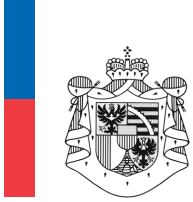


STABSSTELLE FINANCIAL INTELLIGENCE UNIT
DES FÜRSTENTUMS LIECHTENSTEIN

Annual Report 2018

Financial Intelligence Unit (FIU)
of the Principality of Liechtenstein

Financial Intelligence Unit (FIU)
of the Principality of Liechtenstein
Äulestrasse 51
FL-9490 Vaduz
Telephone +423 236 61 25
Fax +423 236 61 29
E-mail info.sfiu@llv.li
Website www.fiu.li

Table of contents

The greatest mistake is to
imagine that we never err.

Thomas Carlyle

I. Foreword

Dear Readers
Dear Colleagues

A successful strategy to combat money laundering and terrorist financing rests on two pillars: prevention and repression. With its mandate to obtain and analyse information for the detection of money laundering, predicate offences of money laundering, organised crime, and terrorist financing, the FIU forms the link between the private sector and the prosecution authorities.

The FIU makes a key contribution to combating abuse: The FIU is situated where prevention is not sufficient and where repression at an early stage would be contrary to the rule of law, and so it is able to take the lead in identifying and measuring the risks, take immediate measures, and filter out information that may form the basis for successful prosecution. To fulfil its mandate, the FIU relies on effective exercise of the reporting obligation by the persons subject to due diligence, on a sound assessment of risks, on smoothly functioning international cooperation, and on close coordination with the prosecution authorities.

The number of reports of suspicion (SARs/STRs) increased significantly in 2018. A precise comparison with the previous year is not possible due to the new data processing system goAML, but the clear increase in the number of reports of suspicion shows a growing awareness on the part of persons subject to due diligence. This is an important step towards strengthening the defensive system.

The assessment of risks has improved with the completion of the first National Risk Analysis (NRA) at the beginning of 2018. Due to methodological considerations, however, the result was not yet sufficiently expressive. Risk assessment is an ongoing process, and the next NRA report will be even sounder thanks to the additional data available.

Far more than 90% of suspected cases have a foreign link: Without smoothly functioning international cooperation, the FIU would be flying blind. International cooperation is based on the rules and mechanisms of the Egmont Group, which guarantee a high degree of effectiveness and confidentiality, predictability, and security. To ensure that this remains the case, the FIU was again engaged in the Egmont Group in the year under review, for instance by heading the project to set up the Egmont Centre of FIU Excellence and Leadership (ECOFEL). On the basis of this work, the Egmont Group received more than 10 million Canadian dollars from the governments of Switzerland and the UK for the establishment of ECOFEL.

Finally, one of our concerns is to ensure a level playing field for all countries. Our involvement in MONEYVAL and the FATF makes a contribution in this regard.

Cooperation with the prosecution authorities clearly improved in 2018: We now have a stronger common understanding of the content of analytical reports, and our approach towards larger clusters of cases is now more frequently aligned.

Successful cooperation was also evidenced with other authorities: Of particular note is the Liechtenstein Initiative for a Financial Sector Commission on Modern Slavery and Human Trafficking, which was launched together with the Office for Foreign Affairs and is jointly funded by the State and the private sector. The authorities are also working well together on the implementation of international sanctions. The revision of the ISG represents a major step towards increased effectiveness and stronger rule of law.

This is the last Annual Report under my direction. As much as I am looking forward to my new responsibility in Switzerland, I will miss the many positive moments in Liechtenstein over the past nearly eight years, most of them together with my colleagues in the FIU. I wish you – and especially my highly esteemed successor Michael Schöb – all the best, much success, and a strong backbone.

Vaduz, July 2019
Daniel Thelesklaf

II. Activities of the FIU

The Financial Intelligence Unit (FIU) is the central authority for obtaining and analysing information necessary to detect money laundering, predicate offences of money laundering, organised crime, and terrorist financing. Its core responsibilities are to receive and analyse reports of suspicion – suspicious activity reports (SARs) and suspicious transaction reports (STRs) – from persons subject to due diligence and to implement the coercive measures set out in international sanctions. The FIU's work in 2018 also focused on dealing with the IMF recommendations of 2014, preparing for the next MONEYVAL country assessment, participating in international bodies, and contributing to the activities of the interagency working group PROTEGE (Working Group on Combating Money Laundering, Terrorist Financing, and Proliferation). PROTEGE serves to coordinate work relating to the further development of Liechtenstein's defensive mechanisms against money laundering, terrorist financing, and organised crime. In addition, the working group has proven to be a suitable body for assessing fact patterns as they arise and coordinating appropriate measures. The FIU also took the lead in carrying out a National Risk Assessment for money laundering and terrorist financing, which was completed at the beginning of 2018.

In 2018, the total number of reports to the FIU reached a new record high. A total of 454 reports were submitted. While the number of reports under the International Sanctions Act (ISG) remained constant, the number of reports under the Due Diligence Act (SPG) increased significantly in 2018. The focus continues to be on fact patterns relating to fraud and corruption offences. There was a significant increase in cases of corruption compared with the previous year. In the year under review, a small number of indications of possible terrorist financing also arose.

1. Receipt and evaluation of reports of suspicion

In 2018, the FIU received a total of 454 reports of suspicion (SARs/STRs) pursuant to the Due Diligence Act (SPG). This is a significant increase over the previous year, but the increase is below average compared with other financial centres.

Of these reports of suspicion under the SPG, 309 (68%) came from banks, 82 (18%) from the fiduciary sector, 37 (8%) from the insurance sector, 7 (2%) from other authorities (mainly the FMA), and 19 (4%) from other persons and entities subject to the reporting obligation. With the exception of "other authorities", the absolute number of cases for all groups of persons and entities subject to the reporting obligation increased significantly over the previous year.

Most reports of suspicion are still triggered by external factors (e.g. requests for mutual legal assistance, criminal proceedings, media reports, or hits in commercial databases).

In 2018, the FIU prepared 138 analysis reports for the Office of the Public Prosecutor, mainly involving fact patterns where the suspicion of money laundering had been substantiated. This figure also increased significantly over 2017.

