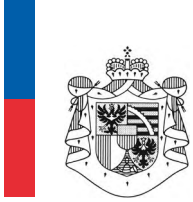


STABSSTELLE FINANCIAL INTELLIGENCE UNIT
DES FÜRSTENTUMS LIECHTENSTEIN

ANNUAL REPORT 2020

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
Email info.sfiu@llv.li
Website www.fiu.li

Table of contents

«… and Justice for All.»

James Hetfield

I. Foreword

Dear Readers

The year 2020 promised to be an interesting one. The Financial Intelligence Unit (FIU) was prepared: Due to entry into force of the TVTG – the Token and TT Service Provider Act – new persons subject to due diligence were expected to establish their registered offices in Liechtenstein. At the beginning of the year, it was not yet foreseeable by how much the reports of suspicion would increase. Taking into account the already rising trend in the reports of suspicion submitted in the «traditional» sectors, the FIU expected to be handling a significantly higher workload. These expectations were indeed realised, and the FIU recorded about double the number of reports of suspicion as in the previous year.

This challenging increase in the reports of suspicion could not be managed simply by more analysis work. The first step was rather to train a significant proportion of FIU employees to analyse this new category of reports. By the end of the year, half of the FIU's employees had received training in special modules, allowing them to carry out analyses using the appropriate blockchain analysis tools. In future, this skill will likely be part of the basic knowledge of an analyst as well as of a compliance officer in the private sector. Virtual currencies are becoming an integral part of the financial world, regardless of how this industry develops in Liechtenstein. Dealing with virtual currencies presents us all with completely new challenges, whether of a technical nature or whether they relate to financial products that have been rather rare in our financial centre until now. In addition to a wide range of new options for financial market participants, there is unfortunately also a certain potential for abuse through investment fraud, illegal services procured on the darknet, or the use of forged or fake identities. Research indicates, however, that only 0.34 % of all cryptocurrency transactions were connected with illegal activities in the year under review.[1]

In addition to expanding its own capabilities, the FIU conducted a large number of discussions with virtual asset service providers (VASPs), i.e., providers of services falling within the scope of the TVTG. Just as these new technologies are uncharted territory for us, the requirements of due diligence law present these new players with major challenges that they must master to protect the financial centre and especially its clients.

These challenges must be met not only through traditional means, but also through innovation. In the year under review, the FIU increasingly sought cooperation with national and international authorities for the purpose of exchanging information. The FIU also participated in an international project of various FIUs on trade-based money laundering in order to strengthen relevant expertise within the FIUs through the exchange of experiences. The FIU also began to form private-public partnerships with selected partners from the private sector for the purpose of discussing bilateral and multilateral analyses on a wide range of issues.

The year 2020 as a whole was full of challenges, further accentuated by the at times massive restrictions due to the coronavirus pandemic. In terms of content, the FIU observed a trend towards more cases of fraud and corruption, although most of the reports of suspicion submitted in the year under review were not clearly due to a predicate offence – which, in the FIU's view, is entirely consistent with the defence mechanisms of the Due Diligence Act. Nevertheless, a significant number of reports of suspicion continue to be submitted rather late, given that too much time is still allotted to special clarifications. Interestingly, this behaviour can be seen equally in reports of suspicion submitted in the traditional sectors as well as in the VASP sector.

Liechtenstein undergoes its country assessment this year, and with it we will again enter an extremely intensive phase of examining the existing AML regime along with its strengths and weaknesses. The speed of evolving innovations and the constantly changing environment make it clear that resting inevitably leads to rusting. For this reason as well, we have decided to tread new paths with this year's annual report, introducing a new vehicle instead of the annual report to present current cases from the FIU's practice to persons subject to due diligence. Alongside training courses and public appearances, we now plan to issue a practice at least twice a year.

Vaduz, March 2021
Michael Schöb

1 see The Chainalysis 2020 Crypto Crime Report, *https://go.chainalysis.com/2020-Crypto-Crime-Report.html*

II. Activities of the FIU

The 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. Alongside operational analysis, the FIU's work in the reporting year mainly involved updating the National Risk Assessment and preparing for Liechtenstein's country assessment by MONEYVAL. By far the bulk of the FIU's energy was spent on processing and analysing reports of suspicion, however.

The number of reports of suspicion submitted in 2020 can no longer be compared with that of previous years without providing background information to explain the trend. A total of 1671 reports of suspicion were submitted, corresponding to an increase of 125 % over the previous year. However, only one third of this substantial growth is attributable to reports of suspicion comparable to those submitted in the previous year. The remainder originated with virtual asset service providers (VASPs), who have been registered for the first time since 1 January 2020 under the regime of the TVTG – the Token and TT Service Provider Act – and are therefore now considered persons subject to due diligence under the Due Diligence Act (SPG).

