APPROVED BY
the order of director of
UNIGAMES UAB dated
26 July 2018

RULES ON PREVENTION OF MONEY LAUNDERING AND/OR TERRORIST FINANCING APPLICABLE TO REMOTE GAMING OPERATIONS

I. GENERAL PROVISIONS

1. The objective, scope and purpose of the rules on prevention of money laundering and terrorist financing (hereinafter the *Rules*) is to implement the requirements of legislation governing prevention of money laundering and terrorist financing at UNIGAMES, private limited liability company (hereinafter the *Company*).
2. The Rules are based on the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, the rules on managing registration log-books of monetary operations, transactions, and customers, as approved by the order of the director of the Financial Crime Investigation Service under the Ministry of Interior of the Republic of Lithuania (hereinafter the *Service*), the list of criteria for recognition of money laundering and suspicious monetary operations or transactions, as approved by the order of the director of the Service, instructions issued for companies running gaming, designed to prevent money laundering and/or terrorist financing, as approved by the order of the director of the director of the Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania, and other regulations.
3. The Rules shall govern identification of monetary operations that can be potentially related to money laundering and/or terrorist financing, personal identification of a client, suspension of suspicious monetary operations (transactions), gathering of details on monetary operations that can be potentially related to money laundering, and communication of such details to the Service, as well as implementation of international sanctions.
4. The Rules shall apply to the remote gaming operated by the Company, in gaming locations and/or devices used by the Company. Remote gaming and remote gaming operation shall have the meaning defined in the Gaming Law of the Republic of Lithuania. Any other terms not defined in the Rules shall be interpreted and used as defined in regulations listed under clause 2 of the same Rules.
5. The Rules shall be binding on the responsible and/or authorised staff members of the Company, provided their function is directly related to implementation of prevention measures on money laundering and terrorist financing, and provided such positions are included in a list approved by an order of the director of the Company (hereinafter the *Employee of the Company*).

II. GENERAL REQUIREMENTS APPLICABLE TO CLIENT IDENTIFICATION

6. The Company shall take targeted and proportional measures in order to identify and verify identification of a customer and/or register a customer:
   6.1. before business relations are initiated;
   6.2. in case if doubts concerning true or authentic nature of identification details of a customer obtained;
   6.3. in any other event given reason to believe that money laundering and/or terrorist financing operation is, was, or will be taking place.
7. The Company shall be further required to verify identity of a customer and/or register a customer:
8. In case an amount is paid, a prize is paid out, or a customer exchanges cash to tokens, or tokens to cash, in the event amount of cash exceeds EUR 1,000, or its equivalent in a different currency, whether or not a transaction in question takes place during one or more related operations.

9. Additional verification of identity means that regardless of previous identification of a customer, his/her identity shall be verified and/or registered in a logbook. This rule applies regardless opportunities for additional identification arising during a single, or several related operations (transactions). If the final amount of operation or value of a transaction is not available at the time of monetary operation, the Company shall be required to identify a customer as soon as it finds that the total value of monetary operations is equal to, or exceeds, the amounts set out in clause 10 of the Rules.
10. In the event several interrelated monetary operations take place, a customer must be identified immediately, as soon as the fact of several interrelated operations is established. Several monetary operations shall be considered interrelated, provided a customer:
    10.1. conducts several operations of cash payment into account per day, with total value being equal to, or exceeding EUR 15,000, or equivalent amount in foreign currency;
    10.2. conducts several operations of cash withdrawal from account per day, with total value being equal to, or exceeding EUR 15,000, or equivalent amount in foreign currency;
    10.3. conducts other monetary operations or enters into transactions per day, where these, according to the details available to the Company, are interrelated, with total value being equal to, or exceeding EUR 15,000, or equivalent amount in foreign currency;
    10.4. conducts several operations of cash exchange to tokens, or token exchange to cash per day, with total value exceeding EUR 1,000, or equivalent amount in foreign currency;
    10.5. makes payments or collects several prizes simultaneously, with total value exceeding EUR 1,000, or equivalent amount in foreign currency.
11. For the purposes of adequate identification of a customer, the Company shall:
    11.1. Conduct regular monitoring of business relations with customers in order to make sure that any monetary operations taking place correspond to the details available on the customer, nature of risk, and source of funds;
    11.2. Apply identification measures of a customer to both new, and existing customers, considering risk level, or in the event of new information related to establishment of risk level of a customer, his/her identity information, activities, and any other relevant factors;
    11.3. Store, review, and update documents, details or information (stored in printed and/or electronic format) produced at the time of identification of a customer, and take steps to ensure they remain both adequate and relevant;
    11.4. Use information from reliable and independent sources for identification purposes.
12. Details available to the Customer on the clients shall be reviewed and updated as follows:
    12.1. At least once per year, if a client is associated with a small risk of money laundering and/or terrorist financing;
    12.2. At least every 3 months, if business relations with a customer reveal at least a single criterion suggesting a considerable risk of money laundering and/or terrorist financing.
13. The Company shall prohibit its staff members to initiate, or to carry on, business relations, as well as to engage in monetary operations in cases below:
13.1. a customer does not offer personal identification details;
13.2. a customer fails to provide full details, or the details are false;
13.3. a customer refuses to provide information required to identify him/her;
13.4. a customer fails to provide sufficient details to allow for his/her identification.
14. An employee of the Company shall inform the manager of the Company (or an authorised individual) of any cases listed under clause 13 of the Rules immediately, and said individual shall, on the grounds provided by law, decide on reporting of a suspicious monetary operation or a transaction to the Service.
15. In the event the Company, during identification of a customer, suspects money laundering and/or terrorist financing, and any further steps of identification of a customer can make him/her suspect that his/her details will be disclosed to competent law enforcement authorities, the Company may

