FIAU

Intelligence Factsheet:

Key figures and observations based on the 2019 STRs received from Remote Gaming Operators

Issued: 28 September 2020

INTELLIGENCE FACTSHEET: KEY FIGURES AND OBSERVATIONS BASED ON 2019 STRS RECEIVED FROM REMOTE GAMING OPERATORS

From a strategic analysis exercise carried out in 2020, the FIAU is making the following points publically available in order to provide the subject persons with an overview of the key points observed in the reports received from the remote gaming sector in 2019.

Not considering the new licensees, in 2019, the total number of subject persons registered as remote gaming operators ("RGOs") with the FIAU Caspar system was 210. From this sector, a total of 1,445 submissions were received, a significant increase compared to the previous years as captured in the table below.

STRs received by year	2014	2015	2016	2017	2018	2019	May 2020	Total
No. of STRs received from RGO	22	32	87	218	700	1,445	741	3,245
Percentage of increase compared to previous year		45%	172%	151%	221%	106%		

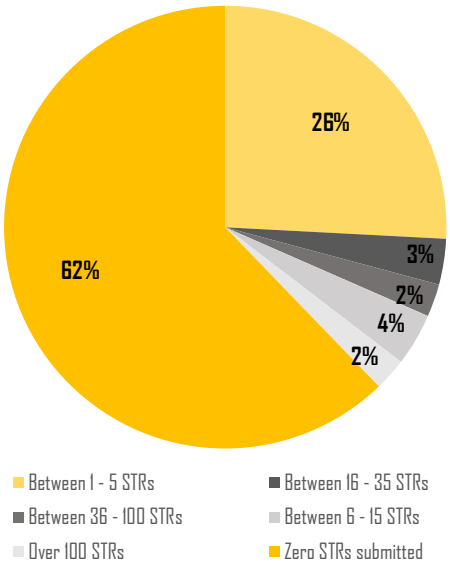
For the purpose of this report, suspicious activity reports and suspicious transactions reported were not differentiated and would be referred to as "STRs".

2019 SUBMISSIONS MADE BY RGOS

From the 1,445 STRs received by the FIAU from this sector in 2019, 32% of these (457 STRs) were submitted by 3 companies and 35% by another 5 companies (498).
Whilst the remaining 33% of STRs (roughly 486) were submitted by 72 entities, 29 RGOs filed 1 report in 2019 with the FIAU.

Thus, the analysis carried out and the results presented in the following paragraphs would reflect accordingly the circumstances and the population of reports reviewed, as per top reporters' submissions.

Distribution of remote gaming entities by number of STRs submitted in 2019



REASONS FOR SUSPICION

The top reasons for suspicion, which led to the particular client, situation or transaction to be investigated and reported to the FIAU, refer to: transactions (46% of the cases), behaviour (21%), identification and verification process and documentation (16%); in addition, adverse media (3%) and high-risk jurisdictions involvements (2%) were also flagged.

Transactions - The main reasons in these instances were inconsistencies noted between the transactions carried out and the customer profile:

- transaction activity which is unexplained or is inconsistent with the known customer profile;
- large volume of deposits which are not in line with customer's known profile;
- complex transactions;
- suspicious narratives or mismatch between the name of the beneficiary and the name of the bank account to be credited'
- Chargebacks.

Other general situations relate to large amounts being deposited, withdrawn and/or significant losses registered in a short period of

When the money laundering/financing of terrorism suspicion is linked to a transaction still to be processed, subject persons must refrain from carrying out the same and must submit an STR. The execution of the transaction must be delayed for one (1) working day following the day on which the licensee files the STR.

Kindly refer to Section 5.8 of the Implementing Procedures Part I for guidance.

time, but with no or limited source of wealth or source of funds information obtained.

Funding Methods – Several STRs referred to the deposits made to fund the betting activity, as these were suspected to be the proceeds of crime, or were stolen from someone else's bank account or were possibly the results of fraudulent activity.
In other instances, wagering only once on a skilled game and then withdrawing a similar sum of the initial deposit made, after every each and single deposit, was another method noted.

Behavioural indicators - In 17% of the instances recorded, the customer became uncooperative when requested to provide required details and/or documentation and in other cases (4%), the customer inexplicable stopped contact.

Identification and verification - Regarding identification and verification, in 15% of the instances in relation to the 2019 STRs submitted by the RGOs, issues were reported in obtaining documentation from customers: the identification documents were unusual or suspicious or were lacking altogether.

Customer profile - For 3% of the STRs, the subjects or persons linked to subjects of STR were adversely known on open sources. Furthermore, there were quite a number of cases in which the source of wealth and source of funds remained unknown, as the customer refused to provide such information, despite the large deposits or the significant losses over short periods of time

High-risk jurisdiction: in approximately 2.17% of the cases, the STRs related to transfers to, or from, high-risk jurisdictions, without apparent sense in doing so.

Chip dumping: The reason for suspicion referred specifically to Intentional loss or movement of funds was documented in 1.52% of the cases.

Cybercrime was reported approximately 1% of the cases, both in instances in which the customer account having been hacked and compromised by a fraudulent third party, as well as hacking the online casino games to generate additional free spins in order to increase winnings.

