysis

Increase in bribery cases; fewer cases involving organised crime and terrorism

Of those cases reported to MROS during 2003 that could be classified mainly as predicate offences on the basis of the facts there was an increase in bribery cases (43 from 22) and a notable decrease in cases involving organised crime (18 from 43) over the previous year. There was also an increase in cases involving forgery (24 from 11), theft (17 from 8), dishonest business management (14 from 5) and arms trafficking (9 from 4).

In the 2002 and 2001 annual reports, cases involving the financing of terrorism as a predicate offence came to 2.3% and 22.8% respectively. In 2003 however the reports in this category came to just 0.6% of the total.

As in 2002, there was a clear increase in the 2003 reporting period in cases which could *not be classified* as definite predicate offences or to which no obvious predicate offence could be attributed. This can be explained mainly by the fact that in the money transmitter sector, which showed a massive increase in reports (461 from 280 in 2002), transactions should have been classified as suspicious on the basis of the customer profile or the receiver country although there was no obvious predicate offence.


Nature of predicate offence
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
100
200
300
400
500
Not classifiable
225 (34.5%)
455 (52.7%)
Fraud
137 (21.0%)
127 (14.7%)
Bribery
22 (3.3%)
43 (5.0%)
Embezzlement
45 (6.9%)
37 (4.3%)
No suspicion
32 (4.9%)
35 (4.1%)
Money laundering
39 (6.0%)
32 (3.7%)
Forgery
11 (1.7%)
24 (2.8%)
Drugs
36 (5.5%)
24 (2.8%)
Organised crime
43 (6.6%)
18 (2.1%)
Theft
8 (1.2%)
17 (2.0%)
Dishonest business management
5 (0.8%)
14 (1.6%)
Arms dealings
4 (0.6%)
9 (1.1%)
Other crimes against property
7 (1.1%)
7 (0.8%)
Terrorism
15 (2.3%)
5 (0.6%)
Other crimes
18 (2.8%)
5 (0.6%)
Counterfeiting
2 (0.3%)
3 (0.3%)
Violent crime
2 (0.2%)
Robbery
2 (0.2%)
Sexual crimes
2 (0.3%)
2 (0.2%)
Blackmail
1 (0.2%)
2 (0.2%)

2.3.9 Domicile of clients

What the graph represents

This graph shows the domiciles of the corporations or individuals who were customers of the financial intermediary.

Graph analysis

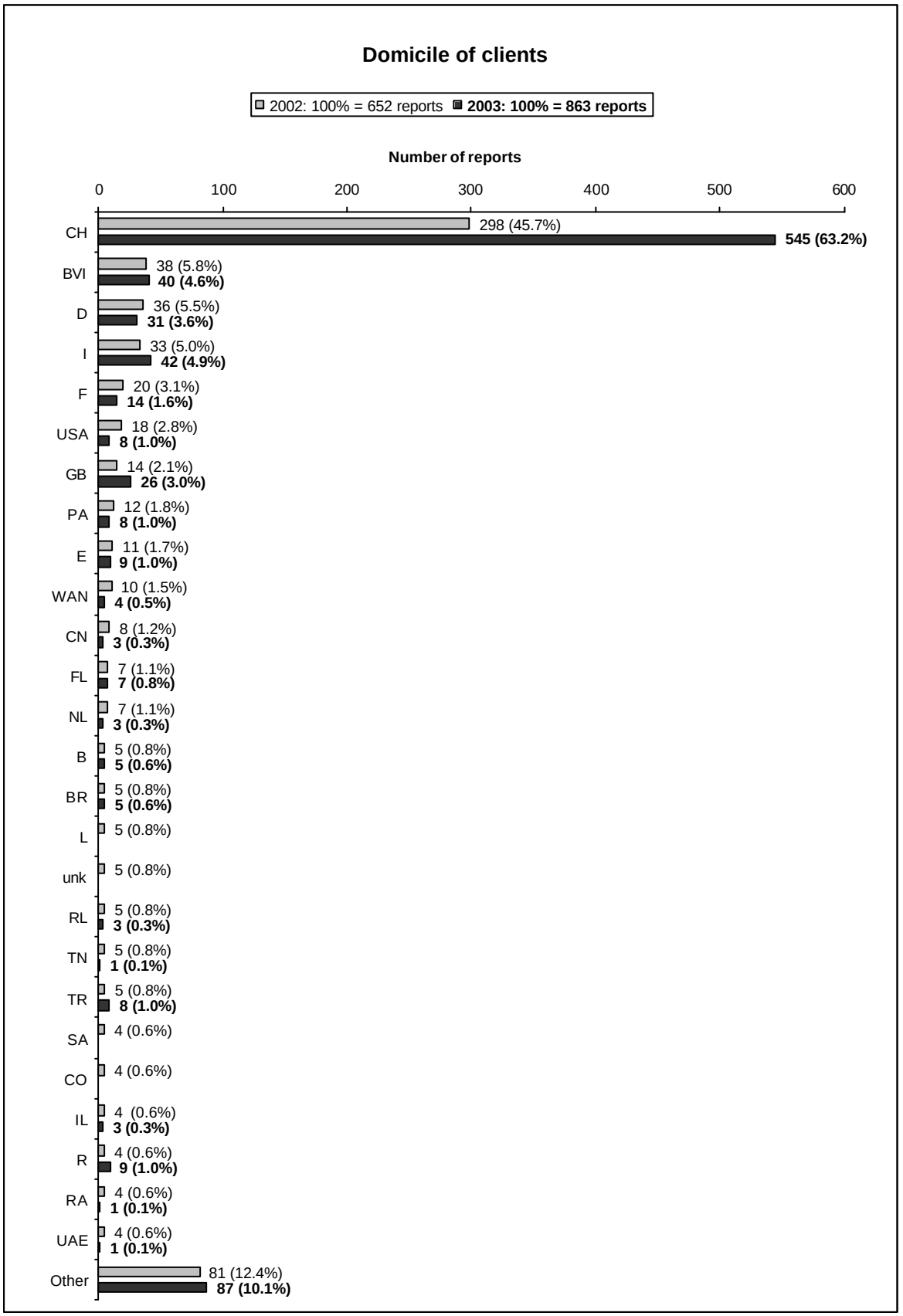
There was a further increase in the number of clients domiciled in Switzerland who were directly involved in a report.

In the 2003 reporting period, 79% of the clients came from western, central or southern European countries. Compared with 2002, this is an increase from 436 clients reported from this geographical area to 682 in 2003. As in previous years, Switzerland is named as the country of residence or domicile of these clients. This is attributable mainly to the fact that an increasing number of reports from the money transmitter sector involved mostly clients who were resident in Switzerland. In 2003 this came to 88.5% of the money transmitter cases.

Accompanying the drop in reports relating to possible financing of terrorism, was a decline in the cases involving clients from Saudi Arabia.

Legend

Other	Countries not geographically classified
unk	Domicile of client unknown
B	Belgium
BR	Brazil
BVI	British Virgin Islands
CH	Switzerland
CN	People's Republic of China
CO	Columbia
D	Germany
E	Spain
F	France
FL	Liechtenstein
GB	Great Britain
I	Italy
IL	Israel
NL	The Netherlands
PA	Panama
R	Russia
RL	Lebanon
SA	Saudi Arabia
TN	Tunisia
TR	Turkey
UAE	United Arab Emirates
USA	USA
WAN	Nigeria


Domicile of clients
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
100
200
300
400
500
600
CH
298 (45.7%)
545 (63.2%)
BVI
38 (5.8%)
40 (4.6%)
D
36 (5.5%)
31 (3.6%)
I
33 (5.0%)
42 (4.9%)
F
20 (3.1%)
14 (1.6%)
USA
18 (2.8%)
8 (1.0%)
GB
14 (2.1%)
26 (3.0%)
PA
12 (1.8%)
8 (1.0%)
E
11 (1.7%)
9 (1.0%)
WAN
10 (1.5%)
4 (0.5%)
CN
8 (1.2%)
3 (0.3%)
FL
7 (1.1%)
7 (0.8%)
NL
7 (1.1%)
3 (0.3%)
B
5 (0.8%)
5 (0.6%)
BR
5 (0.8%)
5 (0.6%)
L
5 (0.8%)
unk
5 (0.8%)
RL
5 (0.8%)
3 (0.3%)
TN
5 (0.8%)
1 (0.1%)
TR
5 (0.8%)
8 (1.0%)
SA
4 (0.6%)
CO
4 (0.6%)
IL
4 (0.6%)
3 (0.3%)
R
4 (0.6%)
9 (1.0%)
RA
4 (0.6%)
1 (0.1%)
UAE
4 (0.6%)
1 (0.1%)
Other
81 (12.4%)
87 (10.1%)

2.3.10 Nationality of clients

What the graph represents

This graph shows the nationality of individuals who were clients of the financial intermediary. In the case of corporations, domicile and nationality are the same.

Graph analysis

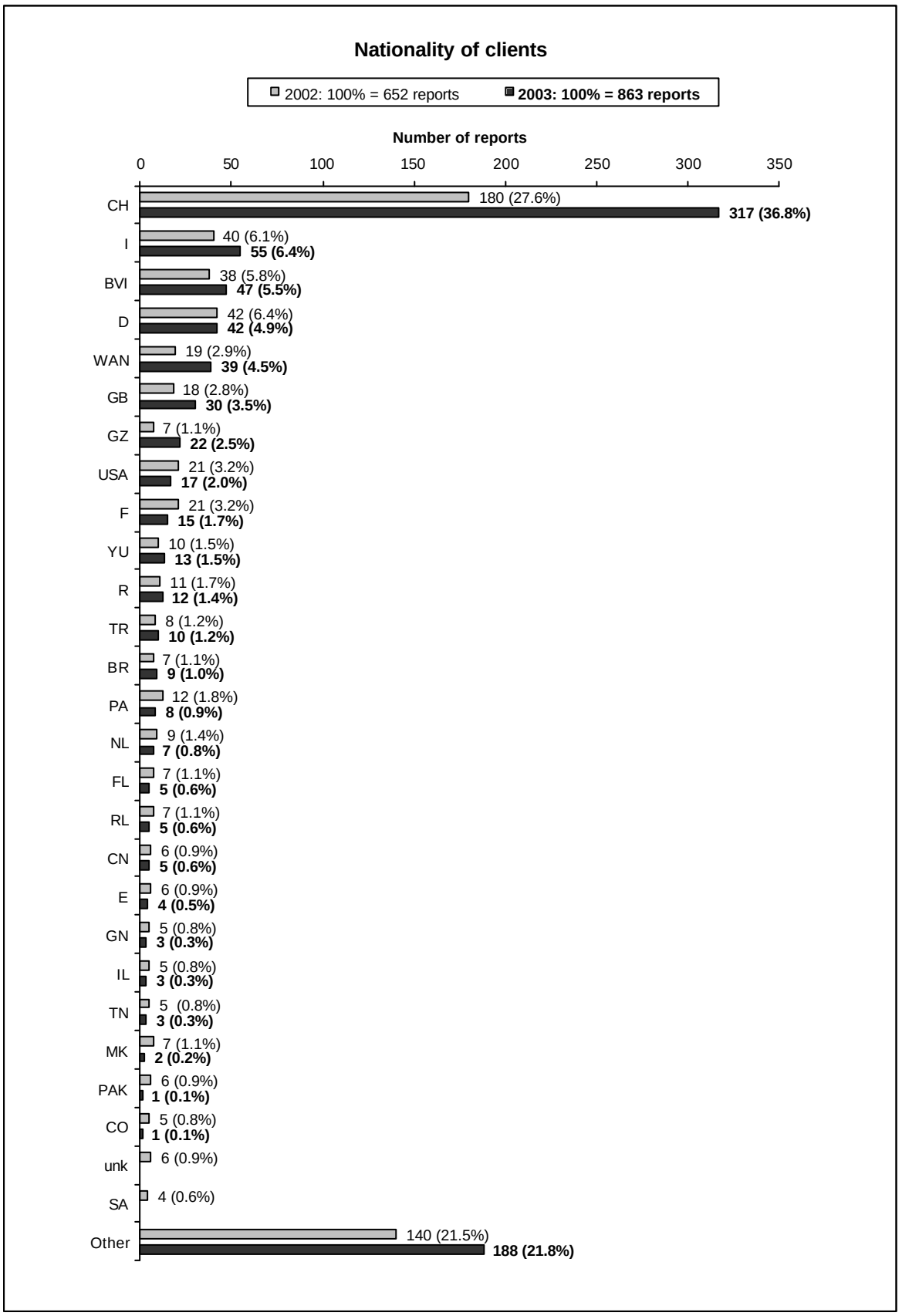
Cases involving individuals with Swiss nationality or whose firms are based in Switzerland continued to increase.

