

Introduction

Garilla Poker is operated by Royal Assa N.V. having its office at Abraham de Veerstraat 9 Willemstad, Curacao. Company Registration number 157430.

Royal Assa N.V. is licensed and authorized by the Government of Curacao and operates under the Master License of Gaming Services Provider, N.V. #365/JAZ as an Information Service Provider.

Objective of the AML Policy

We seek to offer the highest security to all of our users and customers on garillapoker.com for that a three step account verification is done in order to insure the identity of our customers.

The reason behind this is to prove that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else, which is to create the general framework for the fight against money laundering. We also take into account that depending on the nationality and origin, the way of payment and for withdrawing different safety measurements must be taken.

Royal Assa N.V. also puts reasonable measures in place to control and limit ML risk, including dedicating the appropriate means.

Royal Assa N.V. is committed to high standards of anti-money laundering (AML) according to the EU guidelines, compliance and requires management & employees to enforce these standards in preventing the use of its services for money laundering purposes.

The AML program of Royal Assa N.V. is designed to be compliant with :

- EU : “Directive 2015/849 of the European Parliament and of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering”
- EU : “Regulation 2015/847 on information accompanying transfers of funds”
- EU : Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods
- BE : “Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash

Definition of money laundering

Money Laundering is understood as:

- The conversion or transfer of property, especially money, knowing that such property is derived from criminal activity or from taking part in such activity, for the purpose of concealing or disguising the illegal origin of the property or of helping any person who is involved in the commission of such an activity to evade the legal consequences of that person's or companies action;
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from assisting in such an activity;
- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points before.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Organization of the AML for Royal Assa N.V.

In accordance with the AML legislation Royal Assa N.V. has appointed the “highest level” for the prevention of ML: The full management of Royal Assa N.V. are in charge.

Furthermore, an MLRO (Money Laundering Reporting Officer) is in charge of the enforcement of the AML policy and procedures within the System.

The AMLCO is placed under the direct responsibility of the general Management.

AML policy changes and implementation requirements

Each major change of garillapoker.com AML policy is subject to approval by the general management of Royal Assa N.V. and the Anti money laundering compliance officer.

Three step Verification

Step one verification

Step one verification must be done by every user and customer to withdraw.

Regarding the choice of payment, the amount of payment, the amount of withdraw, the choice of withdraw and nationality of the user/customer step one verification must be done first.

Step one verification is a document that must be filled out by the user/customer himself. Following information must be filled in: first name, second name, date of birth, country of usual residence, gender and full address.

The customer is also obliged to provide the scan of his passport or id. Sometimes, a selfie with passport hold in hands will be required.

Step two verification

Step two verification must be done by every user who wants to make a withdrawal to a card or electronic money wallet.

Until step two verification is done the withdraw, tip or deposit will be hold.

Step two verification will lead the user or customer to a subpage where he must send the following confirmation:

If the user wishes to withdraw to a bank card, he will required to send a photo of the bank card he wishes to withdraw to. A photo of the front and back of the card will be necessary. The first 6 digits and the last 4 digits of the card should be visible. CVV code should be blurred.

If the card does not contain the name of the card holder, we would require a screenshot from the mobile banking profile.

If the users wishes to withdraw to an electronic money wallet, we would require a screenshot of the users electronic money wallet profile.

Step three verification

Step three verification must be done by every user which deposit over 5000 EUR (five thousand Euro) or withdraws over 5000 EUR (five thousand Euro) or sends another user over 3000 EUR (three thousand EUR) Until step three verification is done the withdraw, tip or deposit will be hold. For step 3 a user/customer will be asked for a source of wealth.

Customer identification and verification (KYC)

The formal identification of customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC policy.

This identification relies on the following fundamental principles:

A copy of your passport, ID card or driving license, each shown alongside a handwritten note mentioning six random generated numbers.

Also, a second picture with the face of the user/customer is required. The user/customer may blur out every information, besides date of birth, nationality, gender, first name, second name and the picture. To secure their privacy.

Please note that all four corners of the ID have to be visible in the same image and all details has to be clearly readable besides the named above. We might ask for all details if necessary.

An employee may do additional checks if necessary, based on the situation.

Sanctions list and PEP (politically exposed person) check

A Politically Exposed Person (PEP), is an individual who is in a notable public position such as a President, Politician, Mayor, etc.

Transactions involved with PEPs are considered as high-risk transactions, Royal Assa N.V. needs to be aware of your status to minimise this risk.

