Republic of Estonia
Financial Intelligence Unit

Typology Report 10TT202607. Deposits and Withdrawals to Gambling Operators.

Keywords: *gambling, gambling services, casino, online casino, virtual assets, cash, payment card, bank account, risk-based approach*

It is important for obliged entities to assess and understand the potential risks associated with their activities, recognize when such risks may arise, and implement appropriate measures to mitigate them. The purpose of this typology report is to describe a typology commonly encountered in the gambling sector, based on suspicious activity reports received by the Financial Intelligence Unit (FIU), in order to assist market participants in identifying potentially risky situations.

The Financial Intelligence Unit (FIU) requests that transactions be identified based on the risk indicators and behavioral patterns described in this typology notice. If you submit a report to the FIU related to this typology, please refer to the keyword **10TT202607.**

One of the classic money laundering typologies in the gambling sector involves making deposits that are followed by little or no use of gambling services, or only low-risk betting activity[1]. Subsequently, the funds are withdrawn from the gambling operator's systems after a short period of time. This typology is also referred to as *cash in, cash out*[2]. The activity allows an individual to later claim that the apparent source of funds is gambling winnings, as the payout originates from the gambling operator. In reality, the gambling operator's systems are being used to facilitate payments and conceal the true origin of assets.

The FIU is aware of suspicious cases in which this typology has occurred within the systems of Estonian gambling operators.

This method can be used both in physical casino locations and in online casino systems. Payment methods may include bank transfers, card payments, cash, and virtual assets. The use of multiple payment methods and the structuring of transactions by one or more related individuals can further increase complexity. In online casinos, false accounts created using fraudulent identity information may also be used. Such accounts can be created quickly and in large numbers over the internet.

One of the methods used by gambling operators to mitigate risks related to this typology is the closed-loop payment system principle. This means that withdrawals from the gambling operator's systems must be made using the same payment method as was used for the

[1] In practice, there are also situations where a customer makes a deposit but does not find a suitable betting opportunity and therefore decides to withdraw the funds. Such situations may be justified if the customer provides a reasonable explanation and no other risk indicators are present. Therefore, limited or no gambling activity may not automatically indicate a money laundering risk. However, if a similar pattern continues, the customer's behavior should be analyzed with heightened scrutiny and assessed in conjunction with any other potential risk indicators.

[2] Online Gambling: Red Flags and Typoligies for Money Laundering, Terrorist Financing, and Proliferation Financing. https://www.fiu.im/media/1245/online-gambling-typology-2025.pdf

deposit. Where this principle is not applied (open loop), funds can be shifted between different payment methods, for example a cash deposit followed by a withdrawal to a bank account. Open-loop payment systems are significantly more vulnerable to money laundering than closed-loop systems.

Example cases of deposits and withdrawals

The following case studies have been compiled based on information received by the FIU.

Example Case 1

1. The customer made a deposit to a gambling operator.
2. Low-risk bets were placed on events with a high probability of winning.
3. The customer withdrew the funds from the gambling operator's system.

Example Case 2

1. The customer made a cash deposit to a gambling operator.
2. The deposited funds were used only minimally for gambling services.
3. The customer withdrew the funds via bank transfer to a bank account.

Example Case 3

1. The customer made a cash deposit to a gambling operator.
2. The customer made an additional deposit via bank transfer.
3. The funds were used only minimally for gambling services.
4. The customer withdrew the funds via bank transfer.

Example Case 4

1. The customer deposited virtual assets with a gambling operator.
2. The funds were not used for gambling services.
3. The funds were withdrawn from the gambling operator's system to a bank account.

Example Case 5

1. The customer made a deposit using a payment card.
2. The funds were not used for gambling services.
3. The funds were withdrawn from the gambling operator's system in virtual assets to a private address.
4. The funds were subsequently transferred from the private address to a virtual asset exchange platform.

Risk Indicators for Gambling Operators

Risk indicators on their own may not necessarily indicate money laundering, terrorist financing, or sanctions evasion. Therefore, it is important to distinguish normal customer behavior from higher-risk activities when analyzing information. For example, customers may legitimately use multiple bank cards or payment solutions. The size and frequency of deposits may vary due to promotional campaigns organized by gambling operators. Many of the indicators listed below may also occur in the course of ordinary gambling activity. **Consequently, customer-related information should always be analyzed as a whole. A single indicator that may be consistent with normal behavior can become suspicious when combined with other significant information.**

Possible Risk Indicators Related to Deposits and Withdrawals:

- The customer uses deposited funds only minimally for gambling services.
- The customer does not use deposited funds for gambling services at all.
- The customer places low-risk bets.
- The customer structures deposits into smaller amounts.
- Deposits are followed by withdrawals within a short period of time.
- Multiple payment methods are used to make deposits.
- A small payment is made before larger deposits are made (a test payment).
- Different payment methods are used for deposits and withdrawals (for example, a card deposit followed by withdrawal in virtual assets).
- The customer fails to provide documentation required for customer due diligence measures.
- There are suspicions that the customer is acting as a nominee or proxy.
- Documents showing signs of forgery are submitted during onboarding.
- Documents belonging to another person are submitted during onboarding.
- Withdrawals in virtual assets made by different customers are ultimately transferred to the same address or virtual asset exchange platform.
- Deposits in virtual assets made by different customers originate from the same address.
- Multiple customers use payment cards issued by the same service provider, and there are indications that their behavior is connected (such as use of the same IP address, conversion to crypto-assets, and transfers to the same address).
- A payment service provider sends a chargeback request or information indicating possible fraud related to a customer transaction.
- Public sources contain adverse information about the customer indicating possible criminal activity.
- The volume of the customer's transactions is not consistent with their declared income.
- There is suspicion that the person is connected to other individuals (for example, through the use of the same IP address).

When the described behavioral patterns or risk indicators are identified, obliged entities should assess the customer's behavior as a whole and consider applying enhanced due diligence measures where appropriate. If suspicions remain after enhanced due diligence measures have been applied, a report should be submitted to the Financial Intelligence Unit, with reference to the keyword 10TT202607 in the transaction description.