Once again, clients with Swiss passports or with companies with headquarters in Switzerland are at the top of the table in 2003 with 36.8% of the total. This can also be traced back to the continuing increase in reports from the money transmitter sector where more than 46% of the clients have Swiss nationality or are domiciled in Switzerland.

In 2003, a total of 55.2% of clients named in the reports came from western, central and southern Europe.

Legend

Other	Countries not geographically classified	I	Italy
unk	Domicile of client unknown	IL	Israel
BR	Brazil	MK	Macedonia
BVI	British Virgin Islands	NL	The Netherlands
CH	Switzerland	PA	Panama
CN	People's Republic of China	PAK	Pakistan
CO	Columbia	R	Russia
D	Germany	RL	Lebanon
E	Spain	SA	Saudi Arabia
F	France	TN	Tunisia
FL	Liechtenstein	TR	Turkey
GB	Great Britain	USA	USA
GN	Guinea	WAN	Nigeria
GZ	Georgia	YU	former Yugoslavia


Nationality of clients
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
50
100
150
200
250
300
350
CH
180 (27.6%)
317 (36.8%)
I
40 (6.1%)
55 (6.4%)
BVI
38 (5.8%)
47 (5.5%)
D
42 (6.4%)
42 (4.9%)
WAN
19 (2.9%)
39 (4.5%)
GB
18 (2.8%)
30 (3.5%)
GZ
7 (1.1%)
22 (2.5%)
USA
21 (3.2%)
17 (2.0%)
F
21 (3.2%)
15 (1.7%)
YU
10 (1.5%)
13 (1.5%)
R
11 (1.7%)
12 (1.4%)
TR
8 (1.2%)
10 (1.2%)
BR
7 (1.1%)
9 (1.0%)
PA
12 (1.8%)
8 (0.9%)
NL
9 (1.4%)
7 (0.8%)
FL
7 (1.1%)
5 (0.6%)
RL
7 (1.1%)
5 (0.6%)
CN
6 (0.9%)
5 (0.6%)
E
6 (0.9%)
4 (0.5%)
GN
5 (0.8%)
3 (0.3%)
IL
5 (0.8%)
3 (0.3%)
TN
5 (0.8%)
3 (0.3%)
MK
7 (1.1%)
2 (0.2%)
PAK
6 (0.9%)
1 (0.1%)
CO
5 (0.8%)
1 (0.1%)
unk
6 (0.9%)
SA
4 (0.6%)
Other
140 (21.5%)
188 (21.8%)

2.3.11 Domicile of beneficial owners

What the graph represents

This graph shows the domicile of the individuals or corporations who were identified as beneficial owners of assets when the report was filed.

Graph analysis

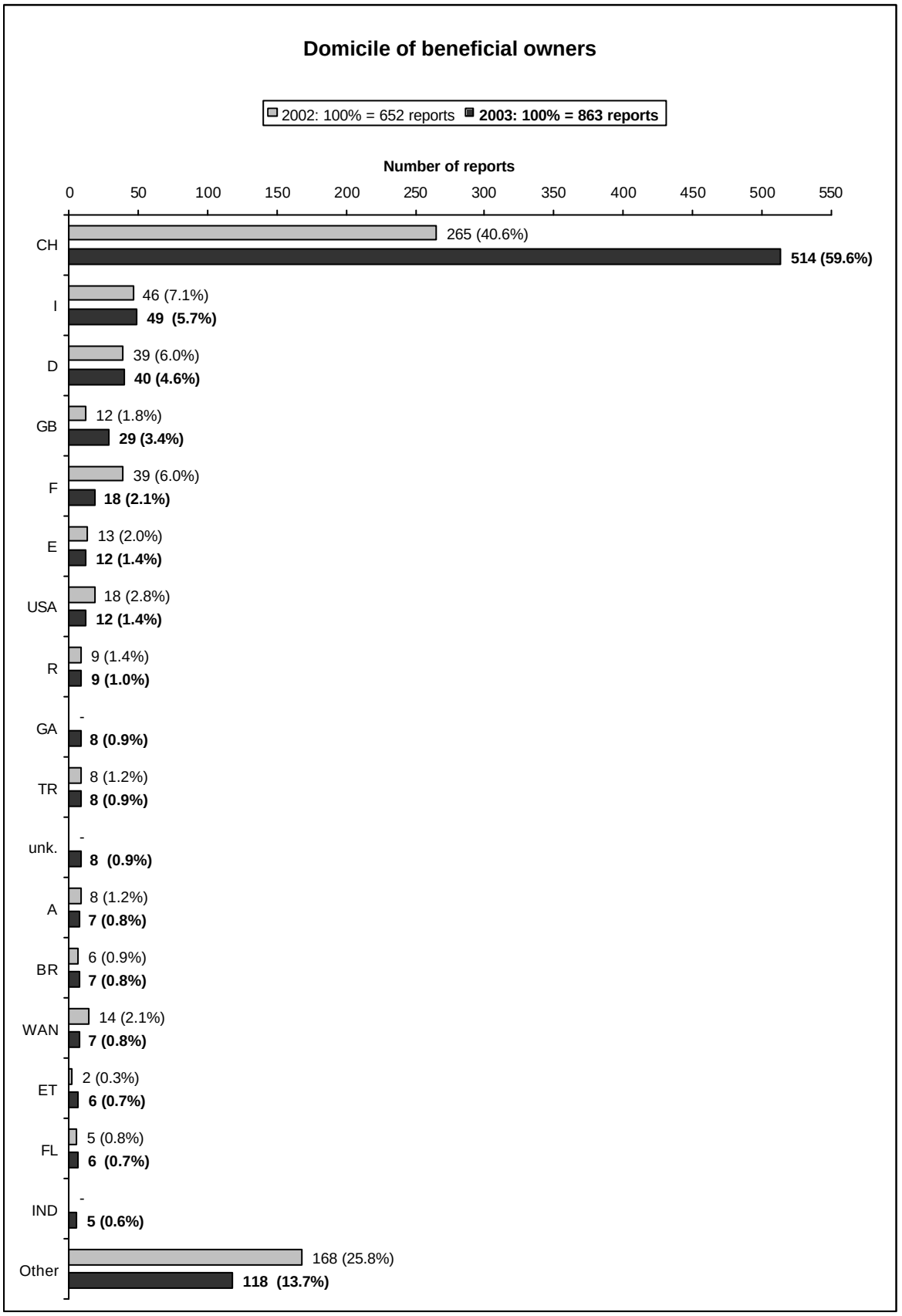
The number of beneficial owners domiciled in Switzerland increased once again.

In 2003, 78.3% of the reports submitted to MROS involved individuals identified as beneficial owners who were resident in western, central or southern Europe. This is an increase over 2002.

As with the statistics under the section *Domicile of clients*, the number of individuals from Switzerland topped the list of beneficial owners with 59.6% of the total. Again, this increase can be attributed to the increase in reports by Swiss-based financial intermediaries in the money transmitter sector. In 86% of the cases the beneficial owner was an individual residing in Switzerland.

Legend

Other	Countries not geographically classified	I	Italy
unk	Insufficient identification	IL	Israel
A	Austria	L	Luxembourg
AZ	Azerbaijan	NL	The Netherlands
B	Belgium	R	Russia
BR	Brazil	RA	Argentina
CH	Switzerland	RL	Lebanon
CN	People's Republic of China	SA	Saudi Arabia
CO	Columbia	TN	Tunisia
D	Germany	TR	Turkey
E	Spain	UAE	United Arab Emirates
F	France	USA	USA
FL	Liechtenstein	WAN	Nigeria
GB	Great Britain	YU	former Yugoslavia
GZ	Georgia		


Domicile of beneficial owners
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
50
100
150
200
250
300
350
400
450
500
550
CH
265 (40.6%)
514 (59.6%)
I
46 (7.1%)
49 (5.7%)
D
39 (6.0%)
40 (4.6%)
GB
12 (1.8%)
29 (3.4%)
F
39 (6.0%)
18 (2.1%)
E
13 (2.0%)
12 (1.4%)
USA
18 (2.8%)
12 (1.4%)
R
9 (1.4%)
9 (1.0%)
GA
-
8 (0.9%)
TR
8 (1.2%)
8 (0.9%)
unk.
-
8 (0.9%)
A
8 (1.2%)
7 (0.8%)
BR
6 (0.9%)
7 (0.8%)
WAN
14 (2.1%)
7 (0.8%)
ET
2 (0.3%)
6 (0.7%)
FL
5 (0.8%)
6 (0.7%)
IND
-
5 (0.6%)
Other
168 (25.8%)
118 (13.7%)

2.3.12 Nationality of beneficial owners

What the graph represents

This graph shows the nationality of those individuals who were identified as beneficial owners of assets when the report was submitted. With corporations, nationality is the same as domicile. Frequently, however, it is only during the investigations by the law enforcement authority that the actual beneficial owners and their nationality are identified.