As has been the case over the past 20 years, the types of offences have predominantly been economic offences (especially fraud, criminal breach of trust, bankruptcy offences). The increase in corruption offences in recent years was again confirmed during the year under review.

As in previous years, most reports of suspicion concerned persons abroad, even though purely domestic cases (20%) were analysed more frequently in 2018 than in the past. 60% of the persons who were the subject of reports of suspicion came from other European countries (of which approximately 80% from Switzerland and EU countries), while 20% were domiciled outside Europe.

2. Combating terrorist financing

Combating terrorist financing is an integral component of the FIU's activities. International cooperation, responding to enquiries, and carrying out clarifications for domestic and foreign authorities are of central importance.

3. Enforcing international sanctions

The number of reports under the Law on the Enforcement of International Sanctions (a total of 10 reports and applications) stabilised at the level of previous years.

4. International cooperation

In cases with an international link, the FIU engages in targeted cooperation with other FIUs, requesting them to provide information or documents necessary for the analysis of a case. The FIU grants corresponding requests from abroad if the requirements set out in the FIUG are met. The number of requests in this context decreased slightly from the previous year. Exchange of information is governed by national legislation and the Principles of Information Exchange established by the Egmont Group of Financial Intelligence Units. International cooperation is not limited to case-specific exchange of information, however, but also includes a general exchange of experience and participation in in-

ternational working groups and organisations such as MONEYVAL, the FATF, the International Monetary Fund, the World Bank, and the United Nations. In addition, the FIU has been designated by the Government as the national focal point of the United Nations Office for Drugs and Crime (UNODC) for asset recovery.

4.1. Egmont Group

The Egmont Group is the worldwide association of 159 national financial intelligence units (as of December 2018). The main work of the Egmont Group consists in particular in setting out the rules governing the exchange of information among the national financial intelligence units and ensuring that such exchange takes place in practice. The FIU has been a member of the Egmont Group since June 2001. The Director of the FIU represented Europe Region II during the year under review and served in that capacity on the Egmont Committee, the group's consultation and coordination mechanism. In August 2018, the FIU Liechtenstein hosted the meeting of the Egmont Committee in Malbun.

4.2. MONEYVAL

MONEYVAL is a committee of experts of the Council of Europe founded in 1997 to support the member states in their fight against money laundering and terrorist financing. MONEYVAL conducts a process of peer reviews. The goal of this process is to ensure that the member states' systems to combat money laundering and terrorist financing are effective and that they comply with the relevant international standards in this field (FATF, Council of Europe, and EU). Liechtenstein will soon be reviewed for the fifth time by MONEYVAL in regard to compliance with these standards. As preparation for this country assessment, the FIU simulated an external country assessment and informed the Government of the outcome.

4.3. FATF

The FATF is an international organisation whose mandate is to analyse the methods of money laundering and terrorist financing and to develop measures to combat them. It is the global standard-setter in this field and currently consists of 37 members. The current minimum standard ("40 Recommendations") was revised in 2012. Since 2015, all members have been reviewed for compliance with and effective application of this standard. Thanks to Liechtenstein's membership in MONEYVAL, the country is also indirectly represented in the FATF.

5. goAML IT solution

In addition to the basic IT infrastructure provided by the National Administration, the FIU has specially designed software and database systems at its disposal for its operational and strategic analysis. Work to replace the existing IT system was completed in 2018. This resulted in substantial additional efforts, which the FIU was, however, able to manage with its existing resources. We would like to take this opportunity to thank all the persons subject to due diligence involved in the implementation of the new system for their participation and their contribution to the successful launch at the beginning of 2019. With the new system, goAML, the FIU will be able to work much more efficiently. The statistics prepared by the FIU will also be adapted to the specifications of the new system.

In connection with the implementation of the new software solution goAML, access to the registration page has been linked to the FIU website, www.fiu.li. Documents are available there for registration and for setting up an interface, as well as a user manual for persons subject to due diligence and for the administrative offices and authorities that wish to communicate with the FIU using this secure channel.

The advantages of goAML for persons subject to due diligence consist primarily in electronic data transmission in a secure environment instead of the previous paper solution and in the possibility of transmitting information using an XML interface. The new database makes it easier for the FIU to reconcile the information it receives and to focus on its mandate to analyse the information necessary to detect money laundering, predicate offences of money laundering, organised crime, and terrorist financing.

III. Case studies/Current practice

1. Introduction

The fact patterns described below come from the practice of the FIU and concern the current reporting period. The case studies are selected with a view to topics identified as relevant, with the goal of illuminating specific questions and developments relating to reporting, as well as trends identified by the FIU with regard to money laundering and predicate offences of money laundering.

These insights and developments also serve as a basis for the FIU to further develop its guidance on the submission of SARs/STRs [https://www.llv.li/files/sfiu/fiu-wegleitung_deutsch.pdf]. They also form the basis for lectures and training sessions at which representatives of the FIU appear as speakers. The goal is to ensure that persons subject to due diligence and their compliance officers receive assistance in their daily work that is as close to practice as possible.

The focus in the year under review is on transaction behaviour and the documentation relating thereto, specious beneficial owners, precious metals trading and custody, and challenges relating to international sanctions. The current case law on Article 17 SPG is also discussed, including confirmation of the legal opinion set out in the FIU guidance.

2. Case law

During the year under review, the Court of Appeal confirmed a decision of the Court of Justice, in which the latter found that a person subject to due diligence had wrongfully considered a suspicion not worth reporting, despite indications to the contrary.[1] The Court consequently found those responsible for submitting the report and the undertaking itself guilty of violating the first sentence of Article 17(1) of the SPG, sentencing the natural persons to suspended monetary penalties for having committed a misdemeanour under Article 30(1)(a) SPG and the undertaking, as the responsible legal person, to a suspended corporate penalty under § 74b StGB.