refuse to continue identification of a customer, and refuse to initiate business relations with such a customer. Such cases shall be reported to the Service.

III. IDENTIFICATION OF A CUSTOMER IN HIS/HER PHYSICAL ABSENCE

16. The Company shall, when conducting remote gaming, identify a customer in his/her physical absence relying on communication measures suitable for identification and/or information made available by the third parties. Whenever identifying a customer in his/her physical absence, the Company shall take steps to identify an verify identity of a customer and to obtain at least the following details on a customer:
    16.1. name (names);
    16.2. surname (surnames);
    16.3. personal ID number (in case of a foreigner, the following details shall be used: date of birth (where available, personal ID number or any other unique sequence of symbols assigned to relevant individual for personal identification), number and expiry date, issue place and date of a residence permit in the Republic of Lithuania (this applies to foreign nationals));
    16.4. picture;
    16.5. signature (except where signature is not required in a personal ID document);
    16.6. nationality (in the event of stateless individual, country issuing personal ID document shall be provided).
17. Whenever a customer is physically absent, the following measures and methods shall be used for identification purposes:
    17.1. information on a customer available to the third parties;
    17.2. measures of electronic recognition issued in the EU and functioning based on schemes of electronic recognition with high or sufficient security level[1];
    17.3. qualified electronic signature, involving a certificate of a qualified electronic signature in compliance with the Regulation (EU) No 910/2014;
    17.4. electronic measures allowing for video communication in one of the methods below:
        17.4.1. genuine copy of a personal ID document or equivalent residence permit in the Republic of Lithuania shall be recorded during direct video communication and identity of a customer shall be established using at least advanced electronic signature in compliance with the Regulation (EU) No 910/2014. For technical requirements applicable to the said procedure, see Annex 2;
        17.4.2. face image of a customer recorded during direct video communication, along with a genuine copy of a personal ID document or equivalent residence permit in the Republic of Lithuania, as shown by a customer. For technical requirements applicable to the said procedure, see Annex 2;
    17.5. Before the services of the Company can be made available, a payment order shall be issued to the payment account of the Company from account of a customer opened at a credit institution registered in a Member State of the European Union or the third country, where requirements equivalent to those imposed by the Law on the Prevention of Money Laundering and Terrorist Financing are in place, and competent authorities conduct monitoring of compliance with these requirements, followed by duly certified, printed copy of a personal identity document of a customer.
18. Identification of a customer in cases listed by sub-clause 17.1 to 17.3 of the Rules provided all of the following conditions exist:

---

[1] Technical and security details are established by the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ 2014 L 257, p. 73), hereinafter the *Regulation (EU) No. 910/2014*

18.1. before the Company proceeds with identification of a customer, such a customer has already been identified by a third party in his/her physical absence or relying on electronic measures allowing for direct video communication using one of the methods listed under sub-clause 17.4 or 17.5 of the Rules, as well as in the event where a customer has been identified in his/her physical absence by issuing a measure of electronic recognition, functioning based on scheme of electronic recognition with high or sufficient security level, or before qualified electronic signature certificate is issued;

18.2. a customer has been identified in cases listed by clause 6 to 9 of the Rules relying on a personal identity document of a customer issued by the Republic of Lithuania or foreign country, or a residence permit in the Republic of Lithuania, provided such document contains details of a customer and provide suitable identification.

