FIAU

Intelligence Factsheet:

Strategic Analysis on Intelligence having an International Element

Issued: 30 September 2020

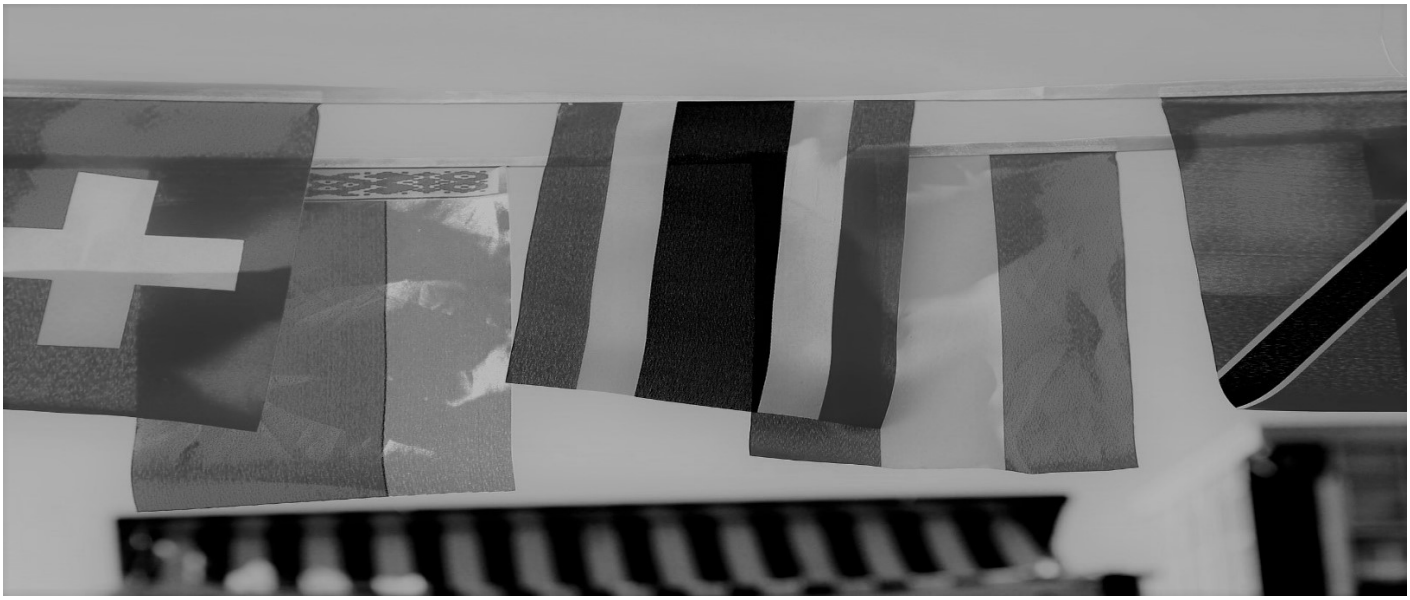
INTELLIGENCE FACTSHEET: STRATEGIC ANALYSIS ON INTELLIGENCE HAVING AN INTERNATIONAL ELEMENT

The following document provides information extracted from the results of a strategic analysis carried out by the FIAU. The next paragraphs aim to provide subject persons with money laundering and terrorism financing ("ML/FT") indicators based on STRs presenting an international element. By "presenting an international element", the STR would include any link to a foreign jurisdiction, including the country of the alleged predicate offence, or the nationality or country of registration of subjects being reported, as well as the use of foreign banking services and others.

The two main reporting sectors for the STRs reviewed for this exercise were credit institutions and remote gaming operators ("RGO"s) and thus, the observations made in the following lines should be considered within this context.

STRs received by year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	Total
No. of STRs received	4	21	41	27	38	50	98	88	150	192	709
Percentage of increase compared to previous year		425%	95%	-34%	40%	31%	96%	-10%	71%	28%	

For the purpose of this report, suspicious activity reports and suspicious transactions reported were not differentiated and would be referred to as "STRs".