Graph analysis

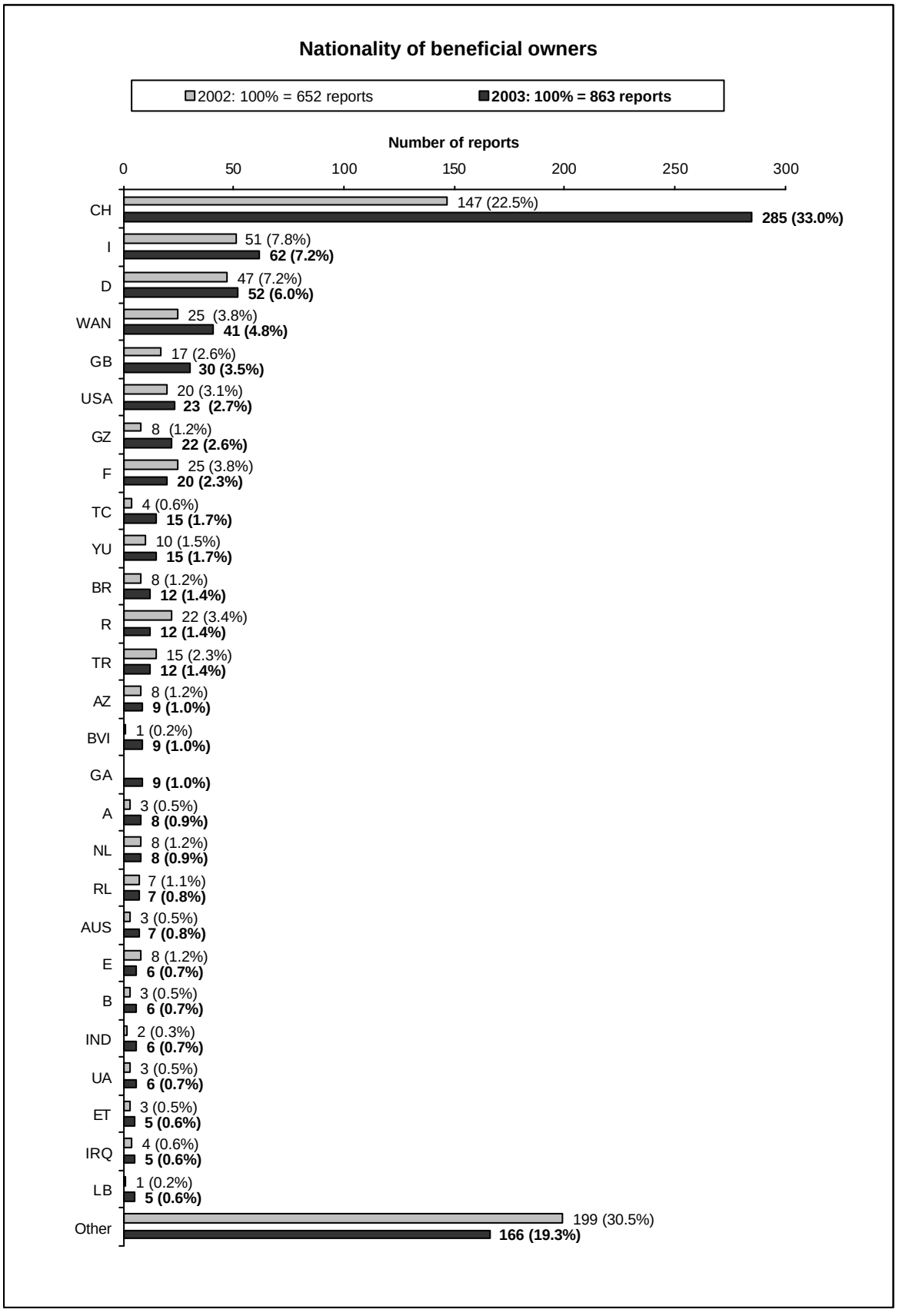
In more than half of the cases, beneficial owners consisted of nationalities from western, central and southern Europe.

Individuals with nationalities from western, central and southern Europe continued to dominate the MROS list of beneficial owners with 55.2% of the total. Individuals with Swiss nationality lead this group with 33%, followed by Italians and Germans with 7.2% and 6% respectively and Nigerians with 4.8%.

Slightly more than 16% of the beneficial owners are of African nationality. This can be explained mainly by the number of reports from financial intermediaries in the money transmitter sector of transactions which were either carried out or refused.

Legend

Other	Countries not geographically classified	GZ	Georgia
unk	Insufficient identification	I	Italy
AO	Angola	IL	Israel
AZ	Azerbaijan	L	Luxembourg
BR	Brazil	MK	Macedonia
CH	Switzerland	NL	The Netherlands
CN	People's Republic of China	PAK	Pakistan
CO	Columbia	R	Russia
D	Germany	RL	Lebanon
E	Spain	SA	Saudi Arabia
F	France	TN	Tunisia
FL	Liechtenstein	TR	Turkey
GB	Great Britain	USA	USA
GN	Guinea	WAN	Nigeria
GR	Greece	YU	former Yugoslavia


Nationality of beneficial owners
2002: 100% = 652 reports
2003: 100% = 863 reports
Number of reports
0
50
100
150
200
250
300
CH
147 (22.5%)
285 (33.0%)
I
51 (7.8%)
62 (7.2%)
D
47 (7.2%)
52 (6.0%)
WAN
25 (3.8%)
41 (4.8%)
GB
17 (2.6%)
30 (3.5%)
USA
20 (3.1%)
23 (2.7%)
GZ
8 (1.2%)
22 (2.6%)
F
25 (3.8%)
20 (2.3%)
TC
4 (0.6%)
15 (1.7%)
YU
10 (1.5%)
15 (1.7%)
BR
8 (1.2%)
12 (1.4%)
R
22 (3.4%)
12 (1.4%)
TR
15 (2.3%)
12 (1.4%)
AZ
8 (1.2%)
9 (1.0%)
BVI
1 (0.2%)
9 (1.0%)
GA
9 (1.0%)
A
3 (0.5%)
8 (0.9%)
NL
8 (1.2%)
8 (0.9%)
RL
7 (1.1%)
7 (0.8%)
AUS
3 (0.5%)
7 (0.8%)
E
8 (1.2%)
6 (0.7%)
B
3 (0.5%)
6 (0.7%)
IND
2 (0.3%)
6 (0.7%)
UA
3 (0.5%)
6 (0.7%)
ET
3 (0.5%)
5 (0.6%)
IRQ
4 (0.6%)
5 (0.6%)
LB
1 (0.2%)
5 (0.6%)
Other
199 (30.5%)
166 (19.3%)

2.3.13 Law enforcement agencies

What the graph represents

This graph shows to which law enforcement agency MROS passed on its reports. The general regulations on the court of jurisdiction and Art. 340bis of the Penal Code determine which federal agency is responsible.

Graph analysis

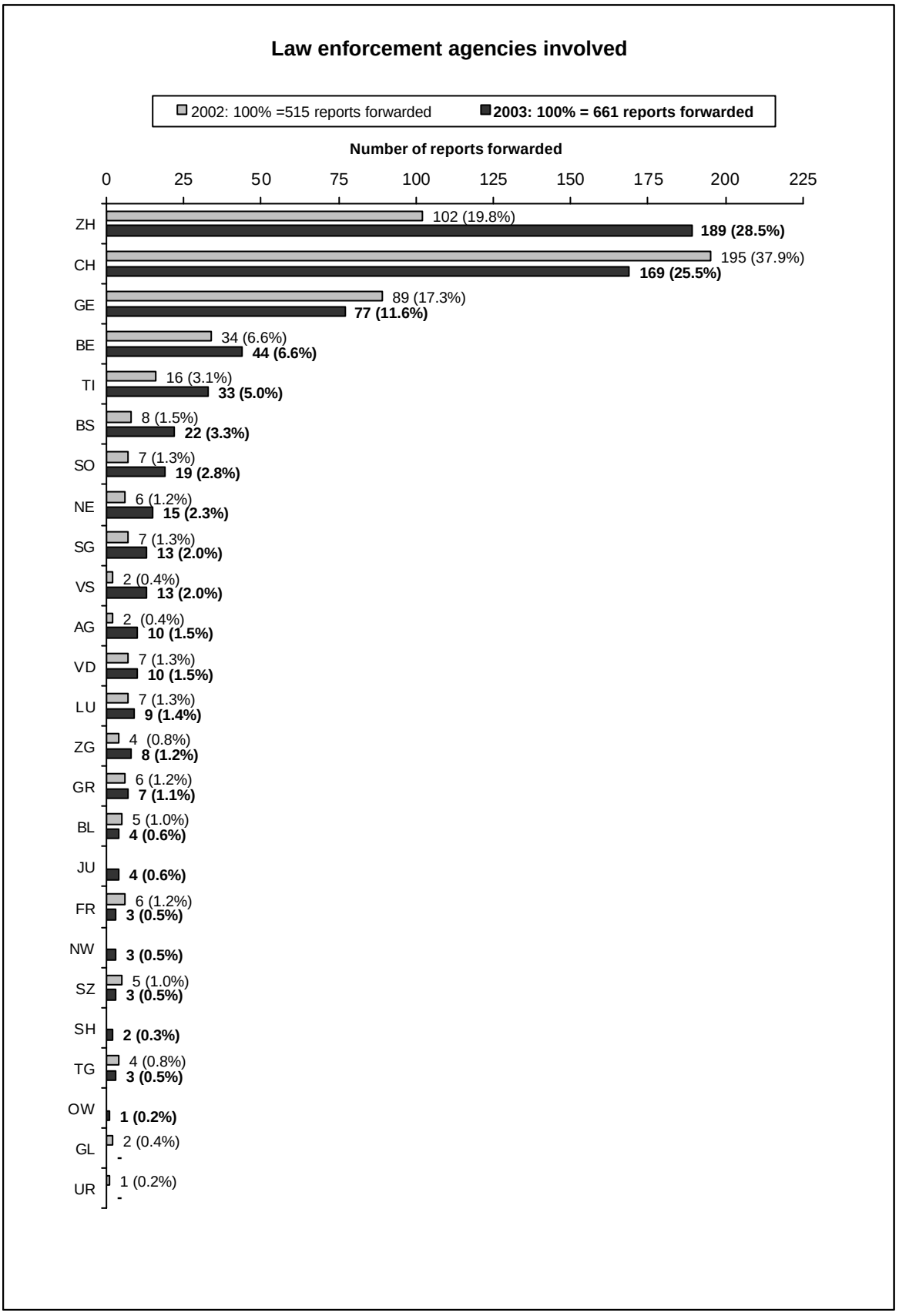
No lightening in workload for law enforcement authorities of Canton Zurich; a slight easing for federal prosecutors.

Under Art. 340bis, the offices of the Attorney General of Switzerland and the Federal Examining Magistrates are responsible for prosecuting cases involving money laundering, corruption and organised crime, which have mainly a foreign connection or where the offence in Switzerland involves several cantons. In 2002, MROS passed on 195 or 37.9% of reports to the Attorney General's office. Last year, the figure was 169 or 25.5%. In this context, the number of reports concerning suspicions of terrorist financing also decreased with only five reports or 0.6% sent to the Attorney General. By contrast 2003 was marked by an increase in cases handled by law enforcement authorities in Canton Zurich. In 2002, 102 or 19.8% of all reports passed on were transferred to the Zurich District Attorney General. But in 2003 the figure rose sharply to 189 or 28.5%. As in 2001 and 2002 in Canton Geneva, there were fewer cases passed on to the law enforcement authorities. In 2001 and 2002 the rate was 29.7% and 17.3% of all cases. In 2003 that figure dropped to 11.6%. The law enforcement authorities in the half cantons of Appenzell Inner Rhoden and Ausser Rhoden handled no reports.

It is too early to see clear tendencies in these figures because cases which would have actually come under federal jurisdiction were transferred to the cantons where proceedings in a related case were pending. The enormous increase in reports from the money transmitter sector also influenced these statistics. These often simple cases usually come under cantonal jurisdiction.

Legend

AG	Aargau
AI	Appenzell Inner Rhoden
AR	Appenzell Ausser Rhoden
BE	Berne
BL	Basel-Land
BS	Basel-Stadt
CH	Switzerland
FR	Fribourg
GE	Geneva
GL	Glarus
GR	Grisons
JU	Jura
LU	Lucerne
NE	Neuchatel
NW	Nidwalden
OW	Obwalden
SG	St. Gallen
SH	Schaffhausen
SO	Solothurn
SZ	Schwyz
TG	Thurgau
TI	Ticino
UR	Uri
VD	Vaud
VS	Valais
ZG	Zug
ZH	Zurich


Law enforcement agencies involved
2002: 100% =515 reports forwarded
2003: 100% = 661 reports forwarded
Number of reports forwarded
0 25 50 75 100 125 150 175 200 225
ZH 102 (19.8%) 189 (28.5%)
CH 195 (37.9%) 169 (25.5%)
GE 89 (17.3%) 77 (11.6%)
BE 34 (6.6%) 44 (6.6%)
TI 16 (3.1%) 33 (5.0%)
BS 8 (1.5%) 22 (3.3%)
SO 7 (1.3%) 19 (2.8%)
NE 6 (1.2%) 15 (2.3%)
SG 7 (1.3%) 13 (2.0%)
VS 2 (0.4%) 13 (2.0%)
AG 2 (0.4%) 10 (1.5%)
VD 7 (1.3%) 10 (1.5%)
LU 7 (1.3%) 9 (1.4%)
ZG 4 (0.8%) 8 (1.2%)
GR 6 (1.2%) 7 (1.1%)
BL 5 (1.0%) 4 (0.6%)
JU 4 (0.6%)
FR 6 (1.2%) 3 (0.5%)
NW 3 (0.5%)
SZ 5 (1.0%) 3 (0.5%)
SH 2 (0.3%)
TG 4 (0.8%) 3 (0.5%)
OW 1 (0.2%)
GL 2 (0.4%) -
UR 1 (0.2%) -

2.3.14 Number of inquiries by other Financial Intelligence Units (FIU)

What the graph represents

This graph shows which FIUs in other countries asked MROS for information and how many individuals and corporations were involved in these requests.