19. Whenever identifying a customer in his/her physical absence, the Company shall be free to request details used for physical identification of a customer or where identification of a customer employs additional details, documents or additional information allowing to identify a customer and to verify existence of reasons for advanced identification of a customer.

20. The Company shall use information made available by the third parties for the purposes of customer identification, when such third party has sufficient measures to ensure that the third party voluntarily complies with both conditions below:

20.1. It shall, upon request, provide the Company with full information and details requested, as necessary in compliance with identification requirements established by law;

20.2. It shall, upon request, provide the Company with copies of customer identification documents as well as other documents pertaining to customer that are required in compliance with customer identification requirements.

21. When a customer is identified using video measures, customer identification process using video measures must be terminated given any of the conditions below:

21.1. Video or audio is communicated not in real time;

21.2. Direct video communication is terminated, or there are issues related to direct communication of video and/or audio;

21.3. Quality of direct video communication and picture does not clearly show face of a customer and/or prevents customer identification based on picture in a personal ID document;

21.4. Quality of direct video communication and sound quality is inadequate, and it is difficult to clearly hear and understand the answers offered by a customer on his/her identity;

21.5. An ID document of a customer is not recorded in full compliance with technical requirements applicable top video communication;

21.6. A customer fails to take adequate and timely steps requested by the Company;

21.7. A personal ID document produced by a customer has been damaged, forged, or there are other attributes leading to doubts as to authenticity of personal ID document in question (e.g. a copy of a document is provided). In this event, a customer identification process may continue, and information required for customer identification, shall only be gathered so as to report it to the Service immediately, in view of a risk of money laundering and/or terrorist financing;

21.8. A personal ID document produced by a customer does not meet the requirements applicable to content of such document;

21.9. The Company has reasonable doubts that a customer under identification is not the holder of a personal ID document provided, supporting identity of a customer;

21.10. More than one individual is involved in direct video communication or direct picture communication, during identification of a customer;

21.11. A customer fails to confirm, at least using advanced electronic signature, an electronic personal identity document (e.g. questionnaire) more than 1 hour, is such confirmation is required;

21.12. An individual does not accept direct video communication;

21.13. Different languages or other reasons prevent a customer and the Company from communicating or understanding each other;

21.14. During customer identification using video surveillance, the Company shall, in view of the risk of money laundering and/or terrorist financing, be free to suspend and terminate identification procedure also due to other circumstances other than listed under sub-clause 21.1 to 21.14.

22. The Company may not extend or renew identification of a customer involving video surveillance that has been terminated, and identification of a customer shall only be available in a new identification procedure.
23. The Company shall, when using customer identification measures involving video surveillance, take the following steps:
    23.1. Ensure that direct video communication takes place upon consent of a customer only;
    23.2. Ensure that only video made on real time can be communicated, that identification process is unbroken, and that customer identification steps are not taken in different times;
    23.3. Ensure that the measures used guarantee quality and colourful recording of video and/or audio, if applicable, that records are easily reproducible and recordable, and any personal data received when using the same are not altered or used for different purposes inconsistent with customer identification;
    23.4. Make sure that any measures used meet the technical requirements applicable;
    23.5. Ensure protection of personal data of a customer;
24. Any video records and pictures made during identification of a customer and stored by the Company shall bear an entry stating full name and personal ID number of a customer, IP address (in case a customer relies on hardware for identification purposes), and used by a customer when applying fo identification, as well as the date video recording was made or a picture was taken.

