
# GUIDANCE NOTE

## ON

# SUBMITTING SUSPICIOUS TRANSACTION REPORTS BY REMOTE GAMING LICENSEES

*A GUIDANCE NOTE ISSUED BY THE FIAU ON THE INFORMATION WHICH SHOULD BE INCLUDED IN THE SUBMISSION OF SUSPICIOUS TRANSACTION REPORTS BY REMOTE GAMING LICENSEES*

**Issued:** **4 April 2019**

Background Information

A key obligation of anyone considered as a subject person in terms of the Prevention of Money Laundering and Funding of Terrorism Regulations is the submission of Suspicion Transaction Reports (STRs) to the Financial Intelligence Analysis Unit (FIAU) whenever the subject person's Money Laundering Reporting Officer determines that there is knowledge or suspicion that funds are the proceeds of criminal activity or are related to funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism.

STRs are the main source from which the FIAU obtains information to carry out its analytical function and it is therefore of the utmost importance that the information received be of good quality. Moreover, given the ease with which funds (or any other asset) may be transferred, it is important that information is made available to the FIAU within the shortest time possible.

To this end, the FIAU is issuing this Guidance Note to assist remote gaming licensees in identifying the information and documentation that should be provided to the FIAU when submitting a STR. This in an effort to improve the quality of STRs, decrease the need for follow up communications between the FIAU and gaming licensees, and overall improve the efficacy of the analytical process.

**It is to be noted that this is a generic guidance note and, should a subject person have information and/or documentation which is not included in the following list but which it considers to be of relevance to the transaction and/or activity being reported, such information and/or documentation should still be submitted with the STR.**

<u>Section E – Product Information</u>

- Status of account (whether it is active, suspended/blocked, closed) including the balance held in the gaming account as at date of submission of the STR. Where no specific field is available on the STR Form to provide this information, the remote gaming licensee should include it in the general field 'Additional Comments'.

<u>Section G – Suspicious Transaction /Activity</u>

- Value and volume of withdrawals and deposits effected on a yearly basis over at least the five years immediately preceding the submission of the STR[1];
- In their explanations describing the suspicious activity, gaming licensees should, to the greatest extent possible, identify:
    - Unusual and/or significant increases in the value and/or frequency of deposits during a particular timeframe;
    - Gaming activity which is not commensurate with the volume and/or value of deposits;
    - Whether their client effected an unusually large number of deposits using prepaid cards in a relatively short period of time; and
    - Cases in which an unusual time lag had passed between gaming activity and the preceding deposit/s.
- Payment methods used to effect withdrawals and deposits;

[1] If the remote gaming licensee is able to provide data for a longer period of time then it should not limit itself to data for the preceding five years but should submit all the data on withdrawals and deposits available to it.

- Details relating to credit card numbers and/or any other bank account details used, such as the IBAN used for withdrawals and deposits. In the case of a payment service provider (PSP) the account identifier with the PSP should also be provided;
- An excel sheet showing all the deposit/withdrawal transactions (including date, time, amount, deposit and withdrawal method). Any attempted/unsuccessful deposits should, where possible, also be included;
- The IP addresses used to log on to the gaming account;
- The email address and phone number used to register for the gaming account and/or used for communication purposes;
- The statement and attitude of the player during for example a responsible gaming communication and/or following the suspension of a gaming account;
- Copy of due diligence documents (including identification document and proof of address when available);
- Remote gaming licensees should state whether checks were carried out using third party intelligence databases, social media and/or open sources. Any information obtained through such searches should also be provided to the FIAU;
- Any details as to the sources through which adverse information was obtained, including, where available, the URL to any adverse information found online and/or other information on the subject such as the involvement in companies;
- Remote gaming licensees should state whether checks were carried out to identify linked accounts through for example device detection. The account username chosen by the player and identifying similar usernames may also be an important factor;
- Details relating to any third party deposits; and
- A brief explanation on the gameplay, type of wagering and type of games.

It is also of utmost importance to include the contact details of the person submitting the STR in order to facilitate any further communication from the FIAU. The STR form has dedicated fields for the name of the MLRO (reporting person), contact email and contact phone/mobile number. The details provided in these fields should allow the FIAU to easily reach the said person.

Any questions or clarifications in relation to the contents of this Guidance Note may be addressed to the FIAU.

Email: info@fiumalta.org
Tel: +356 21 231 333