The traditional reports of suspicion continued to focus on fact patterns relating to fraud and corruption. In the year under review, significantly more analysis reports (including supplementary reports) were submitted to the Office of the Public Prosecutor (+113 %), the Financial Market Authority (+105 %), and the Fiscal Authority (+100 %) than in the previous year. These figures may of course fluctuate greatly, given that they depend on a wide variety of factors such as the scope and complexity of the analysis, dependence on external information, and preparatory work by the compliance units of the persons subject to due diligence. The additional personnel resources within the FIU had a positive impact, which relieved the burden on analysts, especially in regard to data preparation.

1. Receipt and evaluation of reports of suspicion

Of these reports of suspicion under the SPG, 844 (51 %) came from banks, 679 (41 %) from VASPs, 102 (6 %) from the fiduciary sector, 19 (1 %) from the insurance sector, 4 (0.2 %) from casinos, and 13 (0.8 %) from public authorities (mainly the FMA). With the exception of the fiduciary sector and the casinos, the absolute case numbers rose again significantly compared with the previous year among all groups subject to the reporting requirement.

Most sectors thus recorded an increase in the number of reports of suspicion, with the banking sector in particular showing a very high growth of 56 %.

The FIU's repeated criticism of reporting behaviour over many years, pointing out that reports are often submitted too late and only after excessively long special clarifications have been carried out, along with the failure to take account of information in public sources and the potential for better calibration of automatic transaction monitoring systems, continues to be justified in the year under review, even though significant progress has been noted. Especially in connection with discontinuation of business and the associated reviews of long-standing mandates, clear compliance failings also came to light, arising from inadequate analysis of "old" business relationships. Findings in this regard were reported to both the Office of the Public Prosecutor and the Financial Market Authority.

Improvements were seen in reporting without a business relationship. A total of 30 reports of suspicion were submitted where a suspicion within the meaning of Article 17(1) SPG arose already before a concrete business relationship was established. 29 of these reports wer submitted by banks and one by a trust company. In its guidance on the submission of reports of suspicion (https://www.llv.li/inhalt/118042/amtsstellen/dokumente), the FIU draws attention to the obligation to submit reports of suspicion in these cases as well, provided that a suitable basis exists, such as names, account numbers, details of companies, documents (such as cheques or copies of identity documents), or other information. These important details help the FIU, and subsequently also the persons subject to due diligence, to better understand the behaviour of potentially criminal subjects, to follow their thinking, and also to see how the story they tell may change after they are rejected by a person subject to due diligence, in order to meet the compliance requirements of the next person subject to due diligence they approach.

Analyses of fact patterns relating to fraud as well as those relating to international corruption cases continue to be essential areas of the FIU's daily work. However, an increasing number of fact patterns are being reported as suspicious in light of the constellation and behaviour of the persons involved and without specific indications of a predicate offence. Such analyses are as a rule associated with greater effort, given that a single analysis body often gets to see only part of the whole – a single piece of the puzzle. It has also been noted that the focus on money laundering and the associated search for the underlying criminal act or specific predicate offence can lead to essential aspects being ignored. It is increasingly

being recognised that international financial centres and the defence mechanisms of persons subject to due diligence are vulnerable in regard to other aspects of the preventive system as well. A narrow focus on the search for the predicate offence obscures the view of activities aimed at circumventing international sanctions and financing of terrorism or proliferation. Greater attention must also be paid to the "new" world of virtual currencies, which is forcing all persons subject to due diligence to deal with the associated challenges. These challenges are many-faceted – investments in tokenised assets, investments in crypto funds, exchanging bitcoins for euros, or purchasing legal goods on the internet/darknet, to name just a few.

A few fact patterns were also noted in connection with the trade in Covid protective material, especially where suppliers offered products of questionable origin or quality for sale on the internet. Cases were also reported in connection with the conclusion of purchase contracts with unfavourable terms where commission payments were at the same time made to persons acting as agents for the buyers. The international federation of FIUs supports the fight against the risks arising from the Covid crisis by means of specifically designed training content for analysts in order to detect and suppress such activities.

2. Combating terrorist financing

In the year under review, the tragic impact of terrorist financing was seen in our neighbouring countries. The early detection of financing in such cases proves to be extremely challenging. Especially in this sensitive area, the FIU advises submitting a report of suspicion at an early stage if any indicators arise. Findings from the year under review show that VASPs – i.e. the new category of persons subject to due diligence under the TVTG – and the traditional persons subject to due diligence are equally vulnerable to this risk. By expanding its range of financial services into the area of virtual assets, Liechtenstein is assuming a special responsibility for the services it offers worldwide. The focus of service providers must be on early detection and – where an event occurs – rapid assessment of their own involvement and submission of reports of suspicion where applicable. Speed, completeness, and accuracy of the information provided to the FIU are of the utmost importance. Service providers who fail to turn their attention to these processes at an early stage will be unable to understand and comply with their legal obligations if an event occurs.