IV. ADVANCED IDENTIFICATION OF A CUSTOMER

25. The Company shall, before establishing business relations with a customer, and before commencing identification procedure of a customer, verify existence of circumstances warranting advanced identification of a customer.
26. Advanced identification of a customer shall apply as follows:
    26.1. When transactions or business relations involve natural politically exposed persons;
    26.2. When transactions or business relations involve natural persons residing in third countries, characterised by considerable risk, and having serious drawbacks in terms of prevention of money laundering and/or terrorist financing, and included in relevant lists compiled by the European Commission and the Financial Action Task Force on Money Laundering and Terrorist Financing;
    26.3. When the Company is convinced that elevated risk of money laundering and/or terrorist financing exists;
    26.4. In cases prescribed by the European supervisory authorities and the European Commission.
27. When an employee of the Company finds there is at least one indication for application of advanced identification, he/she shall immediately contact a senior manager appointed by the Company (hereinafter the *senior manager*) or an employee of the Company who administers remote gaming (remote gaming tools) conducted by the Company, and he/she shall report such information to the senior manager. An employee of the Company shall be free to initiate business relations with a customer subject to advanced identification criteria upon approval issued by the senior manager, either verbal or written.
28. An employee of the Company shall, after initiation of business relations with politically exposed persons, take relevant steps in order to identify source of assets and funds related to business relations or transactions involving the Company, and shall further conduct regular monitoring of actions of such politically exposed person.
29. In case a natural person involved in politics no longer holds key public office, the Company shall, within a period of at least 12 months, continue to take into account risk caused by such individual, and shall choose and apply measures proportional to such risk, until it is established that an individual no longer poses a risk inherent to natural politically exposed persons.

30. The Company shall, when proceeding with advanced identification of a customer with respect to natural persons residing in third countries, characterised by considerable risk, and having serious drawbacks in terms of prevention of money laundering and/or terrorist financing, and included in relevant lists compiled by the European Commission and the Financial Action Task Force on Money Laundering and Terrorist Financing, and in cases when Company is convinced that elevated risk of money laundering and/or terrorist financing exist, take one or more additional customer identification measures in order to mitigate the existing risk, and shall be required to:
    30.1. Obtain approval of the senior manager to engage into, or continue, business relations with such customers;
    30.2. Take adequate steps in order to identify source of assets and funds related to business relations or transaction;
    30.3. Conduct advanced regular monitoring of business relations with such customers.
31. The Company shall pay particular attention to any risk of money laundering and/or terrorist financing that may result from transactions conducted, where steps are taken to conceal identification of a customer (i.e. anonymity is preferred), as well as from business relations or transactions with a customer whose identify has not been established in his/her physical presence, and shall, where necessary, take steps to prevent use of such assets for money laundering and/or terrorist financing.

V. REPORTS ON SUSPICIOUS MONETARY OPERATIONS OR TRANSACTIONS

32. The Company shall immediately, within 1 business day after occurrence of such information or suspicions, report to the Service if the Company is aware of, or suspects, that assets, regardless its value have been obtained, directly or indirectly, from criminal activities or results from involvement in such activities, as well as if the Company is aware of, or suspects, that assets in question are designated to support a single, several terrorists, or a terrorist organisation.
33. In the event the Company finds that a customer is engaged in a suspicious monetary operation or transaction, it shall, regardless of amount of monetary operation or transaction, suspend operation or transaction in question (except where it is objectively impossible, given nature of monetary operation or transaction, their conduct method or other circumstances), and within 3 business hours after suspension of a monetary operation or transaction, report operation or transaction in question to the Service. Suspicious operations and transactions shall be identified in view of activities conducted by a customer that, in the opinion of the Company, may be related to money laundering and/or terrorist financing due to its nature, in course of customer identification and regular monitoring of business relations to a customer, including investigation, in the manner prescribed by laws, of transactions entered into during said relations.
34. Whenever the Company becomes aware that a customer intends, or will try, to conduct a suspicious monetary operation or transaction, it must inform the Service immediately.
35. Where the Company is instructed by the Service in writing to suspend any suspicious monetary operations or transactions conducted by a customer, it shall be required to, effective the time indicated or occurrence of specific circumstances, suspend operations or transactions for a period of up to 10 business days. In the event the Company is not required, within 10 business days after issue of such notification or after receipt of an instruction, to comply with temporary restriction of title in the manner prescribed by the Code of Criminal Procedure of the Republic of Lithuania, such monetary operation or a transaction shall be renewed.
36. In the event a customer avoids, or refuses to produce additional information to the Company, based on its request and in the time-limits specified by the same, the Company shall be free to refuse conducting monetary operations or a transaction, and to terminate transactions or business relations with a customer.
37. Employees of the Company and other responsible employees appointed by the Company shall, when informed by the Service that suspension of a monetary operation or transaction may interfere with an investigation concerning legalisation of funds or assets received through criminal enterprise, terrorist

financing and other criminal acts, related to money laundering and /or terrorist financing, abstain, since the moment indicated in a written instruction, from suspending suspicious operations or transactions conducted by a customer.