In summary, the fact pattern indicates that the person subject to due diligence had relied on the information provided by the bank maintaining the account abroad, despite having demonstrable knowledge of allegations against a referred long-standing client: In both Pythagoras and WorldCheck, the client was linked to a bribery scandal, and there were also indications of international arrest warrants and even reports of the clients arrest. The special clarifications carried out by the person subject to due diligence were limited to the foreign banks' view that it did not identify any risk, given that all inflows had been verified and had originated from the client's accounts, and therefore no suspicion of money laundering or criminal origin of the assets was discernible. The person subject to due diligence also argued that no report needed to be submitted to the FIU, given that procedures were already being carried out abroad which resulted in freezing of the client's assets. In further special clarifications carried out one year later, the same conclusion was reached, and the statement of the bank was also cited, according to which the bank conceded that it could of course not be certain from which source the assets on the private accounts had originated. On the basis of a recommendation by the auditors, the person subject to due diligence did end up reporting a suspicion about two weeks after the note had been made concerning the special clarifications.

In its decision, the Court of Justice held that, given that "suspicious facts" trigger an obligation to carry out clarifications, it must necessarily be concluded that mere suspicious facts alone do not trigger the reporting obligation under Article 17(1) SPG. Otherwise, the due diligence obligation under Article 9(4) SPG to carry out special clarifications in the context of risk-adequate monitoring of the business relationship would not make sense. In light of the exclusion of criminal and civil liability set out in Article 19(1) SPG, however, there was no reason to set a high threshold for suspicions triggering the reporting obligation; neither urgent nor well-founded suspicions would be necessary. With regard to the obligation to report "immediately", the Court of Justice found that the report had been submitted far more than a year later and, therefore, no longer in a timely manner.

In its decision, the Court of Appeal also referred to the guidance issued by the FIU on the submission of SARs/STRs, and it emphasised the accuracy of the opinion contained therein that the threshold for suspicion is in any event reached if clarifications carried out in accordance with Article 9(4) SPG as part of risk-adequate monitoring are unable to dispel suspicions concerning fact patterns.

The FIU guidance expresses the following view regarding the timing of submission of reports:

"According to Article 17 SPG, the suspicion must be reported immediately, which means that the report must be submitted as soon as the suspicion arises. No general time requirement can be made, but must be decided on a case-by-case basis. In no cases, however, are delays permissible (e.g. due to the holidays of an employee). As a rule, in the case of ongoing business relationships, the report is subsequent to the clarifications carried out in accordance with Article 9 SPG. But the report must be made as soon as the suspicion exists, even if, in a given case, the special clarifications are not yet completed. The person subject to due diligence must set up the internal organisation in such a way that the decision can be made immediately by the responsible body."

[1] see Decision 14 EU.2018.50

This makes it clear that the obligation to report a suspicion in a given case may well be triggered before the special clarifications have been concluded. This is also supported by the findings of the Court of Appeal regarding the exclusion of criminal and civil liability under Article 19(1) SPG and the fact that a suspicion need not be well-founded (as is required by the Swiss legal order, for instance).

3. Bank account, life insurance policy, and purchase of gold coins

Indicators

- bank-internal transfers between different persons involved
- life insurance policies/total surrender of policies/no evident relationship between policyholder and identified beneficial owner
- purchase of gold coins from surrender value of life insurance policy with payment to third party

In September 2014, N, an EU citizen, entered into a business relationship with a bank in Liechtenstein. The client chose to have correspondence retained at the bank. According to the profile, the assets to be contributed were transferred from an account located in Switzerland. The client was referred to the bank by an asset management undertaking in Liechtenstein.

One year later, N signed an application for a life insurance policy with a life insurance company in the Bahamas. This application was signed in Vaduz. N was listed as the policyholder, insured person, premium payer (single premium), and beneficial owner of the policy. The beneficiary in the event of death was named as another person who was a resident and citizen of an EU member state. EUR 500,000.00 was then transferred as a single premium from the account in N's name at the domestic bank to the account at the same bank in the name of the life insurance company and the corresponding policy number.

Just under a year later, N initiated two partial policy surrenders in the amount of EUR 10,000.00 each in return for their cash value.

In the spring of the following year, a meeting took place between lawyers and the policyholder regarding a possible disclosure in N's country of residence. This was the only such meeting, however; it is unknown whether further steps were taken in that regard.

Another month later, the policyholder cancelled the life insurance policy and requested a transfer to a third party. This third party was an establishment in Liechtenstein which had sold gold coins to the policyholder for a price equal to the surrender value of the policy. This establishment likewise held the bank account used for that purpose at the same domestic bank.

The fact pattern described is the result of an analysis, and it gives rise to the assumption that assets not declared for tax purposes were possibly put first into the business relationship in N's name, then into an insurance policy, and finally into the purchase of gold coins.

The behaviour of the bank involved in this case is particularly striking. Given that all the transactions were conducted via accounts of that same institution, the bank should have carried out simple and/or special clarifications of the business relationship under the SPG. At the end of the process, the bank should then have decided whether or not to report any suspicions. In this case, the bank decided against doing so. After analysing the fact pattern, the FIU decided to refer the case to the Financial Market Authority for further assessment.

4. Pass-through transactions

The following example illustrates a relatively simple case of pass-through transactions. The FIU has commented repeatedly on the issue of pass-through transactions. Pass-through transactions are undisputed indicators as enumerated in Annex 3 of the Due Diligence Ordinance and consequently require clarifications to be initiated and carried out. In addition, however, pass-through transactions using "service companies" have recently become known on a large scale as an incalculable risk for financial institutions. The procedure is similar to that used in the discovered Laundromat cases involving organised crime assets and renowned European banks. The magnitude of the following example is in no way comparable to that of the Laundromat cases. However, it clearly shows that the Laundromat cases are scalable and that the resulting effort for compliance multiplies many times over with pass-through transactions, even with a relatively small number of business relationships.

An account for a foreign company was held at a domestic bank. Over the course of three weeks, this account was endowed by EUR 2 million by way of four transactions. The assets all came from the same account held at a bank in an EU country. All payments had extensive documentation in common. According to that documentation and the business profile, the account holder was a company trading in metal products, specifically copper.

Each of the four incoming payments to the account of the domestic bank was transferred at most five business days to a total of six companies with accounts in Germany, Turkey, Poland, Romania, and Lithuania. On the basis of the documentation provided, these payments also corre-

sponded to the profile of the business relationship, since the transactions in question appeared to be in the metal sector.