We divide PEP's into the following categories:

- Foreign PEPs includes Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials in a foreign country.
- Domestic PEPs like foreign PEPs are individuals who are or have been entrusted domestically with prominent public functions.
- International organization PEPs are persons who are or have been entrusted with a prominent position by an international organization. This may be directors, deputy directors and members of the board or equivalent functions.
- Family members are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.
- Close associates are individuals who are closely connected to a PEP, either socially or professionally.

Sources of information for PEPs databases are almost exclusively official government websites (presidency, government, legislative bodies, supreme courts of

justice, military administration etc.) and official gazettes where laws, decrees, investitures and depositions are published.

The lists we check you comprises the following sanctions lists:

- United Nations;
- European Union;
- US Treasury Department;
- The United Kingdom Ministry of Finance;
- Switzerland SECO;
- Australian sanctions.

PEP lists are always dynamic and are constantly being updated.

Royal Assa N.V. does not provide services to individuals listed in the PEP lists and sanctions lists.

Proof of Address

Proof of address will be done via to different electronic checks, which use two different databases. If an electronic test fails, the user/customer has the option to make a manually proof.

A recent utility bill sent to your registered address, issued within the last 3 months or an official document made by the government that proofs your state of residence.

To make the approval process as speedy as possible, please make sure the document is sent with a clear resolution where all four corners of the document is visible, and all text is readable.

For example: An electricity bill, water bill, bank statement or any governmental post addressed to you.

An employee may do additional checks if necessary, based on the situation.

Source of funds

If a player deposits over a five thousand euro there is a process of understandings the source of wealth (SOW)

Examples of SOW are:

- Ownership of business
- Employment
- Inheritance

- Investment
- Family

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible an employee may ask for an additional document or prove.

The account will be frozen if the same user deposits either this amount in one go or multiple transactions which amount to this. An email will be sent to them manually to go through the above and an information on the website itself.

Royal Assa N.V. also asks for a bank wire/credit card to further insure the Identity of the user/customer. It also gives additional information about the financial situation of the user/customer.

Basic document for step one:

The basic document will be accessible via the setting page on Royal Assa N.V.. Every user has to fill out the following information:

- First name
- Second name
- Nationality
- Gender
- Date of Birth

The document will be saved and created by an AI, an employee may do additional checks if necessary based on the situation.

Risk management

In order to deal with the different risks and different states of wealth in different regions on the earth Royal Assa N.V. will categorize every nation in three different regions of risk.

Region one: Low risk:

For every nation from the region one the three-step verification is done as described earlier.

Region two: Medium risk:

For every nation from the region two the three-step verification will be done at lower deposit, withdraw and tip amounts. Step one will be done as usually. Step two will be done after depositing 1000 EUR (one thousand Euro), withdrawing 1000 EUR (one thousand Euro) or tipping another user/customer 500 EUR (five hundred Euro.) Step three will be done after depositing 2500 EUR (two thousand five hundred Euro), withdrawing 2500 EUR (two thousand five hundred Euro) or tipping another user/customer 1000 EUR (one thousand Euro). Also, users from a low risk region

that change crypto currency in any other currency will be treated like user/customers from a medium risk region.

Region three: High risk:

Regions of high risks will be banned. High risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

Additional measurements.

In addition, an AI which is overseen by the AML compliance officer will look for any unusual behaviour and report it right away to a employee of Royal Assa N.V.

According to a risk based few and general experience the human employees will recheck all checks which are done before by the AI or other employees and may redo or do additional checks according to the situation.

In addition, a data Scientist supported by modern, electronic, analytic systems will look for unusual behaviour like: Depositing and withdrawing without longer Betting sessions.

Attempts to use a different Bank account to for Deposit and Withdraw, nationality changes, currency changes, behaviour and activity changes as well as checks, if an account is used by it's original owner.

Also a User has to use the same method for Withdraw as he used for Deposit, for the amount of the initial Deposit to prevent any Money Laundering.

Enterprise-wide risk assessment

As part of its risk-based approach, Royal Assa N.V. has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and understand risks specific to Royal Assa N.V. and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on Royal Assa N.V. understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is yearly reassessed.

Ongoing transaction monitoring

AML-Compliance ensures that an “ongoing transaction monitoring” is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

This transaction monitoring is conducted on two levels:

1) The first Line of Control:

Royal Assa N.V. works solely with trusted Payment Service Providers whom all have effective AML policies in place as to prevent the large majority of suspicious deposits onto Royal Assa N.V. from taking place without proper execution of KYC procedures onto the potential customer.

2) The second Line of Control:

Royal Assa N.V. makes its network aware so that any contact with the customer or player or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned. In particular these include:

- Requests for the execution of financial transactions on the account;
- Requests in relation to means of payment or services on the account;

Also, the three-step verification with adjusted risk management should provide all necessary information's about all costumers of Royal Assa N.V. at all time.