38. The Company shall communicate to the Service any identification details of a customer and information on one-off cash payment, with minimum total value of cash received of EUR 15,000, or more, or equivalent amount in foreign currency[2].
39. When the Company is reporting details to the Service, the senior manager shall report of a suspicious monetary operation or suspicious transaction suspended of a customer to the Service after log-in to the IT system of the Service, and after completion of a report form of suspicious monetary operations or suspicious transactions approved by the director of the Service. Report addressed to the Service on a suspicious monetary operation or suspicious transaction shall include the following:
    39.1. Identification details of a customer (full name and personal ID number of a natural person (in case of a foreigner, the following details shall be used: date of birth (where available, personal ID number or any other unique sequence of symbols assigned to relevant individual for personal identification)));
    39.2. Criterion approved by the Service, concerning an operation or transaction, allowing to suggest that a monetary operation or transaction is considered suspicious;
    39.3. Method of completion of suspicious monetary operation or suspicious transaction;
    39.4. Date of suspicious monetary operation or suspicious transaction, characterisation of assets subject to transaction (cash etc.), and its value (amount of money, currency used for conduct of monetary operation or transaction, asset market value etc.);
    39.5. Methods of account management;
    39.6. Contact details of a customer (phone numbers, e-mail addresses, contact persons, their phone numbers, e-mail addresses);
    39.7. Entity benefiting from suspicious monetary operation or suspicious transaction (full name and personal ID number of a natural person (in case of a foreigner, the following details shall be used: date of birth (where available, personal ID number or any other unique sequence of symbols assigned to relevant individual for personal identification)), and in case of legal entity, title, legal form, registered address, and registration number, if such has been assigned);
    39.8. Date and time of suspension of a suspicious monetary operation or suspicious transaction;
    39.9. Description of assets that a customer cannot control or use from the moment of suspension of suspicious monetary operation or suspicious transaction (place and other information characterising assets);
    39.10. In the event a suspicious monetary operation or transaction has not been suspended, relevant reasons;
    39.11. Other relevant details, according to the Company.
40. In urgent cases, the Service can be informed verbally (on the phone), to be confirmed, immediately, by the senior manager using tools listed by clause 39 of the Rules.
41. In the event the Service requests further information in writing, as pertaining to a suspicious monetary operation or transaction currently suspended, such information shall be duly provided within 1 business day after receipt of a relevant request, in writing or using technical text communication measures.

---

[2] A report is provided in compliance with the description of procedure on reporting of information on monetary operations or transactions with minimum amount of EUR 15, 000, or more, or equivalent amount in foreign currency, to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania, approved by the order of the Minister of the Interior of the Republic of Lithuania dated 16 October 2017 No. 1V-701, concerning approval of description of procedure on suspension of suspicious monetary operations or transactions, and on reporting of information on suspicious monetary operations or transactions to the to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania, and procedure on reporting of information on monetary operations and transactions with minimum amount of EUR 15, 000, or more, or equivalent amount in foreign currency to the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania.

42. Whenever employees of the Company or any other employees responsible appointed by the Company become aware that a customer intends, or will try, to conduct a suspicious monetary operation or transaction, they must inform the senior manager immediately, and if he/she is out on a business trip, or is otherwise unavailable for other valid reasons, another responsible individual appointed, shall inform the Service immediately.
43. Senior manager or any other responsible individual shall immediately, but no later than within 7 business days after conduct of a monetary operation or entry into transaction report to the Service any identification details of a customer as well as information on one-off cash payment, with minimum total value of cash received exceeding EUR 15,000, or more, or equivalent amount in foreign currency.