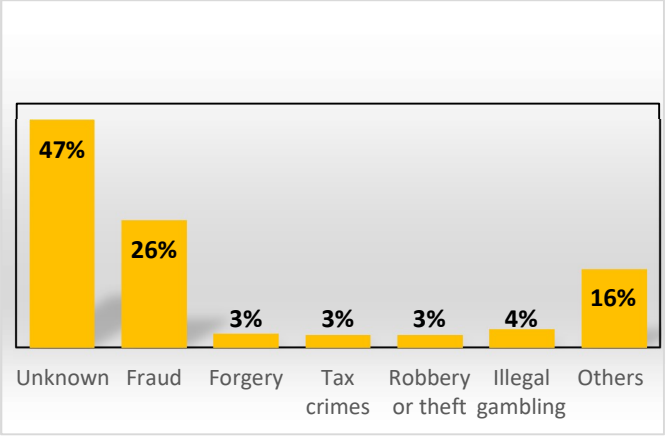
Games: In a number of cases, casino games, sport betting, as well as fixed odds games, mainly blackjack and roulette, were mentioned.

Smurfing, collusion were observed, as well as cases in which the player was using multiple credit cards and then requesting withdrawals for successful deposits to prepaid cards, after minimal gameplay.

PREDICATE OFFENCES, AGGREGATED AMOUNT AND MODUS OPERANDI

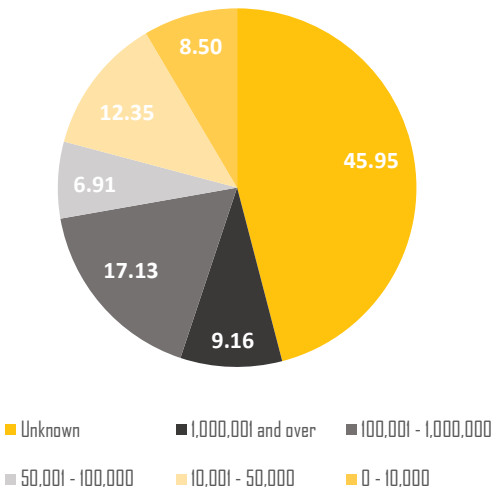
For most of the STRs received from remote gaming operators in 2019, the predicate offence is not identified, being marked as "unknown" or "other".

Suspected predicate offence



Suspected amounts in relation to reports made: Although in In terms of the amounts declared for the majority of the STRs, these are below €10,000 in 32% of the instances, followed by the amounts ranging from €100k to € 1 million in 22% of the cases. However, significant amounts over € 1 million were reported for 36 STRs.

Suspected amount range



Modus operandi and funding methods: Apart from remote gaming operators and accounts used in majority of the cases reported to the FIAU, the use of e-wallets, bank accounts held in the name of natural persons held abroad, credit and debit cards

mainly issued outside Malta, as well as prepaid cards were flagged to have been part of the methods used.

CASE STUDIES

Several cases and typologies noted are presented below.

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

A young EU citizen, with a declared annual income of approx. € 30K deposited approximately € 250k in 2019, amounts ranging from € 10 to € 36K, mentioning he was also a successful poker player. However, the customer's gameplay consisted mainly of sportsbook products.

The customer's source of funds / wealth could not be established and the known income of the customer was inconsistent with the level of funds going through the account.

Case 2 – Multiple prepaid cards, withdrawals following minimum gameplay

For example, a national of another member state would periodically made deposits of considerable amounts during a single session by means of multiple prepaid cards. Then he would engage in very little gameplay and then withdraw the amounts in an account with a PSP.
The customer also made frequent deposits and withdrawals within 1-2 minutes of such deposits, without any reasonable explanation.
In terms of games chosen, the customer's gameplay indicates he was mainly playing slots games and wagering small amounts on these games. Occasionally, he would play Roulette and Blackjack where he will wager large stakes.

Case 3 – Law enforcement enquiries and adverse media

An RGO carried out a review of one of his customer's activities, which was triggered by a law enforcement enquiry. Initial online searches seemed to indicate that the customer was involved in an online fraud.
Further analysis showed the use of multiple accounts by the customer, by slightly altering his first or last name and using different, but very similar e-mails.
The client deposited mostly from prepaid cards, remote gaming partners, as well as own account.
He played using significantly low odds, short combination lengths, and placed bets on non-European soccer games.
The deposits, rather than being withdrawn, were being lost on such bets.

Case 4 - Large deposits inconsistent with business & risk profile, limited source of wealth/income information

A particular typology was noted in relation to individuals coming from a specific geographical area, linked by nationality and by their residential address being flagged due to suspicious activity by the respective remote gaming companies.
In some instances a number of remote gaming accounts were linked with several other accounts due to having the same device ID being used.
The individuals also failed to comply with the necessary CDD procedures.

The numerous individuals were noted to mostly make use of e-wallet service providers, depositing high amounts of funds, as well as receiving payments from third parties, and having substantial losses in their betting activity.

The sports betting activity and the financial analysis revealed that the majority of their remote gaming accounts incurred high losses and had similar modus operandi in the way they were used especially vis-à-vis the use of betting exchanges.
The reported individuals which made use of this betting exchange, were flagged due to having placed numerous unmatched bets with a high loss probability.
These odds are then matched by an alleged colluding player which has a high probability of success.

In most of the cases, the FIAU considers it more appropriate to send a spontaneous intelligence report to foreign FIUs rather than to trigger an investigation in Malta on the basis of STRs received from the remote gaming entities. This is due to the strong international element that is evident in most of these cases, with the only link to Malta being the remote gaming account with the Maltese-licensed entity.

Although the FIAU does not open its own in-depth analysis in these cases, the majority result in further dissemination to its foreign counterparts. As a result, information received through these submissions accounted for 35% of the total spontaneous intelligence reports shared with foreign FIUs in 2019.

From the 1,445 STRs received in 2019, 1,096 of these have been the subject of a spontaneous intelligence reports sent to foreign FIUs in 2019, as well as the first half of 2020.

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