Also, all transaction must be overseen by employees over watched by the AML compliance officer who is over watched by the general management.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager must also be subject to due diligence.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behaviour and the transaction counterparty.

These checks will be done by an automated System, while an Employee crosschecks them for additional security.

The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly justifiable).

Any Royal Assa N.V. staff member must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known of the customer.

3) The third Line of Control:

As a last line of defence against AML Royal Assa N.V. will do manually checks on all suspicious and higher risk users in order to fully prevent money laundering.

If fraud or Money Laundering is found the authorities will be informed.

Reporting of Suspicious transactions on Garillapoker.com

In its internal procedures, Royal Assa N.V. describes in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

Reports of atypical transactions are analysed within the AML team in accordance with the precise methodology fully described in the internal procedures.

Depending on the result of this examination and on the basis of the information gathered, the AML team:

- will decide whether it is necessary or not to send a report to the FIU, in accordance with the legal obligations provided in the Law of 18 September 2017;
- will decide whether or not it is necessary to terminate the business relations with the customer.

Procedures

The AML rules, including minimum KYC standards will be translated into operational guidance or procedures that are available on the Intranet site of Royal Assa N.V..

Record keeping

Records of data obtained for the purpose of identification must be kept for at least ten years after the business relationship has ended.

Records of all transaction data must be kept for at least ten years following the carrying-out of the transactions or the end of the business relationship.

These data will be safely, encrypted stored offline and online.

Training

Royal Assa N.V. human employees will make manual controls on a risk based approve for which they get special training.

The training and awareness program is reflected by its usage:

- A mandatory AML training program in accordance with the latest regulatory evolutions, for all in touch with finances
- Academic AML learning sessions for all new employees

The content of this training program has to be established in accordance with the kind of business the trainees are working for and the posts they hold. These sessions are given by an AML-specialist working in Royal Assa N.V. AML team.

Employees shall be instructed as following:

Definition

Suspicious transaction means a transaction conducted or attempted by, at, or through the Gaming Operation that the Gaming Facility Operator knows, suspects, or has reason to suspect. A transaction which is inconsistent with a customer's known legitimate business or personal activities or with the normal business for the type of securities holdings or contract which the customer holds.

Failure to comply with the requirements of this section may constitute a violation of the reporting rules of the Curacao (formerly Netherland Antilles) Gaming Authority and will result in immediate revocation of License.

How to identify a Suspicion?

An effective systemic approach to identifying suspicious financial activity may safeguard you from the risk of being involved with terrorist financing and money laundering crimes. Use the "SAFE" approach which may assist you in legal compliance and staff training.

S: Screen

A: Ask customer

F: Find

E: Evaluate

Each of the four steps of the systemic approach to suspicious activity identification are discussed in more detail in the following paragraphs.

Screen: Screen the account for suspicious indicators

The recognition of an indicator, or better still indicators, of suspicious activity is the first step in the suspicious activity identification system. The following are some of the suspicious activity indicators most commonly associated with money laundering. Large or frequent cash transaction, either deposits or withdrawals.

- Suspicious activity based on transaction pattern, i.e.

- Involvement of one or more of the following entities which are commonly involved in money laundering,
- Currencies, countries or national of countries, commonly associated with international crime or drug trafficking or identified as having serious deficiencies in their AML / CFT regimes,
- Customer refuses, or is unwilling, to provide an explanation of financial activity, or provides an explanation assessed to be untrue.
- Activity is incommensurate with that expected from the customer considering the information already known to you about the customer and the customers previous financial activity
- Countries or nationals of countries, commonly associated with terrorist activities or the persons or organizations designated as terrorists or their associates. Details can be found on the website about sanction on terrorists or their associates.
- Politically Exposed Persons (PEPs)

Ask: Ask the customer appropriate questions

If your staff carries out a transaction or transactions for a customer, bearing one or more suspicious activity indicators then they should question the customer on the reason for conducting the transaction and the identity of the source and ultimate beneficiary of the money being transacted.

On occasions some of the staff may be reluctance to ask questions of the type mentioned above. Grounds for this reluctance are that the customer may realize that he, or she, is suspected of illegal activity, or regards such questions as none of the questioner's business.

Appropriate questions to ask in order to obtain an explanation of the reason for conducting a transaction bearing suspicious activity indicators will depend upon the circumstances of the financial activity observed.

Another example is when a customer receives "structured" remittances from overseas. In such circumstances staff could question the customer on the reason for receiving numerous remittances within a short period of time on the grounds that one larger remittance would be quicker, cheaper for the sender to send, and less time consuming for the recipient to handle.