VI. KEEPING OF REGISTRATION LOGBOOKS

44. For the purposes of remote gaming, the Company shall keep (complete) the following registration logbooks reflecting monetary operations and transactions (hereinafter the *registration logbooks*):
    44.1. registration logbook of customers who make payments, collect prizes or exchange cash to tokens, or tokens to cash, with total value exceeding EUR 1,000, or equivalent amount in foreign currency;
    44.2. Registration logbook of reports, suspicious monetary operations and transactions;
    44.3. Registration logbook of customers, where transactions or business relations have been terminated.
45. Interim registration logbooks can be kept in both printed and electronic form; details included in the interim registration logbooks shall be entered and processed in an electronic medium.
46. The Company shall include in the registration logbook of customers who make payments, collect prizes or exchange cash to tokens, or tokens to cash, with total value exceeding EUR 1,000, or equivalent amount in foreign currency the following, in chronological order:
    46.1. details of a customer (full name and personal ID number (date of birth in case of a foreign national), and nationality) exchanging cash to tokens, or tokens to cash, as well as details of a customer who makes payments or collects prizes, with total value exceeding EUR 1,000, or equivalent amount in foreign currency;
    46.2. other details on the fact of exchange of cash or tokens, payment of an amount, payment of a prize (date and time of exchange, payment of amount, payment of a prize, amount of money, currency, and exchange method (when cash is exchanged to tokens, or tokens to cash)).
47. Registration logbook of reports, suspicious monetary operations and transactions shall include the following, in chronological order:
    47.1. Identification details of a customer (full name and personal ID number of a natural person (in case of a foreigner, the following details shall be used: date of birth (where available, personal ID number or any other unique sequence of symbols assigned to relevant individual for personal identification)));
    47.2. Criterion approved by the Service, concerning an operation or transaction, allowing to suggest that a monetary operation or transaction is considered suspicious;
    47.3. Method of completion of suspicious monetary operation or suspicious transaction;
    47.4. Date of suspicious monetary operation or suspicious transaction, characterisation of assets subject to transaction (cash etc.), and its value (amount of money, currency used for conduct of monetary operation or transaction, asset market value etc.);
    47.5. Methods of account management;
    47.6. Contact details of a customer (phone numbers, e-mail addresses, contact persons, their phone numbers, e-mail addresses);
    47.7. Entity benefiting from suspicious monetary operation or suspicious transaction (full name and personal ID number of a natural person (in case of a foreigner, the following details shall be used: date of birth (where available, personal ID number or any other unique sequence of symbols assigned to relevant individual for personal identification)), and in case of legal entity, title, legal form, registered address, and registration number, if such has been assigned);
    47.8. Date and time of suspension of a suspicious monetary operation or suspicious transaction;

47.9. Description of assets that a customer cannot control or use from the moment of suspension of suspicious monetary operation or suspicious transaction (place and other information characterising assets);

47.10. In the event a suspicious monetary operation or transaction has not been suspended, relevant reasons;

47.11. Other relevant details, according to the Company.

48. The Company shall include in the registration logbook of customers, where transactions or business relations have been terminated the following, in chronological order:

48.1. identification details of a customer (full name and personal ID number (date of birth in case of a foreign national), and nationality);

48.2. reasons for termination of transactions or business relations pertaining to breaches of procedure of prevention of money laundering and/or terrorist financing.

49. Details shall be entered in the registration logbooks in chronological order, based on monetary operation or documents supporting transaction or any other documents holding legal power, pertaining to conduct of monetary operations or entry into transactions, immediately, but no later than within 3 business days after conduct of a monetary operation or entry into transaction.

VII. PROCEDURE OF KEEPING AND ADMINISTRATION OF REGISTRATION LOGBOOKS

50. Registration logbooks shall be completed and kept in an electronic medium by the senior manager, and if he/she is out on a business trip, or is otherwise unavailable for other valid reasons, another responsible employee appointed by the Company, as indicated in a special order of the director, setting out the scope of duties and responsibilities assigned to an individual acting as a substitute.

51. Interim registration logbooks may be completed in printed form. Interim registration logbooks shall be completed by designated employees of the Company.

52. Responsible employees appointed by the Company shall, within 3 business days, communicate any details included in the interim registration logbooks, to the senior manager responsible for completion of the registration logbooks in electronic medium.

53. Employees of the Company shall ensure protection of data included in the interim registration logbooks from unauthorised deletion, alteration, use, or disclosure to the third parties without a written approval issued by the manager of the Company. The director of the Company shall appoint an employee charged with a duty to ensure protection of the data included in the registration logbooks, and processed in an electronic medium, from unauthorised deletion, alteration, or use by the third unauthorised parties.

54. Details of the registration logbooks shall be stored in a separate file, at the Company server. Details shall be stored for 8 years after termination of transaction or business relations with a customer. Details shall be stored using software allowing for export of details stored to Microsoft Office Excel, Word, or equivalent open-code software, without damaging integrity of the details.

55. Keeping of the registration logbooks shall be verified by the senior manager, and if he/she is out on a business trip, or is otherwise unavailable for other valid reasons, another responsible employee appointed by the Company, as indicated in a special order of the director, setting out the scope of duties and responsibilities assigned to an individual acting as a substitute.