The FIU became aware of the fact pattern in the context of an enquiry addressed to it, and it also conducted research in (online) public sources regarding the companies with accounts abroad that acted as business partners of the metal trader with a domestic account. The brief research revealed that the contracting parties and thus the sellers of copper products were active in the following sectors:

- trading in stones
- online marketing
- trading in clothes, shoes, and jewellery
- wholesale in furniture, carpets, and lighting equipment

Since the bank has not reported any suspicion in this case, it can be assumed either that special clarifications dispelled the described indicators of money laundering, predicate offences of money laundering, organised crime, or terrorist financing, or that such special clarifications were not carried out.

The FIU would emphatically like to draw attention here to the risks associated with pass-through transactions. Numerous cases have been uncovered in which the payment documentation appears to be detailed and is readily provided. On closer inspection, however, the contracts turn out to be empty documents, some of which can even be found as templates on the internet. This phenomenon is not limited to loan or consulting agreements, which should of course always be treated with caution; there has also been a rise in cover stories that appear to be coherent across multiple steps. As a rule, however, mistakes are almost always hidden in even the most sophisticated stories, which can cause the entire house of cards to collapse.

5. Small cog in a large machine

Indicators

- wrong beneficial owner
- opaque ownership structure
- "long-standing client" as an argument for own plausibility check
- underlying documentation
- use of several domiciliary companies that appear to have business relationships

In the course of dealing with and investigating an international case of corruption and bribery originating in South America, it was discovered that a company involved in the case, domiciled in the British Virgin Islands, had an account with a Liechtenstein bank. According to the bank's documentation, the beneficial owner of this account was a long-standing client who himself worked abroad as an asset manager.

It turned out that this company's account served as a vehicle for surreptitiously passing money to public officials in the context of bribery payments. This happened in such a way that the account received assets from other companies domiciled in Panama and the British Virgin Islands as well as other locations, which in turn were under the control of the actual beneficiary of these payments. The assets were received partly as bank transfers and partly as cash and cheque payments. The bribery payments were aimed at the award of contracts for major construction projects in those countries.

For the purpose of further concealment, the money did not remain on the company's account but rather was transferred within the same bank to accounts held by a life insurer, which then opened three life insurance policies with the company as the holder. The asset manager mentioned at the outset was named as the asset manager for the policies.

In the course of further analysis, it was determined that the asset management company domiciled in Europe for which the asset manager worked was wholly owned by a Luxembourg company. One third of their shares – as was known by the bank – were in free float, while one third each were owned by the asset manager himself and by a company domiciled in the British Virgin Islands. The beneficial owner of that company in turn was a woman from South America. Using information obtained from commercial databases, it was ascertained that that woman's brother was in a leading position in a state enterprise involved in acts of corruption.

The overall appraisal of this case turned out to be difficult. Since various probably unrelated transactions were carried out using the account at the bank, and since the personal links between the involved persons could not be conclusively ascertained or explained, it must be assumed that the account appears to have been used by the asset manager to conduct a wide range of transactions. However, all these transactions appear to have in common that the method used to create discretion can in no way be reconciled with the legal provisions in force.

6. Fictitious fiduciary transactions

Indicators

- reasonableness of the structure (overall picture)
- fictitious contracts
- cash payments

A domestic professional trustee founded a Liechtenstein company for a client; based on the company name, the company seemed to be active in consulting and investment. This company issued invoices to another company domiciled abroad, which in turn paid the amounts due into the bank account held in Liechtenstein. The purposes of the transactions indicated that they were intended to be commissions. Other invoices were evidently settled in cash. These invoices contained merely a sentence mentioning the invoicing of the amount for intermediary services as well as a stamp and signature indicating payment in cash. Overall, it turned out that payments totalling some EUR 2.5 million had been made in this way.

In the course of investigations conducted abroad, it was discovered that the client was also the general manager of the foreign company that served as the addressee of the invoices. That company in turn issued invoices to two other companies domiciled in a third country, which again were under the influence of the same client. These two companies yet again paid amounts back to the first company, on the basis of fictitious management contracts and empty invoices.

The client of the domestic professional trustee may thus have been guilty of forgery of documents, corporate fraud, and money laundering. It is up to the court to decide to what extent the professional trustee's conduct is criminal, given that the trustee had made a Liechtenstein company available whose sole purpose was to issue invoices for services that allegedly were never performed. As already stated in Report and Motion 2015-0114, it must be assumed that forged, falsified, or substantively incorrect documents were regularly used for the purpose of maintaining a re-invoicing company that had neither substance nor function.

7. Drugs and yacht

Indicators

- changing beneficial owners
- asset inflows and profile raise doubts
- receipt of surrender and confiscation ruling by the Court of Justice

A bank in Liechtenstein held an account for a company domiciled in the British Virgin Islands that owned a yacht operating predominantly in European waters. The shares in this company were sold by a lawyer in an EU country to a person in Asia. This deal was arranged by another person with citizenship and residence in an EU country. In the past, this person had repeatedly been the subject of proceedings and investigations relating to narcotics offences. In the person's country of residence, the person was considered destitute.

Shortly after the person in Asia bought the company, the person appointed the intermediary of the company purchase as the managing director and as the "representative" for the bank accounts managed on behalf of the company.

In financial terms, the purchase of the yacht was not transacted by the bank in Liechtenstein, and the bank's documentation on the changing beneficial owners over the years appeared plausible and conclusive. The account was to be used for the maintenance of the yacht. No information was found in public sources or commercial databases about the person involved in narcotics offences that would have provided indicators giving rise to the initiation of simple or special clarifications.

One day, the bank received a ruling from the Court of Justice ordering the surrender and confiscation of the property, and so it learned of the allegations made against the governing body of the business relationship maintained at the bank. The bank then reported its suspicion within six business days.

8. ISG freezing of assets in the international context

A Liechtenstein professional trustee managed a company with foreign bank accounts for a client. The beneficial owner of this business relationship and thus of the foreign assets was the subject of coercive measures in force in Liechtenstein, which were enacted in the form of ordinances on the basis of the Law on the Enforcement of International Sanctions.