SUSPECTED PREDICATE OFFENCE

The review of the specific sample of STRs which included predicate offences conducted abroad represented 75.26% of the total sample for the exercise, which ranged from May 2010 until September 2019. The most common predicate offence observed was fraud, mentioned in 52.84% of the specific sample. Tax crimes (12.9%), as well as corruption and bribery (9.52%) followed as most commonly mentioned predicate offences.

The alleged predicate offences are not always identifiable by the subject person, and/or these might not be accurate at times, since the classification is made on the basis of limited information.

Fraud – As previously mentioned, fraud was highlighted as the main predicate offence. The main entities that reported fraud as an alleged predicate offence were remote gaming companies (54.94%), followed by credit institutions (22.97%). A similar analysis that looked at the products being used revealed these were mainly remote gaming accounts (51.81%), followed by personal bank accounts.

Tax Crime – The second most prevalent predicate offence was "Tax Crimes" – reported in 12.9% of all STRs analyzed. From those analyzed STRs, credit institutions were the main reporters (35.7%) followed by investment services licensees (15.5%) and remote gaming companies (14.3%). The most common product that was used when laundering funds allegedly derived from tax crimes was bank accounts (both personal and corporate).

The most common red flags in the STRs that mentioned tax crimes were: transactional activity which was unexplained or inconsistent with the customers known profile and customers who were uncooperative when requested to provide supporting documentation.

Corruption and bribery – Credit institutions were responsible for 39.2% of all STRs that included corruption or bribery, followed by investment services licensees (16.2%). The reason for most STRs being submitted in relation to corruption and bribery was adverse media and the most commonly used products in this case were the bank accounts (natural and legal persons).

Other – Other alleged predicate offences with links to foreign jurisdictions make up a total of 24.74% of the sample.

DISSEMINATED REPORTS

In the majority of cases, when the link to Malta is remote or solely based on a particular use of service or product, the FIAU disseminates the information to its foreign counterparts, through a spontaneous intelligence report.

In addition, those STRs from the sample which resulted in an analytical report being forwarded to the Malta Police for further investigation consisted of 20.23% of all finalised STRs having a foreign criminal element. Moreover, other cases in which a spontaneous dissemination was sent to other national authorities and/or Malta Police were only 0.97% of all finalised STRs.

In other instances, some reports would have insufficient elements to establish a link to potential money laundering or terrorist financing activities; and thus such reports result in being closed with no further dissemination, and stored in the FIAU's database and should further intelligence be obtained which could change the outcome of the previous report, the appropriate action would be then taken by the FIAU.

REASON FOR SUSPICION

The most common reasons for suspicion, for all STRs that were looked at for the study were (in their order of frequency of appearance):

- Customer became uncooperative when requested to provide required details and/or documentation on a transaction or operation;
- Large volume deposits which are not in line with the customers' known profile;
- Unusual or suspicious identification documents or lack of documents;
- Company and/or transactional structure is unnecessarily complex;
- Subject persons linked to subject of STR are adversely known to open sources; or
- Transfers to, or from, high-risk jurisdictions, without apparent economic business reason/sense.

CASE STUDIES

Case 1 - Large deposits inconsistent with business & risk profile, limited source of wealth/income information

The FIAU received an STR to report that a local company, holding a local bank account, received several payments totalling €102,400 from various natural and legal persons. Initial analysis revealed that payments were received from over 20 jurisdictions.