Graph analysis

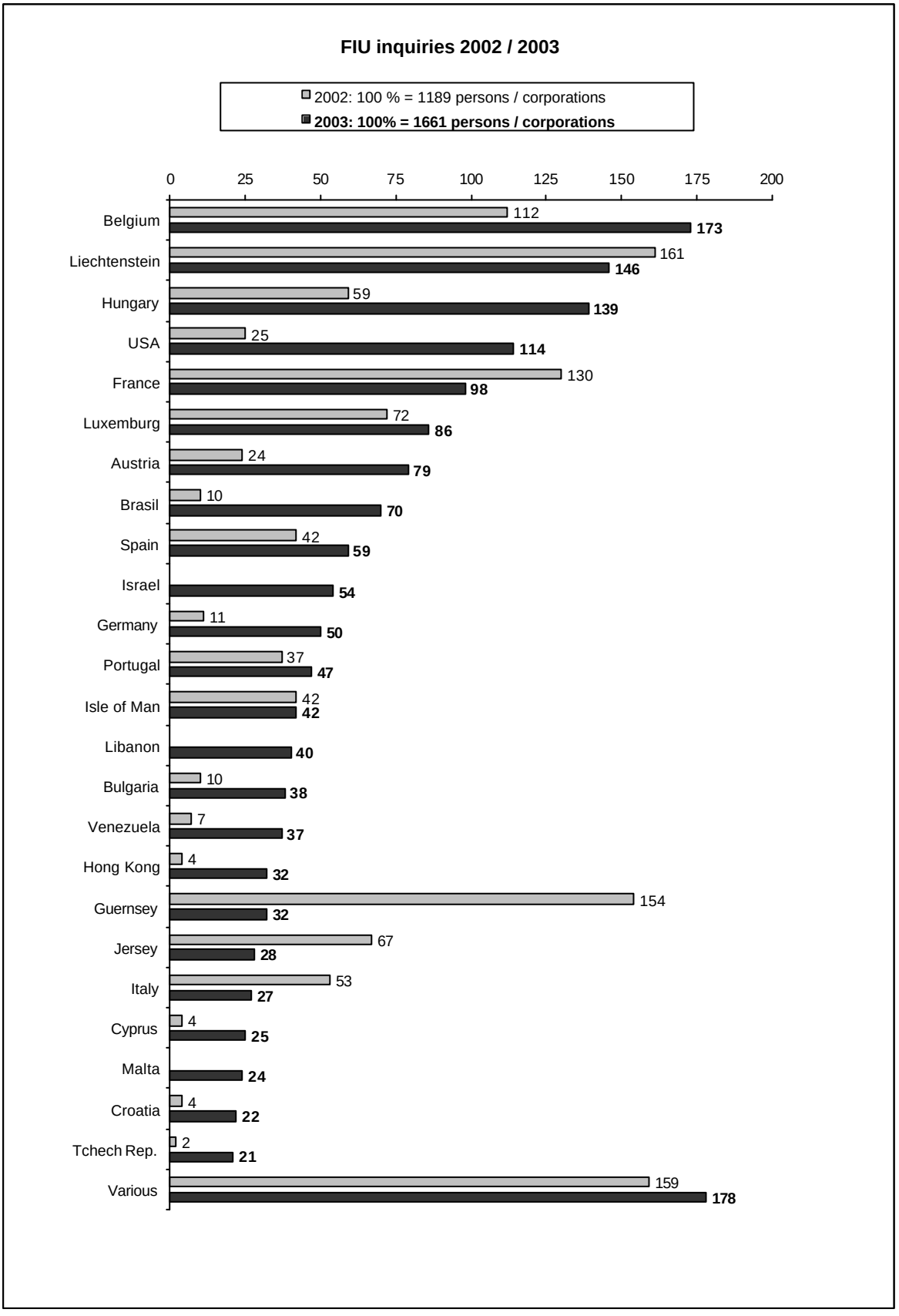
The number of FIU requests continues to increase sharply. In 2003, the increase amounted to 40% more than the previous year. MROS replied to requests from 50 countries. International cooperation is an important tool in the fight against money laundering.

FIUs are the foreign counterpart agencies of MROS with whom it carries out a formal exchange of information in the fight against money laundering (see Art. 32 of the Money Laundering Act and Art. 10 of the decree on the Money Laundering Reporting Office). The exchange of information takes place mainly between the members of the Egmont Group.

When MROS receives an inquiry from abroad, a check is run on the individuals and firms and details are stored in its own GEWA database. Should the individuals or corporations later appear in reports by Swiss financial intermediaries, then GEWA indicates possible criminal activity abroad.

The heading „Others“ includes countries which have made inquiries about only a small number of individuals or companies. These were Andorra, Bermuda, Cayman Islands, Chile, Colombia, England, Finland, Gibraltar, Greece, Ireland, Korea, Latvia, Mauritius, Mexico, Monaco, the Netherlands, Norway, Rumania, Russia, Serbia, Singapore, Slovakia, Sweden, Turkey, Ukraine and the United Arab Emirates

On average MROS ran checks on 138 individuals or companies a month at the request of other FIUs.


FIU inquiries 2002 / 2003
2002: 100 % = 1189 persons / corporations
2003: 100% = 1661 persons / corporations
0
25
50
75
100
125
150
175
200
Belgium 112 173
Liechtenstein 161 146
Hungary 59 139
USA 25 114
France 130 98
Luxemburg 72 86
Austria 24 79
Brasil 10 70
Spain 42 59
Israel 54
Germany 11 50
Portugal 37 47
Isle of Man 42 42
Libanon 40
Bulgaria 10 38
Venezuela 7 37
Hong Kong 4 32
Guernsey 154 32
Jersey 67 28
Italy 53 27
Cyprus 4 25
Malta 24
Croatia 4 22
Tchech Rep. 2 21
Various 159 178

2.3.15 Number of inquiries made to other Financial Intelligence Units (FIUs) by MROS

What the graph represents

This graph shows the countries approached by MROS for information about individuals and corporations and the number involved.

Graph analysis

Requests by MROS to FIUs in other countries have doubled within a year. Information about 1,075 individuals and companies was requested from a total of 56 countries in connection with reports received from Swiss financial intermediaries. The information received helped in numerous cases to decide whether to pass on a report to law enforcement authorities.

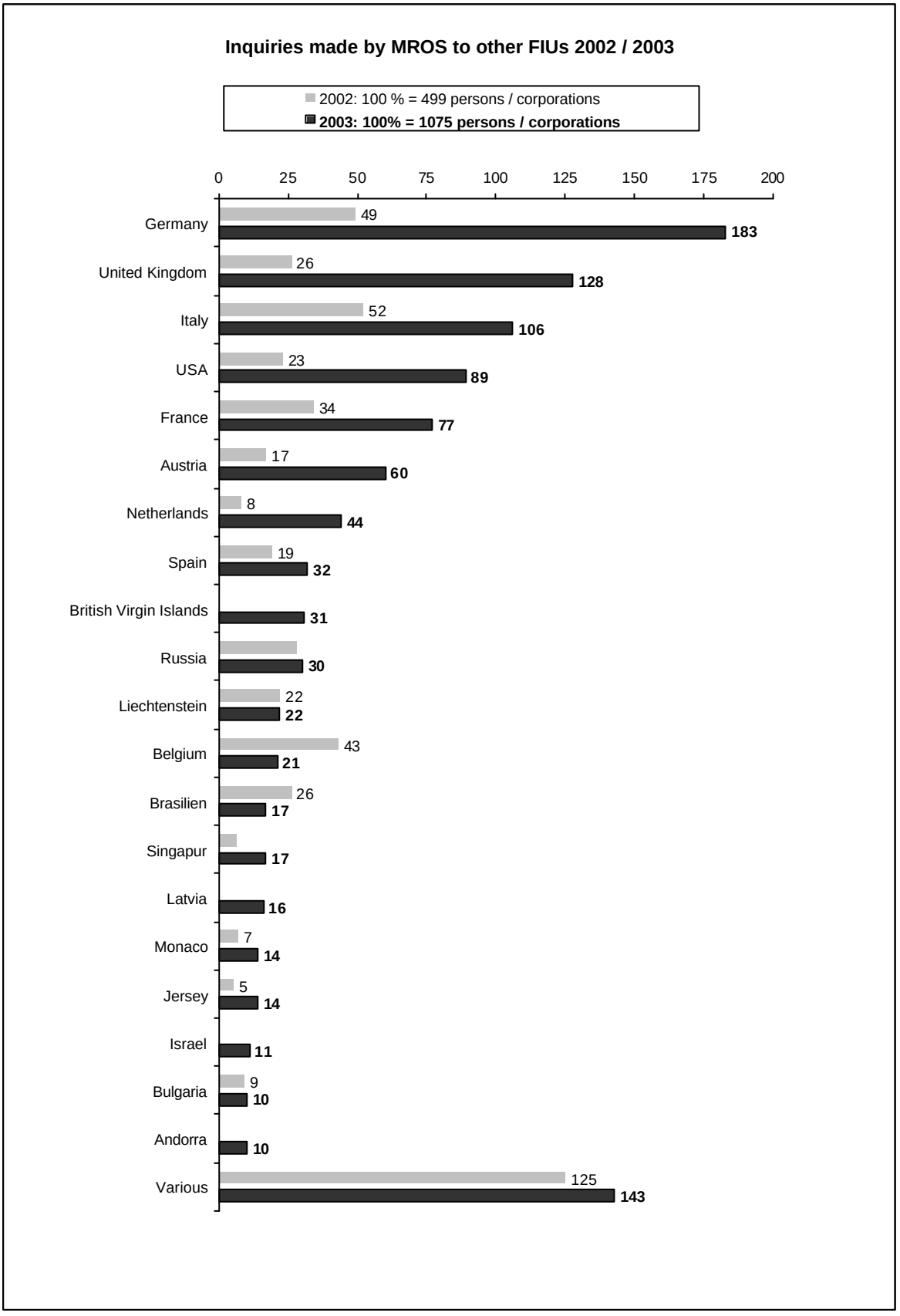
When MROS receives a suspicious activity report from a Swiss financial intermediary in which individuals or companies from abroad are involved, MROS may request information from the respective countries about these individuals or companies.

This way MROS receives important information which could be crucial when making a decision on whether to pass on a suspicious activity report to Swiss law enforcement agencies. MROS can also make inquiries to supplement files at the request of a Swiss supervisory or law enforcement agency.

In 2003 MROS approached FIUs abroad with 309 requests involving 1,075 individuals or companies to follow up suspicious activities reports and requests from Swiss supervisory or law enforcement agencies.

The heading „Others“ includes countries approached by MROS for information about only a small number of individuals or companies. These were Argentina, Barbados, Canada, Cayman Islands, Colombia, Costa Rica, Croatia, Cyprus, Czech Republic, Denmark, Guernsey, Hong Kong, Hungary, Isle of Man, Japan, Jersey, Lebanon, Lithuania, Luxembourg, Malta, Mauritius, Macedonia, Mexico, New Zealand, Norway, Panama, Paraguay, Philippines, Poland, Portugal, Rumania, Serbia, Sweden, Thailand, Turkey, and the United Arab Emirates.