3. Enforcing international sanctions

The FIU has identified a great need to raise awareness among persons subject to due diligence in regard to the enforcement of international sanctions. Enforcement of international sanctions was therefore declared the key topic for training sessions, presentations, and private-public partnerships in the year under review and was visualised using examples.

Circumventing sanctions, along with bribery and corruption, is facilitated by the abuse of legitimate processes and services. Auditors, lawyers, and fiduciaries can be used by criminals, in some cases negligently or even unknowingly. Criminals act as intermediaries and use their skills, knowledge, and abilities to create documentation, transfer funds, and create highly complex structures that move large amounts of criminal money and effectively conceal ownership. The involvement of services offered in the financial centre not only damages its reputation, but also torpedoes international efforts in these areas. It is therefore important to create a high level of awareness in these issues beyond money laundering as such.

4. International cooperation

In cases with an international nexus, 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 FIU Act (FIUG) are met. The number of requests in this context was stable, while active exchange of information increased substantially with entry into force of the TVTG, due to links with customers obtaining services from VASPs. 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 international working groups and organisations such as MONEYVAL, the FATF, the International Monetary Fund (IMF), the World Bank, and the United Nations.

4.1. EGMONT Group

The Egmont Group is the worldwide association of currently 166 national financial intelligence units. 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. Two FIU staff members participated in two Egmont Group project working groups looking at large-scale transnational money laundering.

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 be reviewed in September 2021 for the fifth time by MONEYVAL in regard to compliance with these standards.

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.

III. Focus: VASPs

1. Overview

With entry into force of the Token and TT Service Provider Act (TVTG) on 1 January 2020, virtual asset service providers (VASPs) became subject to the Due Diligence Act (SPG). In the autumn of 2019, initial talks were held in this regard with individual market participants in the new VASP sector. The primary aim was to gain insights into the envisaged underlying business models, to clarify substantive questions regarding the handling of SPG obligations relevant to the submission of reports of suspicion, and to discuss technical questions regarding the transmission of reports of suspicion (including installation of a goAML interface).

Since these initial positive talks with market participants, the FIU has made intensive efforts to keep its overall view current with respect to companies active on the Liechtenstein VASP market. This process is supported by close cooperation on VASP issues with the Financial Market Authority and by continuous and personal exchanges with market participants and their representatives. The FIU is in general very pleased with the interest and engagement shown by the VASP sector in its efforts to rapidly implement the relevant provisions of the SPG and the requirements set out in the relevant FIU guidance.

