

**Intelligence Factsheet:**

# **Cash Usage, Tax Crimes, Corruption and Bribery**





# INTELLIGENCE FACTSHEET: CASH USAGE, TAX CRIMES, CORRUPTION AND BRIBERY

Following a strategic analysis carried out by the FIAU on the intelligence received, the following points were extracted and are publically shared in order to help subject persons better identify and assess risk, as well as adequately calibrating measures and controls in place, if necessary.

In this regard, the document can be of interest to all subject persons, particularly in the course of carrying out and/or updating the Business Risk Assessments and Customers Risk Assessments, as required under Chapter 3 of the FIAU Implementing Procedures Part I.

Trends in reporting and red flags identified below are not exhaustive and subject persons should keep themselves up-to-date with emerging trends and developments in typologies published by the FIAU, as well as other international expert bodies.

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



## 1. USE OF CASH TRANSACTION IN MALTA - KEY FIGURES AND CASE STUDY

### METHODS AND ALLEGED PREDICATE OFFENCES

**When ATM cash deposits** were reported in STRs, “tax crimes” was the predominant alleged predicate offence, in approximately 55% of the instances. This would be viewed as undeclared income: individuals receiving income in cash and deposit such funds using ATMs to possibly avoid contact with the bank representatives.

Trafficking in human beings and migrant smuggling (10%), and illicit traffic in narcotics (6%) were the two other most reported alleged predicate offences.

**When ATM cash withdrawals** were conducted, the most predominant alleged predicate offence reported by the subject person was terrorism and/or terrorist financing activities (29% of instances); followed by fraud and tax crimes, each registering in approx. 19% of the cases reviewed.

Tax crimes was the most chosen alleged predicate offences in relation to over-the-counter (“OTC”) **cash deposits and withdrawal**, followed by fraud, illicit traffic in narcotics and participation in organized criminal group for OTC deposit, as well as terrorism and terrorism financing and corruption and bribery for OTC withdrawals.

### Case Study

A self-employed individual has effected numerous cash deposits in his bank accounts in Malta to cover a number of loan repayments, totalling over € 200,000 in 3 years’ time.

These deposits were compared to the income tax returns of the same individual, which had been collected by the bank, and his transactions were inconsistent with his customer profile. It was later confirmed the individual was declaring far less income than he was actually generating through his business, thereby substantially evading the payment of tax.

## 2. TAX CRIMES: KEY FIGURES AND RED FLAGS

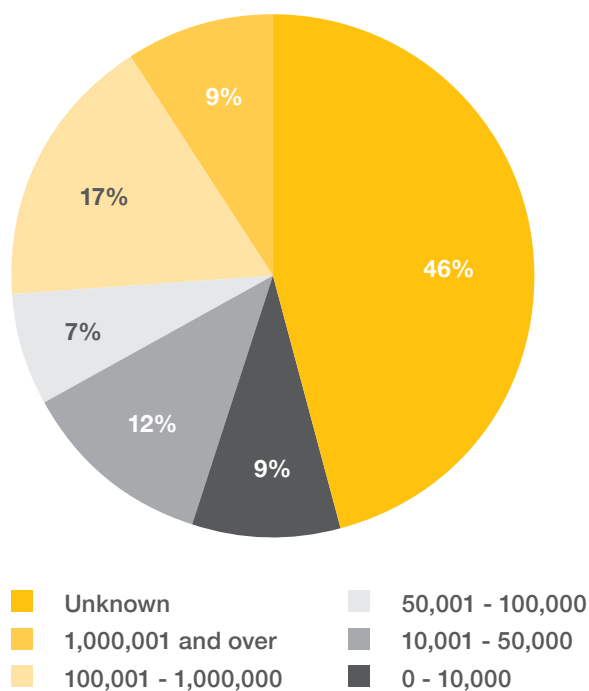
### ALLEGED PREDICATE OFFENCES

In STR submissions with the FIAU throughout the years 2015 until 2019, fraud (34%) and tax crimes (25%) were the most reported alleged predicate offences, followed by other predicate offences (41%).

**Reporting Entities:** When compared to the total STRs submitted by each sub-sector, tax-related offences were mostly flagged in STRs submitted by investment licensees (50% of sample reviewed), Credit institutions (30%), insurance licensees (29%), PSPs (21%), as well as accountants and auditors (approx. 20%).

**Suspected amount generated from tax-related offences:** Although in 45.95% of the STRs in which tax crimes were identified as alleged predicate offences, the amount was unknown, in 17.13% of reports, the suspected amounts were identified to be in the range of EUR 100,001 to EUR 1,000,000.

### Suspected amount generated from tax-related offences (range)



In tax-related STRs reviewed, **the involvement of natural persons** was observed in 74% of instances and 26% of these involved legal persons; **In 71% of cases, local entities or natural persons was documented**, whilst in 31% of these, international origin was noted.

