

AML Policy of Curacao Co N.V.

Last updated: 25/05/2026

For Deposits and Withdrawals.

(AML Anti-Money-Laundering policy of shock.com)

Introduction: shock.com is operated by **PR Entertainment N.V** having its office at Zuikertuintjeweg Z/N Zuikertuin Tower Unit 1B & 1C, Curacao. Company Registration number 163398 ("Company," "We," or "US").

Objective of the AML Policy: Company seeks to offer the highest security to all users and customers. For that reason a multi-step account verification process is used to appropriately identify the users. The reason that users are identified is to ensure that the details of the person opening and using an account identify the actual user and that the deposit methods used are not stolen or being used by someone else. This comprises the basic framework for Company's policies against money laundering. The steps outlined below are designed to provide general guidance on how Company will carry out its AML policy by using increasingly detailed information for customer identity verification. Company reserves the right to, based on its sole discretion, escalate the identification requirements by asking for more detailed documents earlier in the process or by asking for additional documents not listed below. The user shall provide all such documents when requested by Company. If the user does not provide all such documents that Company requests, Company may ban, cancel, lock, or otherwise block the user's account until the earlier of the user providing the documents or the Company terminating its relationship with the user. Company puts reasonable measures in place to control and limit ML risk, including dedicating the appropriate means. Company is committed to high standards of anti-money laundering (AML) according to the EU guidelines. Company requires management & employees to enforce these standards in preventing the use of its services for money laundering purposes.

The AML program of shock.com 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 shock.com:

In accordance with certain AML legislation, shock.com has appointed the “highest level” for the prevention of money laundering: the full management of Company is in charge.

Furthermore, an AMLCO (Anti Money Laundering Compliance Officer) is in charge of the enforcement of the AML policy and procedures within the Company.

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

AML policy changes and implementation requirements:

Each major change of shock.com AML policy is subject to approval by the general management of Company and the AMLCO.

Multi step Verification:

Step one:

Every user must provide an email address to open an account. In order to deposit or withdraw any funds, every user must verify that email address and provide the user's: name, address, occupation, date of birth.

Every deposit and withdrawal to and from the Company is scanned by the Company's choice of analytic service. The service notifies company employees of potential risks associated with a user's wallet. Depending on the results of those scans, the Company may escalate the verification process.

Step two:

Company reserves the right to require step two verification for deposits and withdrawals for any reason, including but not limited to, the amount and size of the deposit, frequency of the deposits, suspicious activity. In addition, any user whose crypto wallet triggers Company's blockchain analytics service will be required to perform this second step of verification. Company may also, at its sole discretion, require any user to perform the second step of verification for any reason. Step two verification will lead the user through Company's identity verification process which may include, but is not limited to, providing Company with: a picture of the user's government identification card or its equivalent, selfies to be scanned with AI, other similar information.

Step three:

If the previous steps alert Company to additional concerns, or at its discretion, the user may be asked to provide additional documentation, which includes but is not limited to: a utility bill, proof of the source of funds, etc.

Customer identification and verification (KYC)

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

This identification relies on the following the required steps of Company's choice of identity verification service and any additional requests made by Company.

Risk management:

In addition, Company's identity verification and wallet scanning technologies will continue to look for unusual behaviour and alert the appropriate employees of Company.

While using a risk based approach, manual reviews by Company employees may also be utilized.

Enterprise-wide risk assessment

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

The EWRA is reassessed yearly.

Ongoing transaction monitoring

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

This transaction monitoring is conducted on multiple levels:

1) The first Line of Control:

The provision, by the user, of attestations of name, DOB, location, and occupation are the first line of control. Upon deposit or withdrawal, crypto wallets are scanned for suspicious activity. Upon the triggering of an alert or the deposit/withdrawal of a certain amount of money, more information is required. Company also works solely with trusted Payment Service Providers who all have effective AML policies in place to prevent the large majority of suspicious deposits onto Company’s website from taking place without proper execution of KYC procedures.

2) The second Line of Control:

Company’s continual scanning of all deposits and withdrawals creates opportunities for Company to address any growing concerns. In the event of those concerns, Company uses an identity verification service. By using the website, the user agrees to submit to these services. Company reserves the right to request any additional information that it, in its sole discretion, is necessary or advisable.

Also, all transactions are overseen by employees who are over-watched by the AML compliance officer who is over-watched by the general management.

Specific transactions submitted to the customer support manager, possibly through their Compliance Manager, are also subject to due diligence.

Determination of the unusual nature of one or more transactions sometimes depends on a subjective assessment of: employee’s knowledge of the customer, the financial behavior of the customer, the parties to the transaction.

These checks will first be done by an automated system, while an Employee may manually check for additional security when necessary or advisable.

(3) Third line of control:

The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds may be identified as a special risk, must be rapidly considered, and additional analysis may be conducted, including manual checks.

All Company staff and employees inform the AML division of any problematic transactions which they observe.

Reporting of Suspicious transactions on shock.com

Reports are made to the appropriate authorities when required by law.

Reports of problematic transactions are analysed within the AML team in accordance with the internal procedures.

Depending on the result of this examination and on the basis of the information gathered, the AML team will determine the appropriate FIU authority to which a report must be made and whether to terminate its relationship with the user.

Procedures

The AML rules, including minimum KYC standards, will be translated into operational guidance or procedures that are available to Company and its employees.

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.

This data will be safely encrypted and stored.

Training:

Company employees will take manual actions on a risk based approach for which they get special training.

As part of the training and awareness program:

- Company requires mandatory AML training for its employees who participate in the transaction process in accordance with the latest regulatory evolutions
- The content of this training program has been tailored to match the duties of Company employees.

Auditing

Internal audits are performed regularly. Reports are made about AML activities on a regular basis.

Data Security:

All data given by any user/customer will be kept secure and will not be sold or given. Only if under the compulsion of law, or to prevent money laundering, data may be shared with the necessary AML authority.

Company will follow all guidelines and rules of the data protection directive Directive 95/46/EC.

Contact us:

If you have any questions about our AML and KYC Policy, please contact us:

- By email: support@shock.com

If you have any complaints about our AML and KYC Policy or about the checks done on your Account and your Person, please contact us:

- By email: support@shock.com