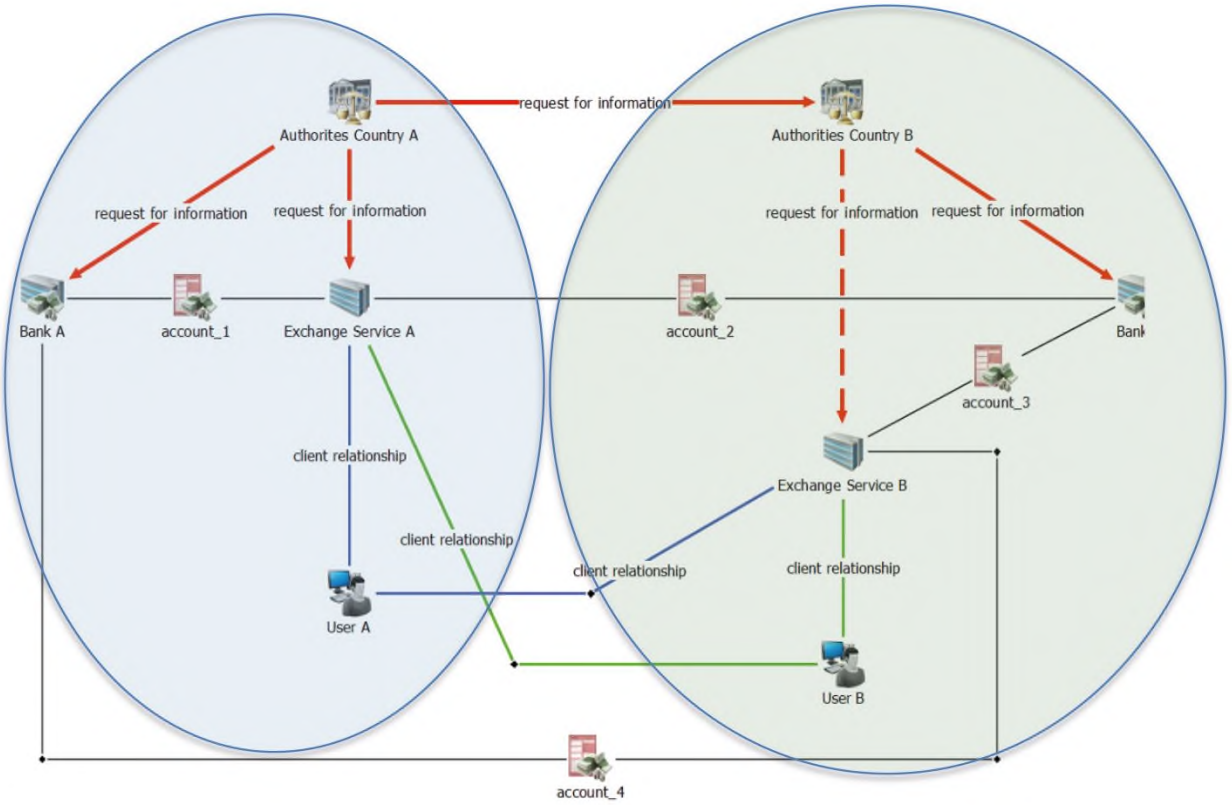
To meet the new requirements of blockchain transaction analysis and the expectations of market participants in their dealings with the competent authorities, the FIU made efforts already at an early stage to contact professional providers of blockchain analysis tools as well as providers of training in the field of blockchain analysis. By the end of January 2020, three FIU employees had received training as blockchain analysts, and two additional employees received training over the course of the year. This means that about half of all FIU employees are now qualified in blockchain analysis.

2. Overview of the interplay of market participants

First of all, the commencement of activities by VASPs domiciled in Liechtenstein requires that persons subject to due diligence and authorities alike familiarise themselves with the characteristics of the sector. The following diagram provides an overview of the actors involved – clients, VASPs, banks, authorities – and the relationships of these actors, some of which cross national borders. This illustrates what challenges the parties are confronted with if a business transaction does not proceed as envisaged by one or more of the participants.

To assess the functioning and responsibilities, it is absolutely necessary that the authority has an idea of the specific interrelationships in any fact pattern to be analysed. Key elements are:

- Countries of domicile of the banks and VASPs involved (relevance for application of the SPG with all consequences such as the obligation to submit reports of suspicion and to respond to requests for information from the FIU)



- Knowledge of the services offered such as brokerage, exchange, or the provision of fiat accounts
- Nationalities and countries of domicile of the clients

3. Reporting behaviour

Reports of suspicion from the VASP sector were submitted almost exclusively by VASP exchange service providers, namely 679 reports of suspicion in the reporting period, accounting for approximately 41 % of the total number of reports of suspicion. The suspicions generally related to the following categories:

- Unauthorised access to wallets (phishing/hacking attacks)
- Fraud schemes (incl. recalls at fiat correspondent banks)
- Identity theft (by exploiting vulnerabilities in remote onboarding processes)
- Exposure of transaction participants to darknet markets or other addresses with high-risk exposure (tumblers/mixers, unregulated or weakly regulated exchange service providers, etc.)
- Uncooperative client in the context of carrying out simple or special clarifications
- Possible exposure to persons, social media accounts, or addresses (address clusters) associated with financing of proliferation
- Possible exposure to persons, social media accounts, or addresses (address clusters) associated with financing of terrorism

Also in the VASP sector, there has been a clear tendency towards excessively long clarifications, which as a rule leads to reports of suspicion being submitted too late.