56. The employees of the Company shall be prohibited to inform, or otherwise let know, any customer or other individuals that information on the monetary operations taking place, or transactions conducted by a customer, or resulting investigation is communicated to the Service.

VIII. CLOSING PROVISIONS

57. In the event the Service, having received a report or other details using electronic text communication measures, has a reason to doubt reliability or contents of a report or details provided, it can request

correction of details provided. A responsible individual who has provided a report or other details using electronic text communication measures shall be required to correct such details immediately.

58. The Company shall, regularly or following material events or changes to the management and operation of the Company, monitor implementation of the Rules, and introduce stricter procedures on internal control where necessary.
59. The Company shall review the Rules regularly and update them where necessary.
60. Responsible employees of the Company shall be introduced to the Rules. Failure to respect the Rules shall make the employees of the Company liable to sanctions provided by law.

ANNEX 1

CONDITIONAL ATTRIBUTES OF SUSPICIOUS MONETARY OPERATIONS

1. A monetary operation or a transaction shall be considered suspicious where:
   1.1. a customer exchanges cash to tokens, or tokens to cash in a given calendar day, with total value exceeding EUR 15,000, or equivalent amount in foreign currency. This criterion shall apply under the following circumstances:
      1.1.1. *a monetary operation is extremely large to a specific customer;*
      1.1.2. *a customer tries to remain unidentified, i.e. he/she has covered his/her face, avoids proximity of surveillance cameras, tries to keep his/her personal ID document at hand, etc.;*
      1.1.3. *a customer exchanges cash to tokens, or tokens to cash in a given calendar day, with total value exceeding EUR 15,000, or equivalent amount in foreign currency, although previously this was unusual to a customer;*
      1.1.4. *a customer refuses, upon request of the Company, to provide valid explanation and information of monetary operations currently conducted;*
      1.1.5. *the Company is aware that a monetary operation of a customer may pertain to money laundering and/or terrorist financing.*
   1.2. A customer regularly exchanges cash to tokens, or tokens to cash, without taking part in a game. This criterion shall apply under all of the following circumstances:
      1.2.1. *a customer cannot, or refuses to, clarify the basis for such monetary operations;*
      1.2.2. *a customer regularly exchanges cash to tokens, or tokens to cash without taking part in a game, although previously this was unusual to a customer;*
      1.2.3. *the Company is aware that a monetary operation of a customer may pertain to money laundering and/or terrorist financing.*
1.3. The nature of monetary operations and transactions results in suspicion of intention to avoid inclusion of monetary operations and transactions in the registration logbook of suspicious monetary operations and transactions, kept by the Company. This criterion shall apply under the following circumstances:
      1.3.1. *a customer, not conducting cash exchange operations, takes part in games without interruption and for extended period of time;*
      1.3.2. *a customer refuses, without a reason, and without offering a valid and full explanation, to conduct cash exchange operations, although this is unusual in view of intensity and duration of involvement in a game;*
      1.3.3. *actions taken by a customer where he/she immediately and constantly avoids operations of cash exchange during a game, lead to valid and objective suspicions that such actions pertain to moany laundering and/or terrorist financing.*
2. Employees of the Company and other responsible employees appointed by the Company shall be required to:
2.1. Pay attention to activities that they believe can be related, due to its nature, to money laundering and/or terrorist financing, especially complex or unusually large transactions and any unusual structures of transactions without a clear economic or obvious legitimate purpose;
2.2. Hand over to the senior manager the basis and purpose of such operations or transactions for investigation. Senior manager shall finalise the outcome of investigation of such unusual operations or transactions in writing. Any letters containing outcome of investigations above shall be stored for 8 years, in printed or electronic medium;
2.3. Monitor business relations related to involvement in game by customer regularly;
2.4. Assess the need to update information available on a customer subject to business relations, and, in view of the freshness of information available or any new facts concerning change in such information, update information received at the time of customer identification.

ANNEX 2

TECHNICAL REQUIREMENTS APPLICABLE TO CUSTOMER IDENTIFICATION, IN CASE OF REMOTE IDENTIFICATION, USING ELECTRONIC MEASURES ALLOWING FOR DIRECT VIDEO COMMUNICATION

1. Technical requirements applicable to customer identification, in case of remote identification, using electronic measures allowing for direct video communication (hereinafter the technical requirements) shall set out conditions for customer identification in case of remote identification, using electronic measures allowing for direct video communication (hereinafter the measures) in the methods listed under the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania.
2. **Use of measures, option 1**

2.1. In case of option 1, measures can be used during direct video communication to record genuine personal ID document (hereinafter the ID document) or equivalent residence permit in the Republic of Lithuania (hereinafter the ID document) of a customer, and customer shall be identified at least using advanced electronic signature in compliance with Article 26 of the Regulation (EU) No. 910/2014.