On average, MROS asked FIUs abroad for information about 90 individuals or companies a month.


Inquiries made by MROS to other FIUs 2002 / 2003
2002: 100 % = 499 persons / corporations
2003: 100% = 1075 persons / corporations
0
25
50
75
100
125
150
175
200
Germany
49
183
United Kingdom
26
128
Italy
52
106
USA
23
89
France
34
77
Austria
17
60
Netherlands
8
44
Spain
19
32
British Virgin Islands
31
Russia
30
Liechtenstein
22
22
Belgium
43
21
Brasilien
26
17
Singapur
17
Latvia
16
Monaco
7
14
Jersey
5
14
Israel
11
Bulgaria
9
10
Andorra
10
Various
125
143

3. Typologies

3.1. Terrorist funding

Following the terrorist attacks of 11 September 2001, a Swiss bank reported the opening of an account in the name of X. The assets involved came to around CHF 10 million. X was suspected of financing terrorism and was on the American government's „Terrorist Financing Executive Order" list.
In connection with the suspicious activity report, assets in more than 20 bank accounts were provisionally blocked. The accounts were made out to X and to offshore companies of which X was a beneficial owner.
The report was sent for further processing to the Office of the Attorney General of Switzerland. Subsequent investigations uncovered complicated structures, capital flows as well as various investments made by X. Enquiries also showed that assets deposited in Switzerland between 1990 and 1993 were transferred from a bank in Sudan. This bank was also suspected of financing terrorism.
Suspicions against X grew even more because he had demonstrable personal relations with individuals whose terrorist activities were common knowledge.
Because of the international links investigations are still going on.

3.2. Charity organisations and terrorist funding

A Swiss bank informed MROS of a possible case of terrorist funding through a charity organisation. Apparently this organisation was channeling donations from mosques and Islamic centers to terrorist groups.
An initial analysis of the transactions of the organisation showed that substantial amounts were frequently transferred to individuals in the Middle East.
MROS forwarded the report to the Office of the Attorney General of Switzerland, which in turn ordered the Federal Criminal Police to make the relevant preliminary investigations. Investigations are still pending.
Cases of financing terrorist activities through charity organisations are familiar to Swiss law enforcement authorities. The FATF has also recommended its member states to take steps (Special recommendation VIII), which guarantee the transparency of the accounts of charity organisations. This way the authorities should be able to prevent money being collected under the guise of charity, which in fact goes to terrorist groups.

3.3. Terrorist funding, unregistered financial intermediaries, violation of mandatory due diligence and Hawala

During an in-house control, a Swiss money transmitter noticed a number of unusual transactions by one of its clients, an independent currency exchange office.
The client's modus operandi was as follows: The representative of the money changing office would go the financial intermediary, pay cash into a Swiss-franc account

held by the money changing office and then have the amount transferred from the Swiss-franc account to a US-dollar account. He then had transfers made out in his name but on the account of the clients of the exchange office. Almost all these clients came from the same African country. The assets were transferred mainly to the Middle East.
After analyzing the report, MROS concluded that this case involved a whole network and the amounts being transferred - between USD 40,000 and USD 280,000 - bore no relation to the jobs of the clients of the exchange office (e.g. unskilled workers, employees at a cleaning firm, etc.).
Subsequent investigations showed that two businesses, whose money had been transferred, had connections with terrorist groups.
The investigation by the Office of the Attorney General of Switzerland showed that the assets in question were collected by Africans living in Switzerland and then pooled among the clients of the exchange office. These clients handed the money over to the representative of the exchange office who then paid it into his account and subsequently transferred it in his name to the Middle East.
Later, the money reached Africa via the Hawala system - an informal system for money transfer - so that no link with terrorist groups could be made.
The investigation proved to be extremely difficult because transfers using the Hawala system are not documented and, therefore, cannot be traced.
The Office of the Attorney General, therefore, had no choice but to rely on the statements of the representative of the exchange office.
Similar cases have also occurred in other European countries. Unfortunately in these cases too, the authorities have not been able to prove their suspicions that the money involved was being used to finance terrorism. Nevertheless, it was obvious that the transferred assets had originated from human and drug trafficking.
It is also highly likely that the exchange office, in its role as a financial intermediary and hence answerable to the Money Laundering Control Authority, violated its mandatory due diligence obligations by not reporting these transactions to MROS.
It can also be assumed that the African clients who collected money from their compatriots were acting in a professional capacity, as defined in the petty decree of the Control Authority (VB-MLA, SR 955.20), and could be classified as financial intermediaries. As soon as its investigations are concluded, the Office of the Attorney General intends to inform the Control Authority about the contents of the report so it can also look into the matter.

3.4. Money laundering and trafficking in fake works of art

A European national opened a Swiss bank account and deposited two checks worth around €30,000. The customer told the bank that the money came from the sale of two sculptures. However, he was not able to produce documents recording the sale explaining that it was normal practice in the art market to conclude sales without the transaction being documented.

After the bank had passed the checks on for collection, it noticed that the amount on one check had been forged. An internal inquiry at the bank also revealed that the client was known for his involvement in large scale trafficking of fake works of modern art. One European country had already started investigations against him in this matter.
MROS passed the suspicious activity report to a cantonal law enforcement agency, which has begun investigations against the client on suspicion of fraud, forgery and money laundering.

3.5. No need for a report about business relations?

A company with headquarters in Switzerland opened an account with a Swiss bank in May 2000. The account remained inactive for almost two years until, in 2002, significant amounts were paid into the account and then withdrawn.
The money was deposited in cash, then paid into a dollar account held by the company and later transferred to South America.
In comparison with the size and the business activities of the company that included foodstuffs and audio-visual equipment, the amounts being paid into the account seemed disproportionately high. On studying the bank statements, MROS noticed that over the period of one month more than USD 250,000 had been paid into the account and transferred shortly afterwards.
The almost daily, unrecorded cash payments to South America and the interim account provided even more reason to suspect that the assets came from drug trafficking.
MROS passed the report to a cantonal law enforcement authority, which immediately began an investigation. So far, however, no information has turned up to confirm the suspicions. It was obvious to the company representative that the bank had reported to MROS and he subsequently demanded a copy of the suspicious activity report. Apparently the company representative was himself a financial intermediary with a self-regulatory organisation and worked independently in the money transmitter sector. He suspected that the reporting bank had been simply looking for an excuse to dissolve the business relation. Before the report was made, the bank had never asked him to account for the transactions in question. Had the bank exercised its duty to clarify the matter itself under Art. 6 MLA, it would not have been necessary to report to MROS.
Under Art. 6 MLA, financial intermediaries should try to clarify the background to unusual transactions themselves by questioning the client. If all questions have been answered to the satisfaction of the financial intermediary, then filing a suspicious activity report becomes unnecessary.
MROS did not provide the company representative with a copy of the report but, instead, referred him to the relevant law enforcement authority.

3.6. Money laundering, drugs and a casino

In the spring of 2003, the director of one bank branch visited another branch where he rented a safe deposit box, giving power of attorney to his daughter's partner X. The bank soon discovered that the safe deposit box was being used exclusively by X. A short time later, X was arrested on charges of violating the narcotics act. Following various media reports about the arrest, the bank notified MROS of its business relationship with X. Investigations revealed that X was the manager of a business dealing in precious stones and metals (it should be noted that trade in precious stones is still not subject to the Money Laundering Act).

Moreover, X was already the object of a suspicious activity report from a casino, which suspected X of gambling for the purpose of laundering significant amounts of money. This report was not passed on to law enforcement authorities at the time because of insufficient proof. Following the second report, the information provided by the casino proved to be extremely useful.

X had established an obscure structure to launder illegally acquired assets. He did this through gambling at casinos, dealing in precious stones and using the safe deposit box. MROS passed the report on to a cantonal law enforcement agency, which opened criminal proceedings against X on the basis of violating the narcotics act.

3.7. Money laundering and stock market manipulation

A Swiss bank suspected that assets being transferred into the account of its customer X were of criminal origin. The customer's husband Y had power of attorney over the account. Y worked at bank A and also dealt in stock market options, among other things. His employer had also entrusted him with the independent management of customer money.

On the basis of his work, Y was familiar with the nature of the stock market, the people who worked there and above all the "quiet periods" of the market.

To take advantage of these „quiet periods" (e.g. lunch breaks, flexible time bands etc.), Y opened an account at bank C in his wife's name, giving himself power of attorney. With the assistance of an asset manager at bank C, Y gave stock market orders at purchase prices which were far below the current market price. At the end of the „quiet period", Y sold his undervalued options at the market price and in this way made high profits. To make these purchases, Y helped himself on a short-term basis to his clients' assets, which he managed for his employer.

The bank reported the business to MROS because it had serious doubts about the legality of the transactions. What was especially striking were the frequency of the market transactions and the huge earnings.

The bank suspected Y of using his knowledge of the stock market at another bank to enrich his wife at the expense of his own clients. Y was subsequently accused of market manipulation and disloyal asset management.

3.8. Smuggling ore and financing African rebel groups

Two banks and a financial firm reported their suspicions to MROS regarding business relations in connection with ore smuggling and the financing of African rebel groups. The reporting financial intermediaries had been managing assets derived from the mining and marketing of raw materials from Africa for many years, particularly gold and coltan. The reported assets were held in the name of an African citizen, her close associates and companies, which she managed.

These business activities included the export of precious metals from Africa to Switzerland and other European countries. A report submitted to the UN Security Council by an expert committee raised doubts about the legality of the business activities of the client. The report accused her of having exploited the civil wars in Africa and, in procuring the raw materials including ivory and coltan, of having defrauded the country involved. Moreover, it appeared that the individual was also involved in cigarette and weapons smuggling. Through deft negotiating techniques and weapons deliveries to both sides in a conflict, the client had made a fortune during the political unrest.

The experts, therefore, recommended that the UN Security Council develop an international strategy to investigate the persons mentioned in the report and, if possible, call them legally to account.

On the basis of this information the three financial intermediaries reported their business contacts to MROS. After studying the matter MROS passed the report on to the Office of the Attorney General. In another European country, judicial proceedings have already begun against the client on charges of money laundering and smuggling gold, weapons, cigarettes and coltan. The prosecuting country asked Switzerland for legal assistance and requested that a freeze be put on several million francs. The Office of the Attorney General investigated the case on the basis of the request for legal assistance and the suspicious activity report but was unable to confirm the suspicion of money laundering or illegal business activities in Switzerland. Proceedings in Switzerland were stopped because there was insufficient indication of a predicate offence.

The UN Security Council condemned the activities of the individuals mentioned in the report but left their prosecution up to the countries concerned.

3.9. Money laundering, corruption, petroleum and PEP

Two Swiss banks notified MROS about three business connections involving an important corruption case relating to the production of natural gas in the Persian Gulf.

A European oil company approached X, a consultant in the oil trade, who was supposed to help the company to obtain oil concessions in the Arab country concerned. So the company and X's consulting firm, which was based in an offshore country, signed a contract. Staff members at the oil company had doubts about the legality of the contract, according to which a consultancy commission of more than USD 10 million - USD 5 million of which were to be transferred in advance – was to be paid over the period of several years. It just so happened that the affair became public knowledge and caused a scandal.