IV. Statistics

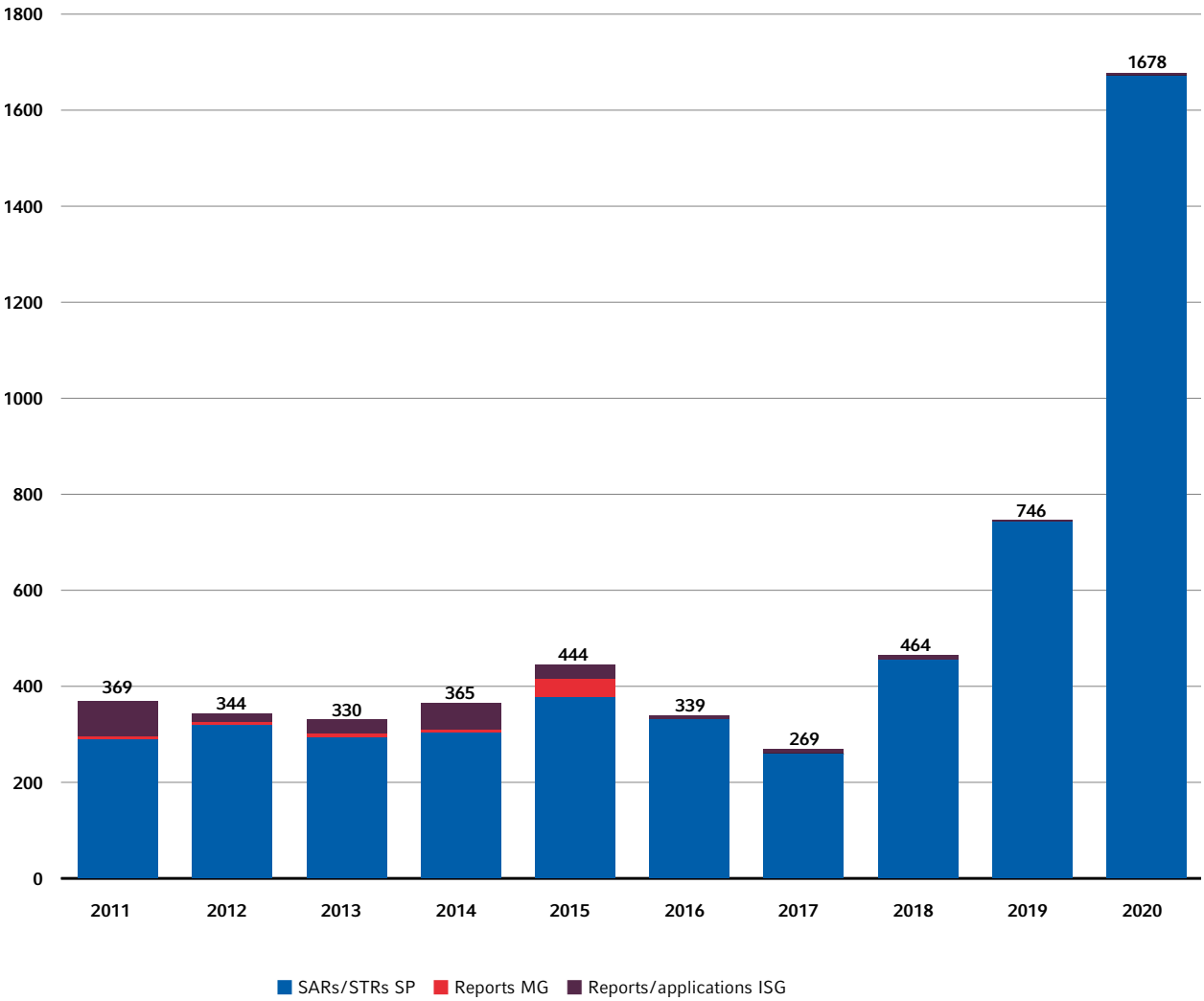
1. Overall view

As already mentioned at the outset, the overall view for the year 2020 is impressive and not alarming as such. Although this very high and sudden increase in the number of reports of suspicion in the year under review requires us to adjust our accustomed scale for the overall view, the increase was within the trend expected by the FIU.

The trend is in general comparable to that in other European countries. The experiences of partner authorities at bilateral meetings on IT infrastructure, electronic reporting portals, and managing the increasing workload also helped to determine the FIU's expectations. Various international partner authorities informed the FIU of their own experiences with a sudden increase in reports of suspicion. Looking back, the switch to an electronic reporting portal effective 1 January 2019 turned out to be the right choice, and even absolutely necessary and timely. The reports of suspicion currently received would no longer be manageable with existing resources if they were still submitted on paper.

The growth trend appears to be confirmed at about 30 % per year, focusing on "traditional" reports of suspicion. In addition, 679 reports of suspicion with a nexus to virtual currencies were submitted this year due to entry

All reports (SPG and MG) and reports/applications ISG



	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
SARs/STRs SPG	289	318	293	303	376	330	259	454	742	1671
Reports MG	6	7	9	7	38	0	0	0	0	0
Reports/applications ISG	74	19	28	55	30	9	10	10	4	7

into force of the TVTG and the resulting due diligence obligation of the VASPs. This accounts for 41 % of all the reports of suspicion submitted.

When the TVTG was passed by the Liechtenstein Parliament and even when the law entered into force on 1 January 2020, the FIU could not gauge how many reports of suspicion should be expected. Accordingly, three employees were trained to analyse blockchain transactions in advance, and two more received training over the course of the year.