**Modus Operandi:** Use of banking activities to facilitate suspected tax crimes and money laundering activities made up approximately 78% of all STRs which were linked to possible tax-related proceeds in the period starting from 1<sup>st</sup> January 2015 until 31<sup>st</sup> December 2019:

- use of personal (46%) and corporate bank accounts (18%);
- both locally (56%) and abroad (15%), and
- the use of wire transfers to receive and send funds (12%).

From reviews of international requests for information received from other financial intelligence units from around the globe, it was concluded that the most prevalent use identified to allegedly launder proceeds of tax crimes were accounts with Maltese credit and financial institutions.

### Red Flags

- Transactional activity identified by the reporting entity was unexplained or inconsistent with known customer profile, such as high amount of cash deposits which are not in line with the individual's known employment;
- Instances when a particular customer of a financial institution did not comply or was reluctant to cooperate with certain requests to provide certain details and/or documentation on a transaction or particular operation;
- Occurrences when the company and or transaction structure was unnecessarily complex and thus raising suspicion; and
- Transfers being conducted to, or from, high-risk jurisdictions without apparent economic business rationale.

### 3. CORRUPTION AND BRIBERY: TRENDS AND TYPOLOGIES

**Reports:** For the period starting from 1<sup>st</sup> January 2015 until 31<sup>st</sup> December 2019, roughly 177 STRs making up to 3% of all STRs submitted by subject persons, referred to suspicion of money laundering as a result of illicit money derived from corruption and bribery offences.

In addition, the FIAU identified another 38 STRs which had links to illicit funds derived from alleged corruption and bribery related offences.

**Main reporting entities:** 85% of STRs submitted by SPs in related to suspicion of bribery and corruption were filed by credit institutions (52%), remote gaming companies (13%), investment services licensees (11%) and company service providers (9%).

**Amounts involved:** approximately 50% the cases reviewed reported the amount of suspected illicit funds as unknown. However, when the amount was known it was noted that:

- 20% of these were in the range of EUR 0-100,000.
- 16% were classified to have a suspected amount of illicit funds ranging from EUR 100,001 to 1,000,000 and
- 14% in the range from EUR 1,000,001 and over;

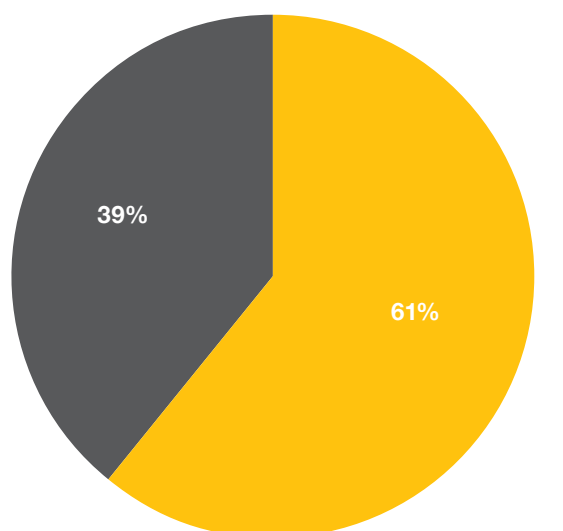
**Involvements:** 61.04% of all the reported involvements were natural persons, out of which 47.39% of these individuals were locals and 52.61% foreign.

**Red Flags most commonly reported:**

- Subjects or persons having a direct or indirect business relationship with the subject person were adversely known to open source information; and
- Transactional activity was considered inconsistent with the known customer profile or such activity had no plausible rationale.

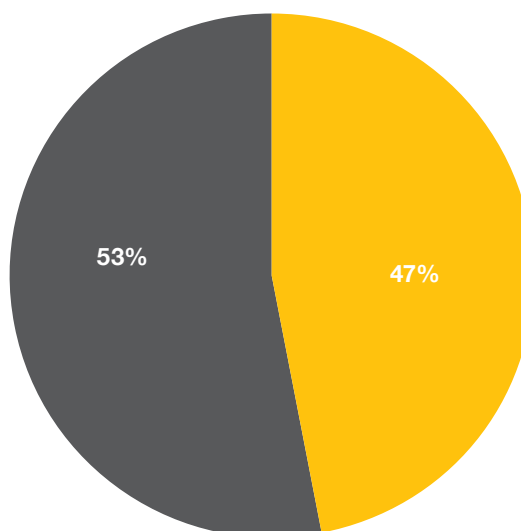
Most prevalent **modus operandi** in these cases were once again the use of banking services, mostly corporate bank accounts in Malta and abroad. This was followed by the use of several foreign and local companies in order to potentially launder illicit funds generated from these offences.

**Type of persons involved in STRs related to corruption and bribery**



■ Natural Persons    ■ Legal Persons

**Type of persons involved in STRs related to corruption and bribery**



■ Local    ■ Foreign

© Financial Intelligence Analysis Unit, 2020

65C, Tower Street,  
Birkirkara BKR 4012,  
Malta

Reproduction is permitted provided the source is acknowledged.

Questions on this document or on the application of AML/CFT  
measures may be sent to **[queries@fiaumalta.org](mailto: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](mailto:info@fiaumalta.org)  
**Website:** [www.fiaumalta.org](http://www.fiaumalta.org)