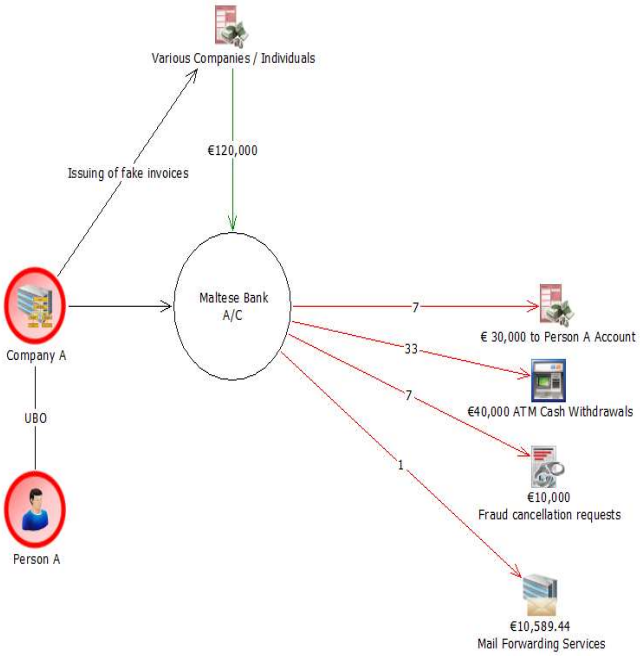
Furthermore, the subject person also informed the FIAU that it had received eight fraud cancellation requests. Upon questioning, the company representatives would provide invoices that, upon investigation, were nearly identical to sample invoices that are issued on the European Union Intellectual Property Office (EUIPO) as a warning and example of fake invoices issued by companies.

As soon as the funds were received in the local bank account, similar amounts would be withdrawn in cash from banks situated in another country through transfers to a personal account held with a foreign bank in the name of the ultimate beneficial owner of the aforementioned company.

Following a number of requests for information, the FIAU discovered that a number of companies that sent money to the locally registered company were known to be potential victims of fraud.

Red Flags:

- Large volume of deposits not in line with customers' known profile
- Several fraud cancellation requests received by the bank
- Majority of withdrawals are conducted using ATMs, which activity was not in line with customer's known profile.



Case 2 – Complex transactional structure

The FIAU had received an STR indicating that an individual, who held bank accounts with a local credit institution, received a number of transfers that were being described as loan payments. Once received the funds were transferred to other credit institutions, including various foreign bank accounts. A number of foreign bank accounts were owned by the same individual whereas the rest were owned by different companies.

During the course of the analysis, the FIAU identified that the beneficiaries of the funds (the companies) were adversely known and of interest to foreign FIUs, and were also adversely known to several open source media. Further analysis revealed that the individual had other associates who were also subject to criminal proceedings in relation to organised crime, embezzlement and tax evasion charges abroad.

During the course of business, the individual was asked by the local credit institution to provide information about the nature of business and information about the companies he transacted with. The individual was unwilling to provide the requested information. During the same period, the individual received dividends from one of the same companies he had previously transacted with. The FIAU was informed by its foreign counterparts that the individual was the UBO of said company.

Red Flags:

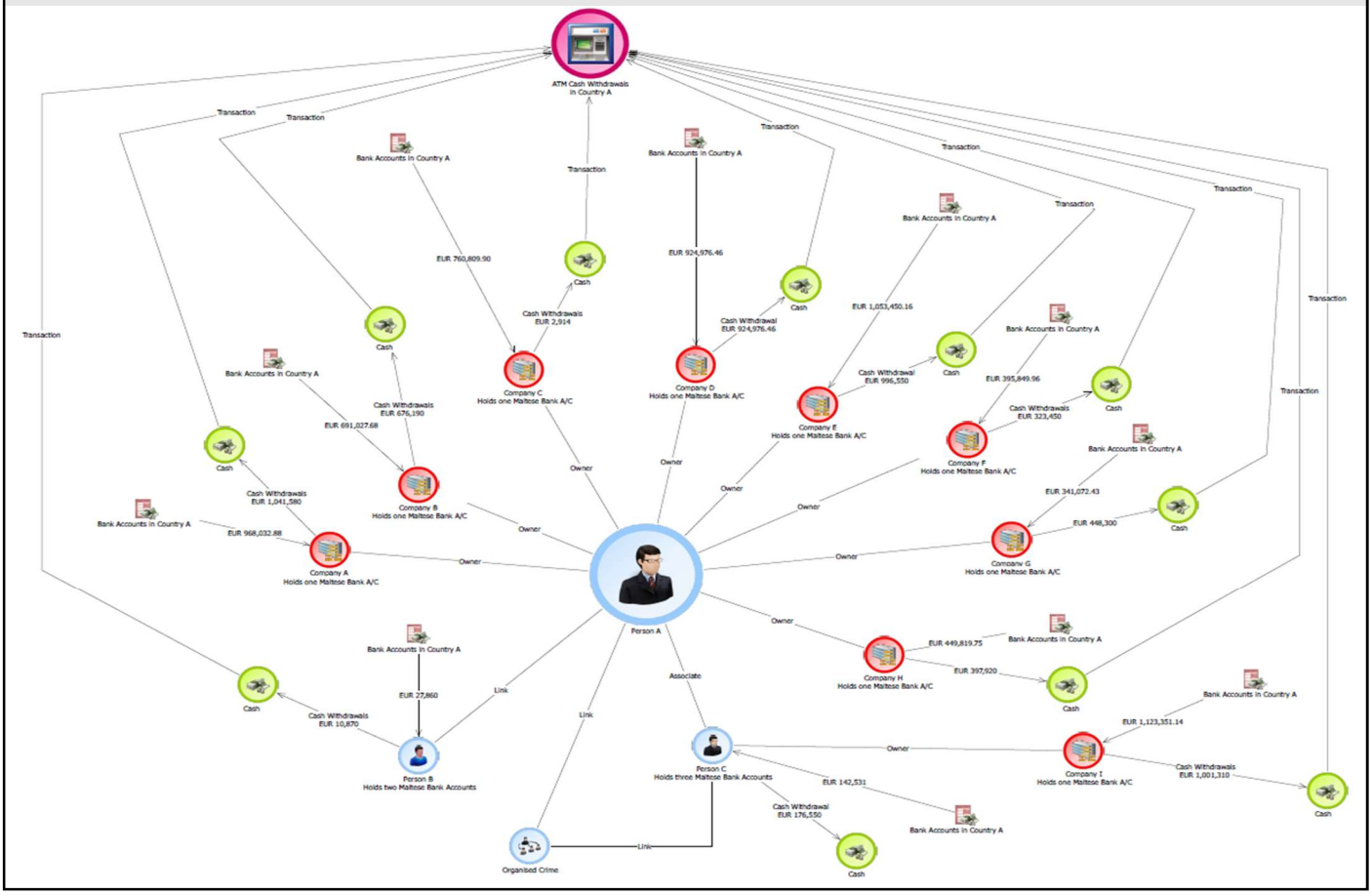
- Complex company and transactional structure which does not make economic sense.
- Subjects or persons linked to subjects of STR are adversely known to open source.

Case 3 – ATM Withdrawals and uncooperative individual

The FIAU has identified a typology whereby three foreign individuals were transferring funds from foreign bank accounts to their own local bank accounts. The foreign bank accounts were held in the names of foreign companies, owned by the same individuals. Further analysis by the FIAU revealed that the individuals had strong ties to organised crime groups abroad and had also been investigated by law enforcement agencies in the same foreign country. It was also noted that in some instances five debit cards were issued for each local bank account. The activity was considered highly suspicious, as the limit of cash withdrawals was linked to the number of cards made available by the bank. This arrangement allowed the card owner to withdraw substantial amounts of cash that would typically not be possible with only one bank card. Furthermore, the ATM withdrawals were made on the same day or the following day that the cash was received. A total of €7,000,000 were withdrawn in two years and were all conducted from the same ATM in the foreign country.

Red flags:

- Large amounts withdrawn from ATMs, activity not in line with the customer's known profile
- High turnover with a low balance – indicative of possible conduit account activity.



65C, Tower Street,
Birkirkara BKR 4012,
Malta

Questions on this document or on the application of AML/CFT measures may be sent to **queries@fiaumalta.org**

Financial Intelligence Analysis Unit
65C, Tower Street,
Birkirkara BKR 4012,
Malta

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org