

Know Your Customer (KYC) Procedures

Surewin B.V

Table of Contents

CHANGE CONTROL	3
1. CUSTOMER DUE DILIGENCE	4
1.1 INTRODUCTION	4
1.2 THE CUSTOMER DUE DILIGENCE (CDD) MEASURES	4
1.3 IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER	5
1.4 OBTAINING INFORMATION ON THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP	5
1.5 IDENTIFICATION AND VERIFICATION OF THE PLAYER	6
1.6 ON-GOING MONITORING	7
1.7 TIMING OF CDD MEASURES	10
1.8 ENHANCED DUE DILIGENCE	11
1.9 SIMPLIFIED DUE DILIGENCE	15
1.10 POLITICALLY EXPOSED PERSONS	15
1.11 APPLICATION OF CDD MEASURES TO EXISTING CUSTOMERS	21
1.12 THE TERMINATION OF THE BUSINESS	22
1.13 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE	23
SCHEDULE 3 – PEP ASSESSMENT FORM	24

Change Control

Version	Name	Date
1.1	Craig Murugan	Date Prepared: 09/04/2024

1. Customer Due Diligence

1.1 Introduction

Surewin B.V adheres to and complies with “Know You Customer” principles, which aim to prevent financial crime and money laundering through client identification and due diligence.

Surewin B.V may at any time ask for any KYC documentation it deems necessary to determine the identity and location of a user.

Surewin B.V will restrict the service, payment, or withdrawal until identity is sufficiently determined, or for any other reason in our sole discretion based on the legal framework.

We take a risk-based approach and perform strict due diligence checks and ongoing monitoring of all clients, customers, and transactions.

As per the Money Laundering Regulations, we utilize 3 stages of due diligence checks, depending on the risk, transaction, and customer type.

- SDD – Simplified Due Diligence is used in instances of extremely low risk transactions that do not meet the required threshold.
- CDD – Customer Due Diligence is the standard for due diligence checks, used in most cases for verification and identification.
- EDD – Enhanced Due Diligence is used for high-risk customers, large transactions or unusual cases.

1.2 The Customer Due Diligence (CDD) measures

CDD measures are not in principle applicable until the two thousand Euro (€2,000) threshold is reached. However, to ensure the proper functioning of AML/CFT controls, a minimum level of CDD measures prior to the said threshold being reached is applied. Thus, simultaneously with the opening of an account, Surewin B.V identifies the customer by collecting the personal details which are set as the minimum applicable in case of low-risk scenarios.

Clients must first register with us and open an account in order to be able to place bets and deposit money:

- They are only allowed to have one account per client, which must be registered personally.
- They are only allowed to create one account on the Website that we supply. If a client tries to open more than one account, all of their bets may be forfeited, and all of their accounts may be blocked or cancelled. Any duplicate / multiple account may be terminated at any moment by Surewin B.V
- Surewin B.V conducts verification checks on clients, and accounts that are found to have provided incorrect or misleading information may be blocked or closed.
- Accounts must contain correct information to allow for the proper risk assessment of the player therefore fictitious, anonymous and numbered accounts are prohibited.
- Documents provided to verify an address should not refer to PO Boxes or ‘care of’ addresses.

Customers who do not reach the CDD threshold of two thousand Euro (€2000) are to be identified, by keeping the details usually obtained through our registration process. These details include:

- a) Full name;
- b) Residential address;
- c) Country of residence;
- d) Date of birth.

Deposits and payments details are reviewed and verified to ensure they match the personal data submitted by the customer, preventing the customer from receiving a deposit or making a payout from or to a third party. Deposits and payments details that are verified, depending on the method of payment used, may include name, date of birth and/address.

Customers not meeting the CDD threshold of two thousand Euro (€2,000) are nonetheless monitored and if an unusual deposit or game activity is noted, they are nonetheless subjected to KYC.

Surewin B.V also ensure that any first withdrawal is subjected to KYC.

1.3 Identification and verification of the Beneficial Owner

Surewin B.V does not support - and the system does not allow - the registration of business participants, organisations, foundations, legal arrangements or individuals acting on behalf of organisations as customers. The registration process will only facilitate the application of an individual. Should an individual be found to be acting on behalf of an organisation, their account will be immediately frozen and suspended.

1.4 Obtaining information on the Purpose and Intended Nature of the Business Relationship

As part of the Customer Due Diligence (CDD) process, Surewin B.V will obtain and assess information regarding the **purpose and intended nature** of the business relationship at the time of account opening or onboarding.

This includes understanding:

- The **expected types and volume of activity**.
- The **source of funds and source of wealth**, where applicable.
- The **customer's business or occupation**, and how it relates to the relationship.

This information helps determine the customer's risk profile and ensures appropriate ongoing monitoring. The level of detail obtained will be proportionate to the assessed risk and the nature of the relationship.

The following measures will be implemented:

- **Customer Profiling:** Information such as occupation, source of funds, gaming preferences, and expected transaction volumes will be collected during registration or account creation.
- **Enhanced Due Diligence (EDD):** For high-risk customers (e.g., VIPs, foreign nationals, PEPs), additional verification and documentation of source of wealth will be required.