It is likely that X concluded the contract with the oil company on behalf of Y, a close relative of an influential politician in the Arab country concerned. The scandal came to the attention of the two Swiss banks, which then reported to MROS about its business dealings with the offshore companies of whose assets X was a beneficial owner. The advance payment of USD 5 million agreed to in the contract had been transferred to one of the accounts reported by the bank.
Because the frozen assets had very likely come from a criminal source (corruption), MROS passed the suspicious activity report to the Office of the Attorney General, which began investigations and has already conducted various searches and interrogations.
As a result of the investigations in Switzerland and other European countries, most of the capital flows have been traced.
Preliminary investigations are still going on and criminal proceedings on charges of money laundering will probably be opened soon.

3.10. Risks of beginning a business relationship by correspondence

In February 2003, X opened an account with a Swiss bank declaring that he wanted to manage his assets from his residence in Spain via Internet. After the bank received the completed documents from X pertaining to the opening of the account, it sent X the Internet access codes.
Shortly after, the client transferred securities from a foreign bank for deposit in Switzerland. From April 2003, these securities were gradually sold. The proceeds from the sales were credited to an account held by Y at the same Swiss bank and then transferred to Y's account at a Swiss Internet bank. Finally almost all the assets which X had transferred to the Swiss bank were transferred to Y's account at the Internet bank.
In the meantime, X complained to the Swiss bank that he had never received his Internet access codes. When the bank informed him that it had sent the codes, the client claimed that his subtenant Y had intercepted the letter containing the access codes and was using them to steal his assets. X's bank then contacted Y's Internet bank and informed it that the assets deposited by Y into his account could be of criminal origin. It also reported its suspicions to MROS.
The Internet bank provisionally froze Y's deposits and also reported to MROS. In addition, X filed a complaint against his subtenant Y.
Investigations by a cantonal law enforcement authority confirmed X's suspicions, and Y admitted having used the access codes to make the transfers. Nevertheless, the accusation of money laundering could not be sustained because X's assets were not of a criminal origin, and Y had not done anything to conceal the origin of the funds or to prevent their discovery. However, criminal proceedings against Y were begun on charges of fraud (Art. 146 Criminal Code) and misuse of a data processing facility for fraudulent purposes (Art. 147 Criminal Code).
This case illustrates the importance of Art. 10 par. 3 MLA, which forbids financial intermediaries from engaging in tip-offs. The article forbids *prima facie* the financial intermediary from informing the parties involved or third parties about the suspicious ac-

tivity report. The Federal Council message of 17 June 1996 (BBI 1996 III 1133) expressly stipulates a ban on information to the parties involved and third parties.
However, this must be qualified (see DE CAPITANI, Art. 10, No. 91). The way the law is formulated leads to the conclusion that the ban on tip-offs is only a goal in itself. This is not the case, however. The aim of the ban is not only to locate and confiscate criminal assets, but also to identify the individuals behind these assets so that they can be prosecuted (see DE CAPITANI, Art. 10, No. 5). But it would be somewhat naive to assume that the success of the law enforcement authorities depends solely on discretion (see GRABER, Art. 10, No. 6). There are exceptions to the principle of an absolute ban on information, which do not endanger the goal stipulated in the law (see DE CAPITANI, Art. 10, No. 91 i.f.; GRABER, Art. 10, No. 7).
This is especially the case with financial intermediaries who, while having a business relationship with a client, do not actively manage the assets entrusted to them. Thus, for example, fiduciaries or asset managers should be able to inform the bank holding the account about the suspicious activity report so that the bank can freeze the account (see DE CAPITANI, Art. 10, No. 86; GRABER, ibid., LOMBARDINI, No. 78 page 682).
In the case described above it can also be assumed that the Swiss bank did not contravene Art. 10 par. 3 MLA. The bank had a reasonable suspicion that this was a case of money laundering. This meant that informing the Internet bank about its suspicion was unavoidable if the latter was going to inform MROS about its dealings with Y, thus enabling the illegal assets to be frozen.

3.11. Money laundering, gatekeeper, corruption, petroleum and PEP

MROS received several reports from a Swiss fiduciary about a possible money laundering case relating to corruption in the crude oil sector. The fiduciary was also involved in the case because she had been given the mandate to manage several offshore companies. The actual administration of the offshore companies, however, was in the hands of a Swiss lawyer who had unlimited power of attorney.
The beneficial owners of the assets of the offshore companies were a large oil company and a close adviser of an African leader.
A number of accounts were opened at various banking institutes in Switzerland in the names of the offshore companies.
The fiduciary was doubtful about the legality of the transactions that went through the accounts of the companies because, according to various media reports, the beneficial owners were facing prosecution for corruption. The fiduciary contacted the lawyer to clarify the situation under her obligations to exercise due diligence. The lawyer's information was incomplete and only given reluctantly so the fiduciary decided to withdraw the lawyer's power of attorney on the accounts of the offshore companies. The fiduciary demanded that the lawyer hand over all bank statements and inform her about the activities of the companies and the origin of the assets.

Because of insufficient information, the fiduciary decided to report the business relationship to MROS which analysed the case and passed the report on to the law enforcement agency.
MROS frequently deals with reports involving the crude oil sector. Corruption and, consequently money laundering in the crude oil branch occurs more frequently than in other sectors due to the enormous sums that must be invested to purchase oil concessions.

3.12. Diversion of assets for the purposes of corruption; unregistered financial intermediaries; gatekeeper

The Swiss authorities received a request for legal assistance from a European country where a criminal investigation had been opened against several employees of a manufacturer of telecommunications equipment because of excessive charges.
A cantonal authority carried out an investigation into the activities of the manager of the Swiss branch as well as a Swiss attorney on suspicion of money laundering, forgery, bribery and fraud.
On the basis of various media reports, MROS received a total of 14 suspicious activity reports from eight banks. MROS passed all the reports to the cantonal law enforcement authority. The frozen assets came to several hundred million Swiss francs.
The investigation in Switzerland revealed that the Swiss attorney, a legal advisor at the company's headquarters abroad, had been assigned by the manager of the Swiss branch to set up a network of bank accounts made out to either the lawyer himself, the manager or to various letter-box companies. The firm transferred money to these accounts in order to pay consultants living abroad. However, the invoices for the consultancy fees had been forged in order to deceive tax authorities in the European country in question. The external consultants were assigned to open up markets in the Middle East, Eastern Europe and North Africa for the manufacturer of telecommunications equipment.
The so-called consultancy fees were probably used to defraud the tax authorities and to bribe officials in the above-mentioned regions to make it easier to open markets there.
Should this theory turn out to be true, it could develop into an extremely interesting case: The money, which was not declared to the tax authorities, was supposed to have been used to bribe foreign officials with the aim of securing important delivery contracts for telecommunications equipment.
The Swiss law enforcement authorities worked with the Money Laundering Control Authority in the investigation because the consultants acted as unregistered financial intermediaries as understood by the Money Laundering Act. In the meantime, the case in Switzerland has been closed because the request for legal assistance was fully met by the Swiss authorities.

The two previous typologies use the term "gatekeeper". This refers to individuals who act as consultants in the legal (attorneys) or the financial spheres (accountants, auditors, etc.).
Based on their advice, money flows are concealed either through the establishment of a complex structure of bank accounts opened at various institutions in the names of different individuals and companies or by the presence of middlemen, making it impossible or difficult to make establish a direct link between the financial intermediary and the client.

3.13. Plausibility of real estate transactions

An East European client of a Swiss mercantile bank paid CHF 140,000 in cash into the account of his brother living in North America. The money was supposed to have come from the sale of a property in Eastern Europe. The customer presented the bank with a contract that fixed the sales price at CHF 260,000. A couple of days following the cash deposit, the account was credited with a further CHF 90,000.
Shortly afterwards, the bank was instructed by the account holder to transfer the whole balance to his account in North America. No sooner had the amount been debited from the account, the client's brother, who had power of attorney, presented the bank with a check for more than CHF 370,000 and explained that the money consisted of the recently debited balance plus savings from North America. He said his brother wanted to buy a house in his native country but, because the purchase had not taken place, the money was now being paid back into the Swiss account. Two weeks later, the individual with power of attorney requested a check to be made out for more than CHF 370,000 to buy a property in North America.
In addition to these transactions, the individual with power of attorney paid CHF 100,000 in cash into his own account. This was supposed to have been the amount remaining from the property sale in Eastern Europe.
These transfers between Switzerland and North America made little sense. Had a property purchase in North America really been planned it would have been simpler to pay the money there. In addition, the bank thought the purchase price of CHF 260,000 for an agricultural property in Eastern Europe to be disproportionately high.
Investigations by MROS in Eastern Europe and North America increased the suspicion that the assets deposited at the bank could have had a criminal source. After analysis, the report was passed on to the law enforcement authorities who began an investigation.

3.14. Interim accounts

Regular payments of money amounting to millions were credited to an account of a West African company at a private Swiss bank and shortly afterwards transferred. The most recent deposit of €6 million came from West Africa and was immediately transferred to a firm in Eastern Europe.

The beneficial owner of the assets of the account holder was an individual from the Middle East domiciled in Western Europe.
Because the company account was obviously meant as an interim account, the bank requested the beneficial owners to provide records of the transactions.
Invoices and bills of lading for equipping a radio station in a West African country were presented to the bank. The radio equipment had been produced in Eastern Europe.
The bank was very impressed by the documents because they had a great number of stamps and official-looking seals. In short, they were too good to be true! The bank suspected that the frozen CHF 16 million may have originated from the embezzlement of the country's national wealth or may have been the proceeds of corruption.
Following its analysis, MROS forwarded the report, together with the results of international inquiries by several Egmont members, to the law enforcement authorities.

3.15. High-cost loans

Two Swiss nationals opened an account with a cantonal bank. However the account holders were not the beneficial owners of the assets deposited in the account but a third person in the Netherlands. High sums of money were paid into the account on behalf of a foreign law firm. Payments were also made directly into the account by third persons. The account holders then paid the money into an account held by a North European firm with the same bank.
This gave the bank reason to doubt the validity of the beneficial ownership. These doubts were strengthened when one depositor inquired into the whereabouts of his money. The depositor said the firm's procedure involved the investor having to pay a 20% security deposit in return for which the depositor would receive a loan at 100%. Unfortunately, the depositors waited in vain for their loans. In this way, around CHF 24 million had been paid into the account.
An investigation by the bank revealed that the beneficial owner had been introduced to the bank by a Swiss woman who was offering a world-wide investment program that she had built up herself. Her procedure was extremely suspicious. To avoid further damage, the bank repaid the money that had been deposited into its account to the investors and terminated the business contact. The Swiss woman had close business relations with an individual living in North America who had recently been arrested and charged with fraud. The amount involved came to USD 160 million.
The Swiss woman was already known to MROS prior to this report. A Swiss regional bank had reported its business dealings with a Swiss-based company, of which the Swiss woman was a beneficial owner. The Swiss woman and an east European partner had also founded a company in the Caribbean that dealt in diamonds and other precious stones. Potential buyers from around the world were brokered by a company based in the Middle East. One of these buyers reported to the regional bank because he had apparently been cheated by the company domiciled in the Caribbean. The suspicious activity report by the regional bank was passed on to a cantonal law enforcement agency, which initiated proceedings against the Swiss woman on suspicion of fraud and money laundering.

Most of the individuals mentioned in the report of the cantonal bank were also in police files. MROS discovered further evidence in eight countries. Because of the international aspects of the case, the report was passed on to the Office of the Attorney General for further handling. Criminal proceedings were opened against the beneficial owner and the responsible body of the north European company.