Under the ordinance in question, the assets abroad were initially also frozen on the basis of the sanction provisions in force there. After these had been lifted, however, the Liechtenstein trustee faced the situation that the assets now released abroad were to be transferred to the client's home country, while the person was still subject to the sanctions in force under Liechtenstein law. The assets of the company were to be transferred to a private foreign account of the person still subject to Liechtenstein sanctions. From that foreign account, the assets would then have been transferred to the territory of the sanctioned person's country of origin.

In the context of this case, the FIU is providing interpretations for the following legal questions:

8.1. Can governing bodies in Liechtenstein approve repatriation via a foreign private account held by the listed person?

The person was listed in the annex under the applicable Liechtenstein sanctions ordinance. According to the ordinance, it was prohibited to transfer assets to the natural persons, entities, and organisations affected by the

freeze or to make assets and economic resources otherwise available, directly or indirectly. The Government therefore had no discretion and was unable to grant exemptions. The bans on transfers also applied to all persons and institutions performing administrative acts in Liechtenstein. If payments were to be executed by governing bodies in Liechtenstein, this would be punishable under Article 10 ISG.

8.2. Are assets situated abroad frozen by the Liechtenstein sanctions ordinance?

According to the Liechtenstein sanctions ordinance, assets and economic resources owned by or under the direct or indirect control of a listed natural person, entity, or organisation shall be frozen. The FIU is of the view that assets situated abroad are not frozen by Liechtenstein law. This means transfers from those foreign accounts would in principle be possible, even without approval by the Government. However, it is still prohibited to transfer assets to the natural persons, entities, and organisations affected by the sanctions or to otherwise make assets and economic resources available, directly or indirectly.

8.3. Is there a reporting obligation for Liechtenstein persons and organisations if assets or economic resources are situated abroad?

According to the Liechtenstein sanctions ordinance, persons and institutions which hold or administer the assets or which are aware of economic resources that should be assumed to be subject to freezing under Liechtenstein law must report this immediately to the FIU. In the FIU's view, the principle of territoriality also generally applies here. However, if persons and organisations in Liechtenstein are aware of assets or economic resources situated abroad, a report must be made to the FIU. The FIU will take note of the report and, where appropriate, contact the foreign authority on the basis of Article 7 ISG. Domestic persons subject to due diligence are not, however, exempt from any obligation to submit a report to the FIU under Article 17(1) SPG.

9. Risks in dealing with precious metals

A Liechtenstein bank submitted an STR regarding the unusual transaction behaviour of one of its clients. The client was a domestic buyer and seller of precious metals. The bank noticed several transactions originating from its client's account, involving changing recipients in various African countries. The special clarifications carried out by the bank showed that the Liechtenstein purchaser and seller of precious metals apparently was purchasing precious metals from two persons in neighbouring countries and then forwarding the purchase price on their behalf directly to recipients in various African countries. The two sellers of the assets stated that they were donating the proceeds to charitable projects.

Even though, in this specific case, a further analysis by the FIU was able to dispel doubts about the fact pattern as a whole, given that it turned out to be plausible, it should be expressly pointed out that the bank acted properly in this case by submitting an STR.

Due to the mostly low transaction amounts from the account of the domestic buyer and seller of precious metals – who, incidentally, is not subject to the provisions of the Due Diligence Act in Liechtenstein – a suspicion of money laundering, predicate offences of money laundering, or even terrorist financing could not be ruled out. In this context, the FIU draws attention to the fact that the coercive measures enacted under the Law on the Enforcement of International Sanctions must always also be taken into account in regard to transactions.

10. Own client as victim of fraud

Fact patterns unfortunately always arise in which a client of a Liechtenstein person subject to due diligence becomes a victim of a crime. Hacking cases appear to be especially fashionable right now. However, these attacks do not target clients' e-banking access, as one might suspect. Rather, the perpetrator hacks the e-mail account of a client or otherwise gains access to it. The attacker gains an overview of the correspondence conducted with a bank or professional trustee and then attempts to emulate that correspondence, with the goal of inducing the person subject to due diligence to transfer assets to the detriment of the rightful client.

In such cases, the FIU is of the view that a suspicious transaction report should in any event be submitted. According to the wording of Article 17(1), the preconditions for doing so are clearly met, because at the latest after the client has alleged that a transaction should not have been carried out, the person subject to due diligence is likely to suspect a predicate offence of money laundering.

This also or even especially applies to cases that progress no further than an attempt. It should also be pointed out that in such cases, it is especially important to report the suspicion "immediately", so that the potential perpetrators can be foiled in an international environment. Naturally, the chances of success depend on the available information. If account numbers (and especially IBAN numbers) of destination accounts affiliated with the perpetrators are identified, this is of course of particular interest.

As already commented on in our Annual Report 2014, the FIU also recommends filing criminal charges with the National Police in such cases. It should be noted,

however, that this step – whether taken by the client or the person subject to due diligence – does not release the person subject to due diligence from the obligation to submit an SAR/STR.

- Digression on Business E-mail Compromise (BEC) schemes

BEC schemes are currently a focus of increasing attention, also internationally. The Egmont Group has recently published guidance on its website at https://egmontgroup.org/sites/default/files/filedepot/external/20190708_EGMONT%20GROUP%20BEC%20BULLETIN-final.pdf, from which the following comments are drawn:

A. How BEC schemes work
BEC schemes generally involve impersonating victims to submit seemingly legitimate transaction instructions for a financial institution to execute. While BEC schemes differ in certain aspects, they all focus on using compromised e-mail accounts to cause financial institutions and/or their clients to make unauthorised or fraudulently induced payments or to send sensitive data to an unauthorised third party. BEC schemes can be broken down into three stages:

Phase 1 – Compromising victim information and e-mail accounts: Criminals first unlawfully access a victim's e-mail account, often through social engineering or computer intrusion techniques. Criminals subsequently exploit the compromised e-mail account to obtain information on the victim's financial institutions, account details, contacts, and related information.