- **Transaction Monitoring:** Actual behaviour will be monitored and compared with expected patterns to detect inconsistencies.
- **Loyalty Program Data:** Customer relationship data from loyalty programs will be reviewed to assess transaction history and gaming behaviour.
- **Risk-Based Approach:** Each customer will be assigned a risk rating to determine the appropriate level of due diligence and monitoring.
- **Ongoing Reviews:** Customer profiles will be periodically updated, especially when significant changes in behaviour are observed.
- **Staff Training:** Employees will be trained to identify and document the purpose of a customer's relationship with the casino and to escalate concerns appropriately.

These measures ensure that Surewin B.V understands the nature of its customers' activities and can identify unusual or potentially suspicious behaviour, in line with regulatory requirements.

1.5 Identification and Verification of the player

Identification and verification of the player

Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

Customers must provide sufficient, clear, and eligible documents for identification verification. The following documents are required: Evidence of identity must include a customer's full name, residential address, and date of birth as they appear in the registration account. Upon reaching the 2000 EUR threshold in deposits the information listed may be verified by obtaining one or more of the below:

- A valid unexpired passport;
- A valid unexpired national or other government-issued identity card;
- A valid unexpired residence card; or
- A valid unexpired driving license.

The verification of the residential address shall be carried out by referring to any one of the following documents:

- A recent statement from a recognised credit institution. Bank Statements are allowed only if they are issued by a subject person carrying out relevant financial business in Curacao or equivalent activities in a reputable jurisdiction.
- A recent utility bill or a similar document should be provided, ensuring that it pertains to services connected to the specific residential property.
- A rental agreement
- A correspondence from a central or local government authority, department or agency.
- Any valid unexpired government-issued document (Passport, National Identity, Driving License), where a clear indication of residential address is provided.
- Documents, other than official government issued documents, must not be more than six months old.

Documents provided to verify an address should not refer to PO Boxes or 'care of' addresses.

If the casino obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly when the type of document is unfamiliar.

Customers are contacted by email to their registered email address requesting them to send the documents. All documents are uploaded in electronic format using the secured platform. Received documents are inspected and compared to images of official documents of the same type. Additional information is requested if any documents do not appear to be authentic or are inconsistent with other known information about the customer.

1.6 On-Going Monitoring

Ongoing monitoring of identity

Ongoing monitoring comprises of continuous and periodic checks to ensure customers remain acceptable, identify changes that could affect a customer risk assessment and any unusual activity. This monitoring is undertaken in three parts:

- Review of CDD/EDD to ensure the information held remains accurate, up to date and appropriate for the customer relationship;
- Scrutiny of transactions to ensure they are in line with CDD/EDD and expected activity of the customer; and
- Sanctions monitoring.

Monitoring CDD/EDD

By monitoring CDD/EDD Surewin B.V can:

- Consider risk assessments for the customer and the business;
- Determine what is expected activity for the customer;
- Help protect Surewin B.V from criminals.

High risk customers will be subject to annual review of EDD including SOW.

Surewin B.V Risk Team will review CDD and EDD accordingly.

When a high risk customer is approved for play their account will be subject to a diary alert that will prompt the risk team to undertake a review of the EDD held. This prompt, delivered via email, will be sent one month before the anniversary of the account approval (and annual thereafter).

The review will consist of:

- Checking the ID document on file remains current
- Review SOW information to ensure it remains accurate using the information held on file via open source checks
- Screen for negative press via internet searches

If any of this information cannot be confirmed as current / accurate the customer will be contacted to provide updated information / documentation.

Upon review of a high risk customers EDD, the risk team will send the review via email for review and approval to a Senior Manager. Any changes to circumstances will be communicated to the MLRO for review, risk assessment and additional approval.

Standard and Medium risk customers CDD will be reviewed during a trigger event.

Valid Due Diligence

Surewin B.V takes steps to maintain valid due diligence documentation for all players. When due diligence documentation is obtained, the expiry date of the identity document is recorded. When the expiry date is approaching, a notification is sent to the Risk team who will in turn contact the player to request an updated identity document be provided.

In respect of other due diligence, such as documents provided for proof of address or source of wealth, these will be considered at trigger events and updates requested on a case-by-case basis. As a standard, if a document was provided more than two years ago updated documentation will be requested.

Should the requested documents not be provided, the case will be referred to the MLRO to consider the appropriate next steps, which may include open-source research to determine if the information held remains current or if non-traditional means can be applied.

Ongoing monitoring of transactions

In line with our risk based approach Surewin B.V must apply appropriate scrutiny to all transactions.