Taking into account the established growth trend in traditional reports of suspicion, this is forcing the FIU to continue and possibly also to expand its prioritisation in the performance of analyses and to further develop its standardisation of electronically submitted reports of suspicion. This also includes considerations regarding the establishment of additional analysis capacities.

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 2016 to 2020 came from the following sectors:

Sector	2016	2017	2018	2019	2020
Banks	221	163	309	540	**844**
Virtual asset service providers					**640**
Professional trustees/ trust companies	56	48	82	132	**102**
Electronic money institutions			2	1	**29**
Insurance undertakings	18	26	31	22	**15**
Public authorities	14	12	7	13	**13**
Fund companies/AIFMs				2	**7**
FIU/non-reg. FI/unknown				4	**7**[2]
Life insurers			6	5	**4**
Casinos				9	**4**
Asset managers/ management companies	0	2	2	1	**2**
Auditors/audit firms	0	0	1	5	**2**
Investment firms			3	2	**1**
PSPs (payment service providers)	10	5	3	5	**1**
Precious metal dealers	0	0	0	0	**0**
Dealers in high-value goods/auctioneers	0	0	0	1	**0**
Investment undertakings	0	0	0	0	**0**
Lawyers	7	1	0	0	**0**
Insurance brokers			2	0	**0**
Finance companies	0	4	0	0	**0**
Total	326	259	448	742	**1671**

The number of reports of suspicion submitted from the individual sectors gives rise to the following findings:

- The increase was generally in line with expectations based on the figures of the past three years.
- By far the most reports of suspicion continue to be submitted by banks – about 51 % this year.
- The surprisingly high increase in electronic money institutions is due to the commencement of activities by market participants in the crypto-asset sector.
- The development of reports of suspicion from VASPs is difficult to interpret after only one year, but it can be assumed that this number will continue to increase in 2021 and that these market participants will soon replace banks as the sector submitting the most reports.
- The decrease in reports of suspicion from the fiduciary sector must be seen in relation to the development so far. In the view of the FIU, an isolated comparison with the figure for 2019 would lead to a false interpretation. It should be noted, however, that the FIU does believe that the number of reports of suspicion from the fiduciary sector is at a low level.

2 This category results from the fact that persons subject to due diligence not registered in the goAML system submitted reports of suspicion. They were then called upon to register.

- The decrease in reports of suspicion from the casino sector may be due to the impact of measures taken as a result of the Covid-19 pandemic. Nevertheless, the number of reports of suspicion from this sector appears surprisingly low. The reasons for this will have to be evaluated in 2021.
- The declining trend among life insurers must also be examined in 2021 together with the FMA and sector representatives.

2.2. Reasons for submission

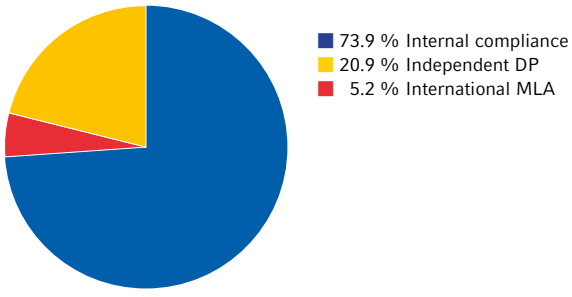
The reports of suspicion (SARs/STRs) are classified according to whether they:

- were submitted pursuant to an institution's own clarifications 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), orr
- originated in independent domestic investigative proceedings (DP).

The distribution of reasons for submission has been stable. The persons subject to due diligence continue to indicate which of these three reasons gave rise to the suspicion leading to the report. This distinction has proven its value and will be maintained.

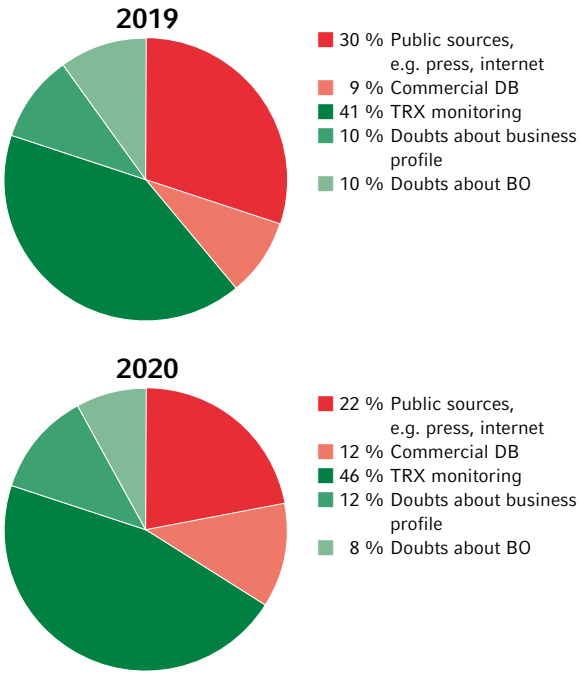
It should be noted that the information is based on the assessment of the persons subject to due diligence, which is then taken note of by the FIU. The following evaluation is used for a finer distinction within each category.