Phase 2 – Transmitting fraudulent transaction instructions: Criminals then use the victim's stolen information to e-mail fraudulent payment or data transmission instructions to the financial institution, in a manner appearing to be from the victim. To this end, criminals will use either the victim's actual e-mail account they now control or create a fake e-mail account resembling the victim's e-mail. To support their instructions, the criminal may provide supporting documents, falsified for this purpose to enhance their apparent legitimacy.

Phase 3 – Executing unauthorised transactions: Criminals trick the employees of the financial institution into conducting transfers that appear legitimate but are, in fact, unauthorised or fraudulently induced. The fraudulent transaction instructions direct the payments to the criminals' accounts at domestic or foreign financial institutions. Financial institutions in East and Southeast Asia as well as Western and Eastern European countries are common destinations for these fraudulent transactions. However, it should be noted that criminals often adapt their strategies and that destination countries can change quickly.

2. BEC typologies
The following frequent BEC typologies should help persons subject to due diligence recognise BEC schemes in practice:

Scenario 1 – Criminal impersonates a client: A criminal hacks into and uses the e-mail account of a financial intermediary's client to send a payment order to the financial intermediary. Based on this order, the financial institution sends a transfer to an account controlled by the criminal.

Scenario 2 – Criminal impersonates an executive ("CEO fraud"): A criminal hacks into and uses the e-mail account of a company executive to send a payment order to an employee who is responsible for processing and releasing payments. The employee, believing the executive's e-mailed instructions are legitimate, releases the payment without knowing that the transfer is for the perpetrators' benefit.

Scenario 3 – Criminal impersonates a supplier: By e-mail, a criminal purports to be a supplier of a company or a service provider (e.g. real estate agent, trust company, or lawyer) and informs the potential victim that future invoice payments or deposits must be made to a new account number at a new location. On the basis of these instructions, the victim updates the payment information for the supplier and transmits the new transfer details to the financial institution, which subsequently executes the payments for the benefit of an account controlled by the criminal.

11. Promising start-up

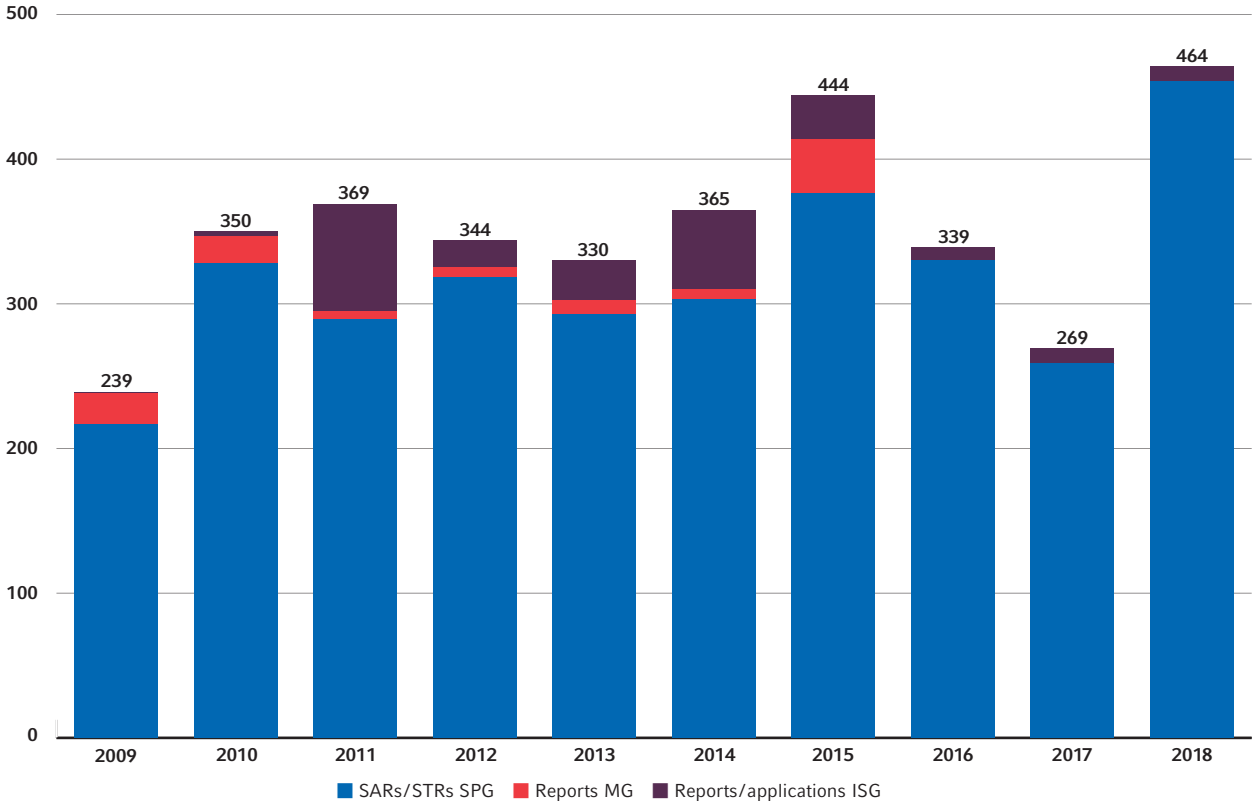
Indicators
- questionable network of companies
- unclear how the business model is actually supposed to make money
- only one deposit was made, which was then distributed to many natural and legal persons
- high level of personal consumption and conspicuous lifestyle

Based on allegations in public sources against a financier and his company in a neighbouring country, it was determined that the financier's investment promises had caused losses in the higher tens of millions. With his promises regarding the expected returns of the products he propagated, the financier managed to gain the trust of a large number of people. Through a widely branching network of companies with impressive-sounding names, he succeeded in placing the assets at various institutions, including a bank in Liechtenstein. Over the course of several years, these accounts were then used to pay returns that had evidently been promised to natural persons and to acquire real estate abroad.

IV. Statistics

1. Overall view

All SARs, reports, and applications for approval



	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
SARs/STRs SPG	217	328	289	318	293	303	376	330	259	454
Reports MG	21	19	6	7	9	7	38	0	0	0
Reports/applications ISG	1	3	74	19	28	55	30	9	10	10

2. Reports of suspicion under the SPG

This heading covers the SARs/STRs submitted to the FIU by persons subject to due diligence pursuant to Article 17 SPG in the case of suspicion of money laundering, a predicate offence of money laundering, organised crime, or terrorist financing.