3.16. The naive girlfriend

The girlfriend of a customer of a major bank appeared at the counter and presented a hand-written power of attorney from her boyfriend. The girlfriend explained to the bank that, unfortunately, her partner was not able to appear in person because he had been arrested a couple of months previously in a southern European country after almost 30 kg of hashish had been discovered in his car. The hashish had been intended for trafficking as well as for his own use. To prove her statement, the conscientious girlfriend provided the bank with a copy of the charge papers and the provisional judgment of the court: Her partner had been sentenced to 3 ½ years in prison.
The bank refused to pay out anything to the girlfriend and conducted a thorough check of the business relationship. It discovered that the account holder was a dealer in precious stones, jewellery and silver articles from Asia. It also discovered that certain cash payments into the client's account had exceeded more that twice his stated annual income.
Enquiries by MROS revealed that the customer was involved in the international drug trade and that he had imported the 30 kg of hashish from North Africa with Zurich as the destination. The suspicious activity report was directed to the cantonal law enforcement authorities.

3.17. Old, but not necessarily wise

A wealthy old woman concluded a contract with a client of a foreign bank concerning the purchase of 25 shares of a Swiss-based company. The charming salesman, who was also the only board member of the company, had rented suitable office space to negotiate with the old woman and had given himself a doctor's title.
Confidently the old woman invested around CHF 50 million in the production of solar cells, which were supposed to be up to 70% effective. Unfortunately, the woman did not know that solar cells are only 30% effective. A 70% effectiveness would have been sensational.
Later the woman's attorney noticed that, according to the tax authorities, the company was only valued at CHF 700,000. This meant that the shares for which the woman paid CHF 50 million had a real market value of only CHF 175,000. In addition, there was evidence that the company was no longer operating.
The seller of the shares was already known to MROS. A couple of months before the submission of the report to MROS, a cantonal law enforcement authority had opened proceedings against him on suspicion of fraud. The report from the foreign bank was

passed on to the cantonal law enforcement authority. Criminal proceedings are still pending

3.18. Forged payment orders enable transfers to offshore companies

A Middle East businessman had business relations with a Swiss bank as the sole signatory and beneficial owner of two offshore companies, in whose names accounts had been opened. In the summer, the businessman had informed the customer care representative at the bank by telephone that two men known to him would like to open an account at the bank into which €10 million would subsequently be paid. The payment, he said, was in connection with the financing of a company. A face-to-face meeting requested by the bank with the two men regarding the planned opening of the account fell through supposedly because of a previous engagement. Afterwards the businessman informed his customer care representative that the transfer in question would be made directly into the accounts of both his offshore companies. This took place a short time later. The money which amounted to €10 million did not, as announced, come from the two men but from an insurance company in a neighboring country. On the following morning, however, €300,000 of the €10 million was transferred. At noon on the same day, the bank received a SWIFT notice from the forwarding bank saying that the previous transfer of €10 million was fraudulent and demanding immediate repayment. Following enquiries by the internal legal department, the bank was given copies of a letter and a criminal charge by the foreign insurance company. This led to the strong suspicion that the €10 million transfer into the accounts of the businessman's offshore companies was fraudulently carried out using forged payment orders. The Swiss bank immediately blocked the assets and reported to MROS who looked into the affair and passed it on to a cantonal law enforcement authority, which is now dealing with it.

3.19. Lucrative advertising

Alerted by a letter from a third person, the compliance division of a financial intermediary analysed the transactions of a new client. Although it had only recently been set up, the sole proprietary advertising firm showed an impressive number of payments into its account. The facts were presented this way: the owner of the firm systematically acquired local plans, copied the addresses of the advertisers on these plans and then billed these firms for the advertising space they were using. This was done although the marketing of advertising space on local plans was the responsibility of another firm. Most of the advertisers paid the bills without looking any further into the matter because they knew they had taken out such publicity. Firms which did not pay the bills immediately were sent reminders or even threatened with court action. Within a short time, more than CHF 370,000 had been paid into the account of the advertising agency. Luckily the manager of the firm was so occupied collecting the bills that he forgot to put his mounting fortune aside. The suspicious activity report was passed on

to the law enforcement authority and it is assumed that the firms that were cheated will get back much of their money.

3.20. Build up your own Internet Empire

A financial intermediary received a call from a man claiming to have been the victim of an Internet fraud. He had been told that if he paid a large sum of money into a Swiss bank account he could easily earn as much as USD 200,000 a year by working at home. It involved operating a so-called Internet Mall - a virtual shopping centre - from his house. The amount of the investment corresponded to the size of the mall one wanted to operate. The larger the mall the more likely was the sale of products and, therefore, the payment of a commission to the operator. The dubious Internet page looked extremely professional and, at first glance, gave the impression that the enterprise had worked closely with well-known firms such as Amazon.com, Dell or Disney. One of the victims said that the commission was never paid and the bold promise of a money-back guarantee was never honoured. Because of various complaints by irate investors at http://www.badbusinessbureau.com/ , an Internet page devoted to combating fraud, it had to be assumed that a large number of individuals had been attracted by the possibility of earning a fortune by managing their own business from home and had invested considerable amounts. After thorough analysis, the suspicious activity report was passed on to the Office of the Attorney General.

3.21. Weapons deliveries and bribery payments

During an in depth analysis of a business relationship, a financial intermediary concluded that the accounts of various foreign companies with one and the same beneficial owner were being used simply as interim accounts. It was also determined that the source of a large part of the assets in the accounts was a marketing agreement between an Asian firm and a Russian business specialized in the development and production of weapons. The weapons manufacturer had recently been accused of making illegal weapons deliveries to Iraq. As a result, the US spoke of imposing sanction against the firm. At the moment, the Office of the Attorney General is investigating whether the money involved came from bribery payments.

3.22. Cash transactions for a retail business

The secretary of a company that also did the accounts for a trade association connected to the company, appeared frequently alone at the counter of a bank to make cash withdrawals. In spite of the fact that he had only a collective power of attorney, the secretary presented credible documents from his employer that permitted him to make this kind of transaction. He also paid off the credit card bills of his employer in cash instead of using a payment order.

A check by the bank of the credit card transactions revealed that the kind of operations, in particular casino payments, did not correspond to the activities of a union. This situation prompted the bank to report to MROS. Although the data base con-

tained no evidence of a predicate offence, MROS nevertheless decided to pass this affair on to the cantonal law enforcement authorities. The union secretary was arrested and subsequent enquiries brought various offences to light, in particular embezzlement and forgery.

3.23. Cash deposits in small notes

A financial intermediary held an account into which three east European citizens paid several hundred francs in small notes almost daily. The account holder, who was also of east European origin, explained to the financial intermediary that he and his friends worked in the hotel and restaurant sector and the deposits were the tips they had earned. Because they always treated their guests with utmost courtesy, the gratuities were correspondingly high.
MROS discovered that the three men belonged to an east European group which was on police files in various cantons because of theft, robbery and receipt of stolen goods. MROS immediately sent the report to the law enforcement authorities.

3.24. The missing foreign exchange dealer

Because of a seizure order by the Zurich judiciary, a financial intermediary was obliged to report all previous and existing accounts of two Zurich foreign exchange firms which were known mainly abroad. It seems that the head of the firms, which had shown excellent returns, had himself not returned to work following a well-earned vacation abroad. He gradually withdrew customer assets in cash and closed the companies' accounts at a London securities' firm. Shortly before his disappearance, the head of the two companies had sold them to a third party. In the meantime, bankruptcy proceedings have been opened and it can be assumed that more than 1,700 customers will lose everything. Investigations by law enforcement authorities are still underway. There is still no trace of most of the customer investments or the suspect.

3.25. Professional money transmitter?

During a routine check, a Swiss financial intermediary also offering money transmitter services noticed that one of its clients, a taxi driver, had transferred more than CHF 200,000 mainly to countries in Eastern Europe over a period of six months. The financial intermediary looked into the matter under Art. 6 MLA and discovered that the taxi driver's main customers were prostitutes whose earnings he offered to transfer to their native countries. The financial intermediary pointed out to the taxi driver that he himself was acting as a financial intermediary and therefore had to register as a Self Regulatory Organisation, or SRO. The customer replied that the procedure was too complicated and that he would no longer offer the service. Not long after, the same branch noticed that numerous transfers were again being made to Eastern Europe. This time however the sending party was a woman who explained that she was employed by the taxi driver. Because there was no evidence that the assets involved were illegally acquired, MROS did not pass the report on to a law enforcement author-

ity. However, the Money Laundering Control Authority was informed about the activities of the taxi firm under Art. 10 of the Money Laundering Reporting Ordinance.

3.26. "Nigerian letters"

Enquiries by a money transmitter revealed that a Swiss national had transferred more than CHF 150,000 to various recipients in a West African country within the space of a couple of months. The sender explained to the money transmitter that he had invested the money into an oil company based in West Africa and that he soon expected high returns. Following a check of the documents provided by the client, the money transmitter was sure that the client was a victim of Nigerian swindlers.
The money transmitter informed the client of the fraudulent activities but he was adamant in his conviction that his business partners were not involved.
Although MROS had no evidence that the money being transferred had a criminal source, it sent the report to a cantonal law enforcement authority because MROS wanted the authorities to explain the fraud to the person sending the money. Subsequent investigations by the cantonal police showed that the money being transferred indeed came from the sender's own assets. The police also explained in detail how the swindlers worked and advised him explicitly not to send any more money to West Africa.
Six months later another money transmitter reported the same Swiss national to MROS because he had transferred more than CHF 50,000 to West Africa within a few months. It was clear to this money transmitter too that this was the "Nigeria Connection" at work again.
The sender was, as are most victims, fully convinced that this could never happen to him. Today he is wiser. The promised returns amounting to millions never materialised.

Further information on this topic is available at www.fedpol.admin.ch – Updates – Warnings – Nigerian swindlers.

3.27. Robbing your own business

A Swiss man transferred CHF 5,000 to California via a money transmitter. A day later, the same man again transferred CHF 5,000 to the USA. The client could not provide documents (bank receipts or similar) attesting to the source of the money and claimed that the reason for the transfer was that he was donating money to someone. The transaction was refused because of a lack of credibility. Based on the report from the financial intermediary and following enquiries by the cantonal police, MROS made an astonishing discovery in the analysis of the individual: The man making the transfer had been robbed only two days before the transactions and a huge sum of cash had been stolen from his office. This was proof enough for MROS to send a suspicious activity report to the law enforcement authority. A judgment is still pending.

3.28. The money transmitter exercises due diligence

Two people of African origin were providing money transfer services to Africa. Gradually this service was expanded to other countries particularly in Europe. Clients were found on the Internet. The money to be transferred was paid in cash and the service providers used the transfer facilities of a Swiss enterprise which offered Western Union money transfers. Within a year, the suspects had made transfers amounting to CHF 500,000. In view of the frequency of these transactions, the money transmitter demanded to know the source of the money. The explanations of the two African men did not sound credible and led to reports by two different money transmitters to MROS.

As is often the case with money transmitters, the information and the inquiry results they provide MROS are insufficient for a report to be directed to a law enforcement agency. Nevertheless, the fact that the two men did not have permission from the supervising authorities to operate as money transmitters led to a report to these authorities to take the necessary measures. In the meantime, the Africans continued their activities this time with a third party in which they tried to keep the amounts involved in their transactions lower (smurfing). But money transmitter firms also had doubts about the legitimacy of these transactions and filed a report. Records of a successful prosecution of one of the two Africans for an economic crime that had been reported to MROS by a law enforcement authority under Art. 29 par. 2 MLA were found in the MROS database. The report was then submitted to this law enforcement authority to check whether the money or part of it had any connection with the above conviction. Investigations are continuing.