Reasons for submission



The motivation for these finer distinctions is that the FIU is interested in knowing which specific indicators are identified by persons subject to due diligence. This information is to be used in the further development of the non-exhaustive indicators listed in Annex 3 of the Due Diligence Ordinance and, above all, as a basis for further training and awareness-raising.

Distribution of internal compliance



In terms of content, a comparison with the previous year shows an increase in findings from transaction monitoring, which undoubtedly is also due to the fact that this is one of the most fundamental required competences of VASPs, together with the client onboarding process. The more intensive and evolving use of commercial databases also appears to be leading to a higher number of positive matches.

Here as well, the figures are based on information provided by persons subject to due diligence in each individual case. Often, several elements give rise to a suspicion; accordingly, multiple responses are possible.

A subcategory of "suspicion of a specific predicate offence" was deliberately omitted, however. As already explained in previous years as well as in the instruction on submission of reports of suspicion, it is not the responsibility of the persons subject to due diligence to focus on finding or determining a predicate offence. This is the responsibility of the FIU or of the downstream prosecution authorities, and such a focus would lead to overly narrow attention of the persons subject to due diligence.

Especially during this year under review, the FIU used training sessions as well as public and private talks to draw attention to the risk that may arise for persons subject to due diligence from other areas such as circumvention of sanctions or financing of proliferation and terrorism.

The wide range of existing, changing, and new sanctions poses special challenges for persons subject to due diligence. A focus on the search for a predicate offence in cases of circumvention of sanctions entails that crucial elements are not seen or are not given the proper weight due to the lack of indicators of a specific predicate offence of money laundering. However, the nature of sanctions means that the persons and entities affected by them will make up a story about the content of a business relationship, the source of wealth/funds, or the justification of money flows in order to avoid the sanctions. Invented stories generally have the disadvantage that they may be recognised as implausible overall when aspects of transaction monitoring, verification of the business profile, authenticity of the beneficial owners, and verification of public sources are considered as a whole.

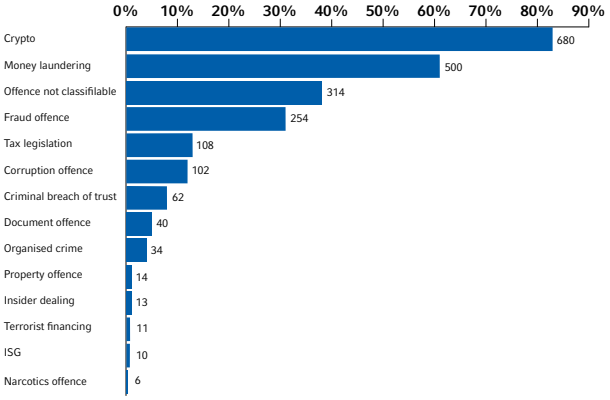
2.3. Statistics according to offence

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



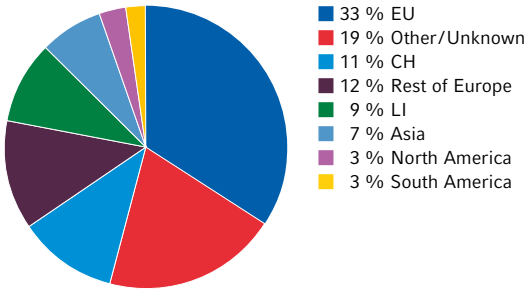
The development in 2020 clearly shows two elements. First, it is evident that the impact of cryptocurrencies on the activities of the FIU and other authorities such as the Financial Market Authority, the Office of the Public Prosecutor, the Court of Justice, and the National Police has become a reality as expected. Second, it is apparent that non-specific predicate offences – "money laundering" or "offence not classifiable" – are being mentioned more frequently. Our cautious assumption is that the criticism repeatedly expressed by the FIU is now leading persons subject to due diligence to believe that they can recognise suspicious situations at an earlier stage. Overall, this growing awareness of the existing risk situation enhances the defence mechanism of the financial centre in the following respects:

- Increasing the intensity of the internal discourse on risk appetite among persons subject to due diligence
- Broadening the FIU's field of view by replacing the strict focus on a specific predicate offence
- Improving the bases for strategic analysis