2.1. Evaluation by sector

The reports of suspicion (SARs/STRs) received by the FIU in the years 2014 to 2018 came from the following sectors:

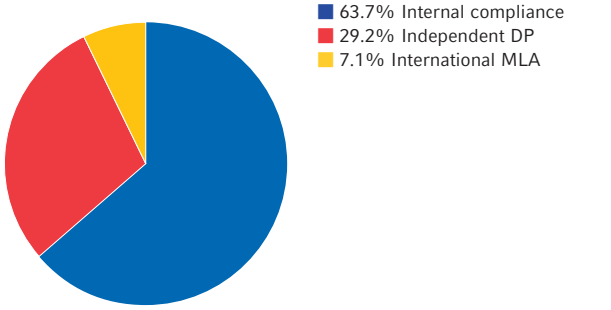
Branche	2014	2015	2016	2017	2018
Banks	192	245	221	163	**309**
Public authorities	7	10	14	12	**7**
Precious metal dealers	1	0	0	0	**0**
Dealers in high-value goods/auctioneers	1	0	0	0	**0**
Investment undertakings	0	0	0	0	**0**
Lawyers	6	7	7	1	**0**
Professional trustees/trust companies	63	65	56	48	**82**
Asset managers/management companies	4	3	0	2	**2**
Life insurers					**6**
Insurance undertakings	21	30	18	26	**31**
Electronic money institutions					**2**
Insurance brokers					**2**
Investment firms					**3**
Auditors/audit firms	1	3	0	0	**1**
PSPs (payment service providers)	7	12	10	5	**3**
Finance companies	0	0	0	4	**0**
Total	303	376	330	259	**448**

2.2. Reasons for submission

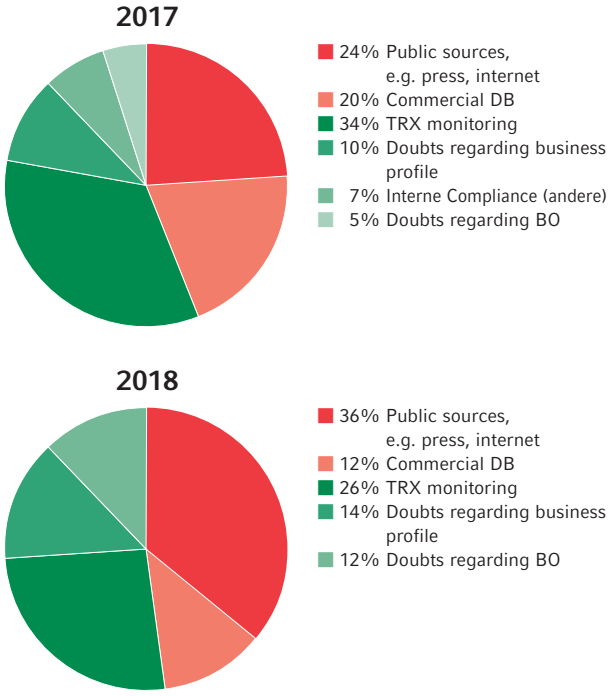
The reports of suspicion (SARs/STRs) are classified according to whether they

- were submitted pursuant to an institution's own investigations of unusual or conspicuous transactions (internal compliance),
- were submitted on the basis of knowledge gained by the person subject to due diligence pursuant to international requests for mutual legal assistance (MLA), or
- originated in independent domestic investigative proceedings (DP).

Reasons for submission



Breakdown of "Internal compliance"



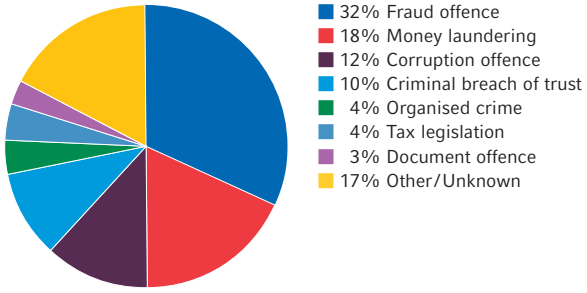
2.3. Statistics according to offence

These statistics provide information on the predicate offences (types, number, and places of commission) and on the origin of the contracting parties of the persons subject to due diligence and of the beneficial owners of the assets.

2.3.1. Predicate offences

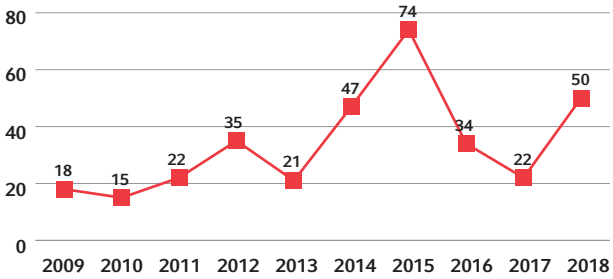
A predicate offence is the offence from which the assets originate or might originate or through which the assets have been generated. For the statistics, the predicate offences are relevant that are ascertained by the FIU's analysis of the reports of suspicion (SARs/STRs) pursuant to the Due Diligence Act, even where these results are only preliminary. This assessment may change over the course of any criminal proceedings that might be conducted.