3.29. Criminal organisation and casinos

The managers of a casino were made suspicious by the behavior of several customers who played with considerable sums and carried out currency exchanges in amounts running as high as CHF 100,000. Because of security service action, these customers were observed more closely and the amounts played and won were recorded. At the same time, the casino came across various media articles reporting on the activities of a mafia gang at a foreign casino. The individuals mentioned in the articles were identical with those who had been observed in the Swiss casino. Consequently, the casino managers sent a report to MROS informing it that they suspected the clients of money laundering. Information provided to MROS by the FIU of the country of origin of the suspects showed that they had been prosecuted in the past for involvement in organised crime. The report was therefore sent on to the Office of the Attorney General of Switzerland. In view of the significance of the facts, the Federal Gaming Commission also opened an investigation.

3.30. Casino and bank: alert financial intermediary

The people responsible for the supervision of a casino observed a roulette player who made considerable wagers. An inquiry with a credit information firm revealed that the

client had suffered considerable losses. The casino decided to report to MROS. Although the amounts the customer was playing were considerable (several thousand francs), the various enquiries made by MROS could not prove the suspicion of either money laundering or the existence of a previous crime. The suspicious activity report was subsequently filed. Two months later, however, a bank submitted a report concerning the same customer. The report was based on the fact that the client had been arrested on charges of drug trafficking. MROS called up the first report from the casino which had been stored in the GEWA data base and both reports were sent to the cantonal law enforcement authorities.

4. International scene

4.1. Egmont Group

Membership in this group, which consists of the national FIUs of various countries, requires an operative FIU such as MROS acting in its capacity as a central, national authority to receive suspicious activity reports from financial intermediaries, analyse them and, if necessary, pass them on to the law enforcement authority. Members are also required, either on a legislative basis or by a memorandum of understanding (MOU), to exchange relevant intelligence with other foreign counterpart offices.

At its plenary meeting in July 2003 in Sydney, the Egmont Group increased its membership to 84 from 69 Financial Intelligence Units, or FIUs. The countries listed in italics are new:

1. *Albania*
2. Andorra
3. *Anguilla*
4. *Antigua and Barbuda*
5. *Argentina*
6. Aruba
7. Australia
8. Austria
9. Bahamas
10. *Bahrain*
11. Barbados
12. Belgium
13. Bermuda
14. Bolivia
15. Brazil
16. British Virgin Islands
17. Bulgaria
18. Canada
19. Cayman Islands
20. Chile
21. Colombia
22. Costa Rica
23. Croatia
24. Cyprus
25. Czech Republic
26. Denmark
27. *Dominica*
28. Dominican Republic
29. Dutch Antilles
30. El Salvador
31. Estonia
32. Finland
33. France
34. *Germany*
35. Great Britain
36. Greece
37. *Guatemala*
38. Guernsey
39. Hong Kong
40. Hungary
41. Iceland
42. Ireland
43. Isle of Man
44. Israel
45. Italy
46. Japan
47. Jersey
48. Korea (Republic)
49. Latvia
50. *Lebanon*
51. Liechtenstein
52. Lithuania
53. Luxembourg
54. *Malaysia*
55. *Malta*
56. Marshall Islands
57. *Mauritius*
58. Mexico
59. Monaco
60. Netherlands
61. New Zealand
62. Norway
63. Panama
64. Paraguay
65. Poland
66. Portugal
67. Rumania
68. Russia
69. *Serbia*
70. Singapore
71. Slovakia
72. Slovenia
73. *South Africa*
74. Spain
75. *St. Vincent & Grenada*
76. Sweden
77. Switzerland
78. Taiwan
79. Thailand
80. Turkey
81. United Arab Emirates
82. USA
83. Vanuatu
84. Venezuela

South Africa is the first African country to become a member of the Egmont Group, an informal gathering of different national *Financial Intelligence Units*.

Besides the annual plenary meeting, there were meetings of working groups in March and October 2003 in Bern and Ottawa – MROS having organised the former. MROS has one member in each of the *legal* and *outreach* working groups. The *Legal Working Group* is mainly responsible for all legal and fundamental issues as well as cooperation between the individual national FIUs within the Egmont Group. The *Outreach Working Group,* on the other hand, is responsible for recruiting new members and for the expansion of the Egmont network.

Further information about the Egmont Group as well as the complete and up-to-date list of all operative FIUs in the group is available on the new homepage www.egmontgroup.org.

4.2. FATF / GAFI

The Financial Action Task Force (FATF) is an intergovernmental body which works at the national and international level to develop and promote strategies against money laundering and the financing of terrorism[1]. The tasks of the FATF, which was first under the chairmanship of Germany (FATF XIV) and, since July 2003, presided over by Sweden (FATF XV) are focused on a general stepping up of the fight against money laundering and the financing of terrorism. This finds its expression in the broadening of its recommendations (see sections 4.2.3 and 4.2.4). The number of non-cooperating countries is declining (Section 4.2.1) and is giving way to an increase in FATF membership (Section 4.2.2) and closer cooperation with international organisations (Section 4.2.5). The FATF has adopted a new form for its typologies (Section 4.2.6), which should prove useful in the development of new regulatory standards.

4.2.1 Non-cooperating countries (NCCT)

In its last report[2] the FATF discussed the situation in the fight against money laundering and the financing of terrorism in non-cooperating countries and territories (NCCT) during 2003. The so-called Black List of NCCT for 2003 consisted of the following countries: the Cook Islands, Egypt, Guatemala, Indonesia, Myanmar, Nauru, Nigeria, the Philippines and Ukraine[3]. Grenada, St. Vincent and the Grenadines were dropped from the list, while in the cases of Nauru[4] and Myanmar[5] the FATF introduced measures because of their systematic unwillingness to cooperate.

[1] http://www.fatf-gafi.org/AboutFATF_en.htm - Programme

[2] http://www.fatf-gafi.org/pdf/ncct2003_en.pdf

[3] http://www.fatf-gafi.org/NCCT_fr.htm

[4] http://www.fatf-gafi.org/pdf/PR-20011205_en.pdf

[5] http://www.fatf-gafi.org/pdf/PR-20031103_en.pdf

4.2.2 Development of the FATF: new members and regional associations

In 2003, the FATF welcomed Russia and South Africa as new members. With the presence of Russia all G8 countries are now represented in the FATF. South Africa's membership is also welcome because it is the first African country to join the Egmont Group. Because of the constant increase in members (currently 33[6]) it is becoming increasingly difficult to reach decisions because the FATF system requires a unanimous vote. The regional organisations based on the FATF model are steadily gaining importance because they assume tasks concerning the assessment of countries which are not FATF members, and monitoring those countries which have recently been taken off the NCCT Black List. At the moment there are five regional organisations: Africa, Asia/Pacific, Caribbean, Europe and South America. The FATF is presently considering setting up new regional groups especially in the Middle East and Central Asia.

4.2.3 Revision of 40 FATF recommendations

The adoption of the 40 recommendations at the plenary meeting in Berlin was doubtlessly the most important FATF event in 2003. Switzerland, which worked actively on reviewing the regulations, welcomed the acceptance of these new international standards.[7] With the adoption of the new recommendations, national legislation should also be adapted. Compliance with the new recommendations will be monitored within the framework of mutual evaluations among member states (from end 2004). To this end, the Swiss authorities have set up inter-departmental working groups to accelerate the necessary changes. These changes are scheduled to be introduced in 2005.

4.2.4 FATF recommendations against terrorist funding

The development of the special recommendations was continued by a working group. This process permitted the acceptance of new regulations. The FATF has presented the contents of specific special recommendations in Best Practice documents[8] as well as in explanatory remarks[9]. As mentioned in the 2002 MROS report, the FATF also carried out a self-evaluation in 130 countries relating to compliance with the recommendations. The FATF is now analysing the results of these self-evaluations to establish priorities regarding technical assistance for countries without sufficient financial resources. To this end the G8, on the occasion of the Evian summit, decided to create

[6] http://www.fatf-gafi.org/Members_en.htm

[7] http://www.efv.admin.ch/d/internat/finanzpl/pdf_auss/FATF_PressRec_0603_d.pdf

[8] Combating the Abuse of Alternative Remittance Systems: International Best Practices (Special Recommendation VI)

[9] Combating the Abuse of Alternative Remittance Systems: International Best Practices (Special Recommendation VI)

Combating the Abuse of Non-Profit Organisations: International Best Practices (Special Recommendation VIII); http://www.fatf-gafi.org/pdf/SR8-NPO_en.pdf

a new platform to coordinate technical support internationally[10]. In addition the FATF, besides working with the United Nations Security Council Counter-Terrorism Committee (UNCTC),[11] is now cooperating with the recently established Counter-Terrorism Action Group (CTAG).

4.2.5 International cooperation

To ensure international compliance with the 40 recommendations and eight special recommendations, the FATF has strengthened its collaboration with the IMF and the World Bank. Both organisations have recognised the recommendations as international standards in the fight against money laundering and the financing of terrorism. The FATF, IMF and World Bank have agreed to create a common methodology based on the AML/CFT-Method[12], which the FATF formally recognised on 11.10.2002. The FATF has set up a working group to develop this new common methodology.

4.2.6 Meeting to discuss money laundering typologies

In 2003, the typologies conference in Mexico was somewhat[13] different from that of previous years. The FATF treated the topics on the agenda in three working groups: terrorist financing with the assistance of non-profit organisations, terrorist financing by electronic payments and money laundering through insurance. Two topics were discussed at the plenary meeting: politically-exposed persons and "gatekeepers"[14]. The goal of this new kind of meeting was to achieve better understanding of the procedures in money laundering and to use the knowledge resulting from this understanding to formulate future recommendations.

[10] http://www.g8.fr/evian/extras/499.pdf

[11] http://www.un.org/docs/sc/committees/1373/

[12] Anti Money Laundering and the Combat against Terrorist Financing

[13] Reports from the previous years : http://www.fatf-gafi.org/FATDocs_en.htm - Trends

[14] "Gatekeeper": a person involved in consulting either in the legal field (e.g. lawyers) or financial field (e.g. accountants or auditors).

5. Internet - Links

5.1. Switzerland

5.1.1 Money Laundering Reporting Office Switzerland

www.fedpol.admin.ch	Federal Office of Police / MROS

5.1.2 Supervising authorities

http://www.ebk.admin.ch/	Federal Banking Commission
http://www.bpv.admin.ch/	Federal Office of Private Insurance
http://www.gwg.admin.ch/	Federal Finance Administration/Money Laundering Control Authority
http://www.esbk.admin.ch/	Federal Gaming Commission

5.1.3 National associations and organisations

www.swissbanking.org	Swiss Bankers Association
www.swissprivatebankers.com	Swiss Private Bankers Association

5.1.4 Others

http://www.zoll.admin.ch/	Federal Customs Administration
www.snb.ch	Swiss National Bank

5.2. International

5.2.1 Foreign reporting offices

http://www.fincen.gov/	Financial Crimes Enforcement Network/USA
www.ncis.co.uk	National Criminal Intelligence Service/United Kingdom
www.austrac.gov.au	Australian Transaction Reports and Analysis Centre
www.ctif-cfi.be	Cel voor Financiele Informatieverwerking / Belgien

5.2.2 International organisations

www.fatf-gafi.org	Financial Action Task Force on Money Laundering
http://www.unodc.org/	United Nations Office for Drug Control and Crime Prevention
http://www.egmontgroup.org/	Egmont Group
www.cfatf.org	Caribbean Financial Action Task Force

5.3. Other links

www.europa.eu.int	European Union
www.coe.int	European Council
www.ecb.int	European Central Bank
www.worldbank.org	World Bank
www.bka.de	Bundeskriminalamt Wiesbaden, Deutschland
www.fbi.gov	Federal Bureau of Investigation, USA
www.interpol.int	Interpol
www.europol.eu.int	Europol
www.bis.org	Bank for International Settlements
www.wolfsberg-principles.com	Wolfsberg Group
www.swisspolice.ch	Conference of the Cantonal Police Commanders of Switzerland