2.3.2. Nationality/domicile of contracting party

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

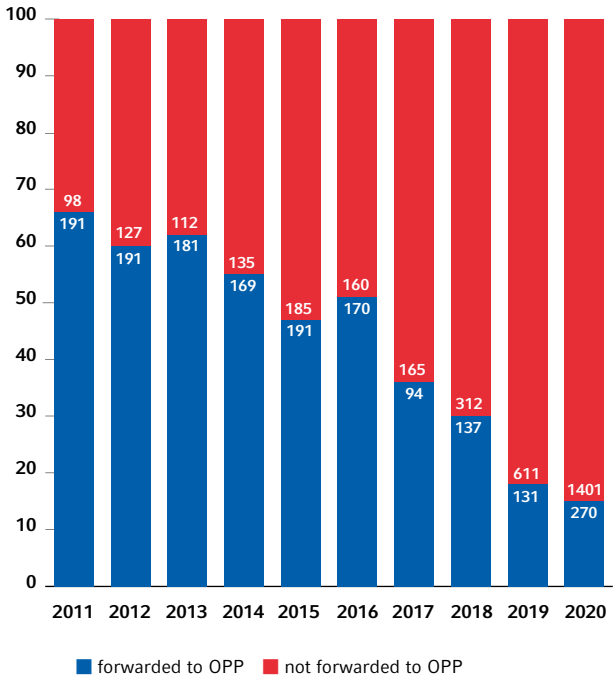
Nationality of involved persons by region



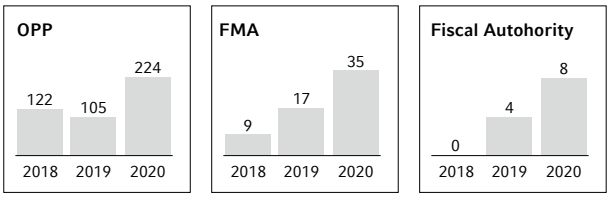
2.4. Analysis reports forwarded to the Office of the Public Prosecutor

The statistics on reports forwarded (until 2016) and analysis reports, if continued as in previous years, would be as follows:

Reports forwarded / Analysis reports

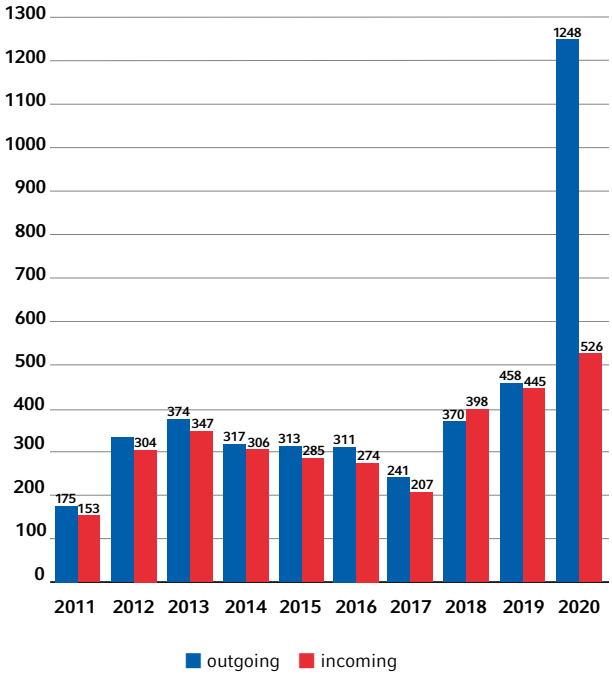


But this presentation distorts the real picture, as already explained under II. Activities of the FIU. This format does not indicate how many SARs/STRs or parts thereof ultimately ended up in the reports sent to the prosecution or supervisory authorities. An FIU report consists in an analysis of the information available to it and is not limited to mere forwarding of the reports of suspicion. There has accordingly been a growing recognition of the unsuitability of the ratios reported in these statistics. Consequently, we switched to the following presentation as of the beginning of this year:



2.5. International cooperation

FIU information exchange



The statistics for information exchange with international partner authorities are stable and in line with the recorded increase in reports of suspicion.

The increase in the volume of outgoing information to foreign partner authorities is due to the reports of suspicion from VASPs. Reports of suspicion especially from this sector are very often based on fact patterns which – apart from the domicile of the domestic VASP – have no nexus to Liechtenstein. Rather, it can often even be assumed that clients do not know or do not care that a VASP is domiciled in Liechtenstein.

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*
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*
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)*
STR	*Suspicious transaction report (report of suspicion involving at least one transaction)*
TRX	*Transaction*