Predicate offences



2.3.2. Corruption offences

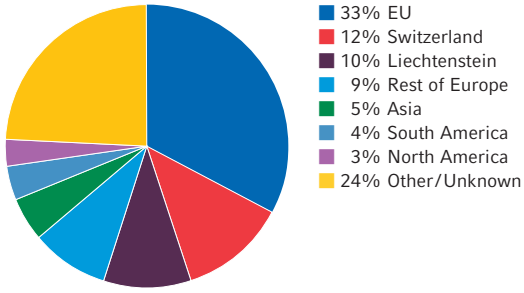
Corruption offences by year



2.3.3. Nationality/domicile of contracting party

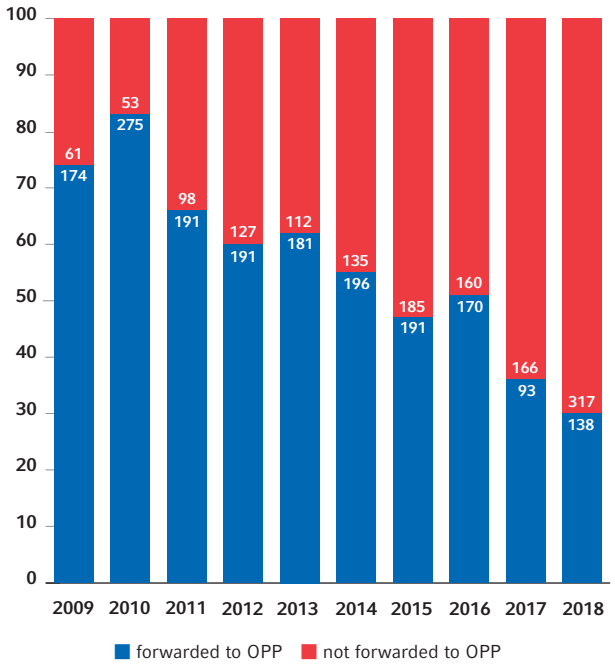
These statistics provide information on the origin (for natural persons) or domicile (for legal persons) of the contracting parties of the persons subject to due diligence indicated in the SAR/STR.

Nationalities/domiciles of contracting partys by region



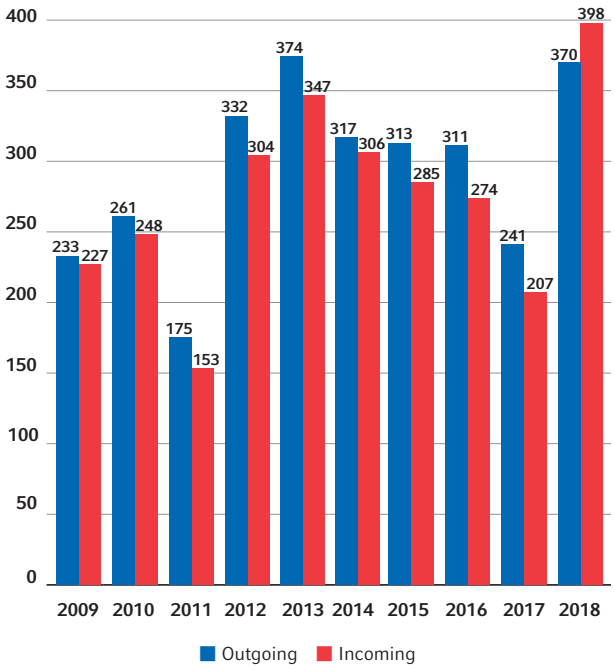
2.4. Analysis reports forwarded to the Office of the Public Prosecutor

SARs forwarded to the Office of the Public Prosecutor



2.5. International cooperation

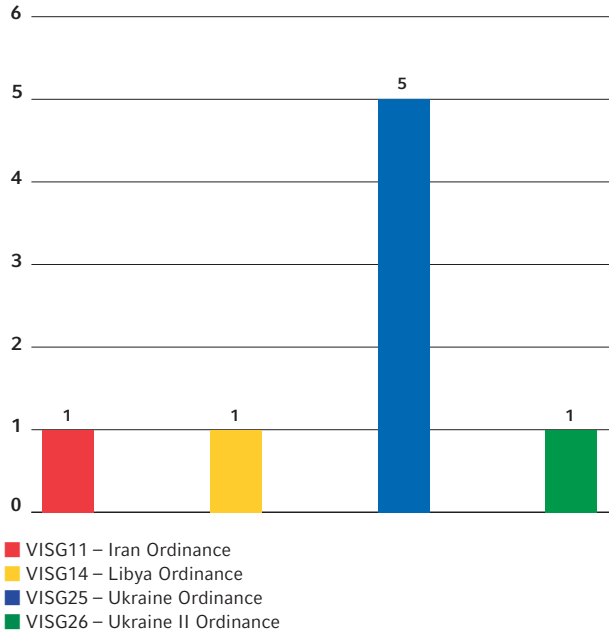
FIU information exchange



3. Approvals and reports under the ISG

This heading covers all reports and applications for approval transmitted to the FIU pursuant to an ordinance on coercive measures. Persons with their residence, registered office, or a branch in Liechtenstein are required to report or to submit an application for approval.

Reports and applications under the ISG



V. Abbreviations

DP	*Domestic proceedings*
EEA	*European Economic Area; Liechtenstein became a full member of the EEA on 1 May 1995*
EU	*European Union*
FATF	*The Financial Action Task Force is an expert group established by the G7 and the European Commission in 1989 with the mandate to analyse methods of money laundering and to develop measures to combat it. It currently consists of 36 members, including 34 jurisdictions and two international organisations (the European Commission and the Gulf Cooperation Council).*
FIU	*Financial Intelligence Unit*
FIUG	*Liechtenstein Law of 14 March 2002 on the Financial Intelligence Unit*
FMA	*Financial Market Authority Liechtenstein*
goAML	*Electronic reporting portal of the FIU for submitting reports of suspicion and for responding to requests for information*
ICRG	*International Co-operation Review Group (a working group of the FATF)*
IMF	*International Monetary Fund*
ISG	*Liechtenstein Law of 10 December 2008 on the Enforcement of International Sanctions (International Sanctions Act)*
MG	*Liechtenstein Law of 24 November 2006 against Market Abuse in the Trading of Financial Instruments (Market Abuse Act)*
MLA	*Mutual legal assistance*
MONEYVAL	*Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism*
OECD	*Organisation for Economic Co-operation and Development*
SAR	*Suspicious activity report (report of suspicion not involving a transaction)*
SPG	*Liechtenstein Law of 11 December 2008 on Professional Due Diligence for the Prevention of Money Laundering, Organised Crime and Financing of Terrorism (Due Diligence Act)*
StPO	*Liechtenstein Code of Criminal Procedure of 18 October 1988*
STR	*Suspicious transaction report (report of suspicion involving at least one transaction)*
TRX	*Transaction*
UNODC	*United Nations Office on Drugs and Crime*