2.2. When a genuine personal ID document of a customer is recorded during direct video communication, personal ID document in question shall be displayed in one of the following methods:

2.2.1. personal ID card and a residence permit in the Republic of Lithuania shall be displayed from both sides;

2.2.2. when a passport is displayed, picture of a passport with a picture of a natural person and cover of a passport shall be displayed.

2.3. During direct video communication, any personal ID document shall be turned several times, in order to make sure that a document displayed is authentic and genuine.

2.4. When genuine personal ID document of a customer is recorded using direct picture communication, parts of document listed in clause 2.2. shall be recorded. Special software, applications, or other measures shall be used to ensure that pictures are taken without interruptions, and preventing any communication of pictures, except in real time.

2.5. Where actions listed under clause 2.2. to 2.4. are completed, a customer shall confirm his/her identity and truth of the details provided by signing an electronic questionnaire designed to identify a customer (e.g. a questionnaire) using at least advanced electronic signature in compliance with the Regulation (EU) No 910/2014. Confirmation at least using advanced electronic signature must take place immediately, within 1 hour of actions listed by clause 2.2. to 2.4. of the Technical Requirements, and shall be part of a customer identification procedure.

2.6. When confirmation is based on advanced electronic signature, legality and authenticity of a signature must also be verified.

2.7. Direct video communication or pictures communicated directly shall have quality allowing for an easy retrieval of information of information from personal ID documents produced, and clearly display features of an individual portrayed in a picture of a personal ID document.

2.8. Ability to provide additional instructions and commands addressed to customer, in order to alter position of a document.

3. **Use of measures, option 2**

3.1. In case of option 2, measures can be used, during direct video communication, for recording of image of a customer's face and genuine personal ID document produced by a customer.

3.2. In case image of a customer's face and genuine personal ID document produced by a customer is recorded during direct video communication, the following steps shall be taken:

3.2.1. frontal image of a customer's face shall be recorded (image must show face and shoulders of a customer; image must be clearly visible and distinguishable from other objects in the vicinity);

3.2.2. A customer shall demonstrate genuine personal ID document as described in clause 2.2. and 2.3.;

3.2.3. Frontal image of a customer's face and genuine personal ID document must be displayed for certain time together, in order to allow identification of facial features of a customer with the facial features of an individual presented on the picture of a personal ID document produced;

3.2.4. A customer shall be asked questions on his/her identity, using an approved questionnaire;

3.2.5. Direct video communication shall include pictures of image of a customer's face and personal ID document displayed.

3.3. Actions listed under clause 3.2. shall be taken without interruptions, during the same video communication.

3.4. In case image of a customer's face and genuine personal ID document is recorded using picture communication, the following steps shall be taken:

3.4.1. frontal image of a customer's face shall be recorded (image must show face and shoulders of a customer; image must be clearly visible and distinguishable from other objects in the vicinity);

3.4.2. direct communication of a picture in personal ID document produced. Parts of ID document recorded are listed in clause 2.2. Special software, applications, or other measures shall be used to ensure that pictures are taken without interruptions, and preventing any communication of pictures, except in real time.

3.5. Actions listed under clause 3.4. shall be taken without interruptions; they shall be part of identification of a single customer.

3.6. Once actions listed under clause 3.2., 3.3., 3.4. or 3.5. are taken, a customer shall be informed that by submitting details, he/she further confirms they are correct.

3.7. Ability to provide additional instructions and commands addressed to customer, in order to alter position of facial image or a personal ID document. There must be an option to ask a customer to remove his/her head or face cover, glasses or other objects preventing suitable recording of image of a customer's face.

3.8. Process of direct video communication or direct picture communication, used for customer identification, can involve a single customer only at a time.

3.9. Direct video communication or pictures communicated directly shall have quality allowing for an easy retrieval of information of information from personal ID documents produced, and clearly display features of an individual in question and those of an individual portrayed in a picture of a personal ID document, without any doubts that the personal ID document contains specifically picture of an individual present at video broadcasting. Throughout such actions, video recording must be of high quality, to enable hearing answers given by a customer to questions concerning his/her identity.