Persons engaged in legitimate business generally have no objection to, or hesitation in answering such questions. Persons involved in illegal activity are more likely to refuse to answer, give only a partial explanation or give an explanation which is unlikely to be true.

If a customer is unwilling, or refuses, to answer questions or gives replies which staff suspect are incorrect or untrue, this may be taken as a further indication of the suspicious nature of the financial activity.

Find: Find out the customer's records

The third stage in the systemic approach to suspicious activity identification is to review the information already known about the customer and his, or her, previous transactions and consider this information to decide if the apparently suspicious activity is to be expected from the customer. This stage is commonly known as the "know your customer principle".

Institutions, businesses or professions hold various pieces of information on their customers which can be useful when considering if the customers' financial activity is to be expected or is unusual. Examples of some of these information items and the conclusions which may be drawn from them are listed below.

Evaluate: Evaluate all the above information.

The final step in the suspicious activity identification system is the decision whether or not to make an STR. Due to the fact that suspicion is difficult to quantify, it is not possible to give exact guidelines on the circumstances in which an STR should, or should not, be made. However, such a decision will be of the highest quality when all the relevant circumstances are known to, and considered by, the decision maker, i.e. when all three of the preceding steps in the suspicious transaction identification system have been completed and are considered. If, having considered all the circumstances, staff find the activity genuinely suspicious then an STR should be made.

Staff will seldom, if ever, encounter a situation in which a customer carries out apparently suspicious activity which they have reason to suspect is linked to a specific crime or type of crime. Institutions, businesses or professions are therefore encouraged to make STRs in circumstances where, although they do not know which specific crime or type of crime is connected to the suspicious transaction, there are one or more suspicious activity indicators present, together with an inability or unwillingness on the part of the customer to give a reasonable and legitimate explanation and inconsistency between the financial activity undertaken and that which is to be expected from the customer.

What to Report in an STR?

A STR should include the following details:

- personal particulars (name, identity card or passport number, date of birth, address, telephone number, bank account number) of the person(s) or company involved in the suspicious transaction;
- details of the suspicious financial activity;

- the reason why the transaction is suspicious - which suspicious activity indicators are present?
- the explanation, if any, given by the person about the transaction

Auditing

Internal audit regularly establishes missions and reports about AML activities.

Data Security

All data given by any user/customer will be kept secure, will not be sold or given to anyone else. Only if forced by law, or to prevent money laundering data may be shared with the AML-authority of the affected state.

Royal Assa N.V. will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC)

Money Laundering Reporting Officer (MLRO)

Royal Assa N.V. will appoint a senior employee to be the Money Laundering Reporting Officer (MLRO) as required by the Money Laundering Regulation. The MLRO will have the responsibility for the establishment and maintenance of AML/CTF framework of the company and underlying systems and controls and will provide reports to the Board of the company.

Royal Assa N.V. will ensure that the MLRO is of sufficient seniority within the company and has the relevant experience and understanding of AML/CTF to carry out their duties. Royal Assa N.V. will fully support and ensure the MLRO has necessary resources and will provide ongoing support and development for the MLRO.

The MLRO, with the support of the Board, is responsible for ensuring that the Company meets its AML compliance requirements in accordance with applicable legislation. The MLRO will oversee the AML systems and controls and ensure they are fit for purpose. The main activities of the MLRO comprise, but are not limited to, the following:

- oversight of all aspects of the company's AML and CTF activities;
- focal point for all activities within the company relating to AML and CTF;
- provision of AML training to all staff;
- receiving all internal suspicious activity reports and, where deemed applicable, reporting to relevant authorities on the same;
- be the focal point for law enforcement and other regulatory bodies;
- establishing the basis on which a risk-based approach to the prevention of money laundering and terrorist financing is put into practice;

- supporting and coordinating senior management focus on managing the money laundering/terrorist financing risk in individual business areas; and
- advising the business on new products / processes from an AML perspective.

The MLRO is also required to produce reports for Board meetings including, but not limited to, the following items:

- Confirmation that adequate customer due diligence information is being collected and that ongoing monitoring is taking place;
- Summary data relating to complex or unusual transactions;
- Number of internal consents / Suspicious Activity Reports received from staff members;
- Number of Suspicious Activity Reports sent externally;
- Information on status of staff training within the company;
- Confirmation that all business records have been properly stored and are retained according to regulatory requirements;
- Changes in the law/operating environment which do or might impact the business;
- Changes in the risk matrix affecting the business; and
- Contacts with the regulator in regards of any Suspicious activity reports.

In accordance with our license requirements Royal Assa N.V. is obliged to report any suspicious transactions to the license holder Gaming Services Provider, N.V..