To achieve this the following transaction monitoring is undertaken:

- Special attention will be given to monitoring account activity, and to the extent possible, the purpose and background of any more complex or large transactions and any transactions which are particularly similar, by their nature, to be related to any form of money laundering or the funding of terrorism.
- The risk staff will be responsible for this monitoring and will review any activity that the monitoring system detects and also will determine whether any additional steps are required,
- When the risk agent detects any activity that may be unusual, he or she must notify the MLRO. The MLRO will make an in-depth decision whether or not and how to further investigate the matter.
- The organization will not accept cash or non-electronic payments from clients. Funds may be received from clients only by any of the following methods: credit cards, debit cards, electronic transfer and any other method approved by the respective regulators.
- The organization will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.
- Transfers of funds between clients' accounts are prohibited.
- To the extent the organization utilizes a third party to process and record payments to and from client and accounts, the organization will ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions to these provisions and in accordance with the applicable legislation.
- Records relating to the financial transactions shall be maintained in accordance with the data protection act.
- Fraud / Risk Management teams will monitor transactions.
- The monitoring will always be considered in line with the customer's risk assessment and

expected activity.

- Attempt to remove a card from an account or withdraw to an account which is not the same as the depositing source;
- Customer deposits for the first time with a payment method exposed to chargebacks;
- Customer tries to deposit using a credit or debit card issued in a country that does not reflect the residence of the customer;
- Customer deposits with a new payment method while having a balance in the account.

Moreover, even before reaching the two thousand Euro (€2,000) threshold, Surewin B.V has systems in place which allow it to apply a level of on-going monitoring. Through these systems, Surewin B.V ensures:

- a) To determine the moment in time when the two thousand Euro (€2,000) threshold is met.
- b) To stop players from deliberately avoiding CDD checks by staying under the €2,000 transaction limit.

The latter is ensured through the following procedures:

- a. We are able to determine the moment in time when the two thousand Euro (€2,000) threshold is met through daily reports hitting our risk inbox with a list of Customers meeting this criterion.
- b. Customers opening multiple accounts are closed to avoid having customers opening multiple to bypass the (€ 2,000) rule.
- c. We can detect the application for the opening of an account by a person who has inputted manifestly false details via our SIFT tool. Our Risk team also reviews the list of accounts opened daily to safeguard against this risk.

In such instance, when the two thousand Euro (€2,000) threshold has not been reached, there will be no need for additional CDD documentation to be collected. However, if Surewin B.V already notices inconsistencies at this stage between the information provided by the customer and any other information Surewin B.V may acquire through interaction with the customer, Surewin B.V shall question these discrepancies and take any remedial action it deems necessary, including, where applicable, filing an UTR with the FIU.

This CDD threshold is to be continuously monitored and any customers meeting the threshold should be included on the AML monitoring list.

Sift Tool

We can detect the application for the opening of an account by a person who has inputted manifestly false details. We have a tool called Sift that assists with identifying fictitious accounts.

Sift is a machine learning technology that has become the market leader in fraud prevention, acquiring customers across industries such as e-commerce, fintech, and iGaming.

Key features of Sift Technology:

- Device ID features
- Features that track email address characteristics
- Features that capture physical address characteristics

Sift has been implemented at registration for Surewin B.V

- All new accounts will be screened across Sift database for detecting promo abuse, fictitious accounts.

- Fraudsters will create multiple accounts very quickly to illegally obtain new player bonuses.
- They might change email address, change phone number, or mask their IP address.
- They will be targeting multiple operators in one go and will not have the time or the ability to change every identity signal that Sift is analysing. For example, if they change
- All signals mentioned above, Sift will be tracking the device fingerprint of the user and can link users together as such inconsistencies at this stage between the information provided by the customer and any other information Surewin B.V may acquire through the interaction with the customer, Surewin B.V shall question these discrepancies and take any remedial action it deems necessary.
- Any missed accounts will be picked up upon KYC verifications.

1.7 Timing of CDD Measures

CDD measures are to be applied when carrying out transactions amounting to two thousand Euro (€2,000) or more. The moment in time when the CDD obligations (along with carrying out a customer risk assessment) are triggered and must be applied are to be determined as follows:

In the case of an occasional transaction, the obligation to carry out CDD will be dependent on the value of the said transaction reaching or exceeding two thousand Euro (€2,000). This also applies in the case where a series of linked transactions are executed which, though individually are below the said threshold, they would cumulatively meet or exceed the two thousand Euro (€2,000) threshold. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. The two thousand Euro (€2,000) is to be calculated only based on deposits made by the customer without taking into consideration any bonuses or winnings accumulated onto the account.

The two thousand Euro (€2,000) deposit threshold is calculated considering all deposits effected by a customer since the establishment of the business relationship.

Surewin B.V decided to follow the latter.

If the threshold is met, then a customer risk assessment needs to be carried out, whereby Surewin B.V is to identify the customer, verify his/her identity and, if deemed high risk, determine the customers source of wealth and the source of the funds used for the said transactions or carry out such other measures as may be sufficient to mitigate the risks identified.

The following table sets out the levels of CDD and EDD, depending on Customer Risk Assessment or trigger event.

EDD	Certified CDD			✓
	Selfie with ID – case by case basis			✓
	3rd party background – case by case basis			✓
	Open source research			✓
	SOW			✓
CDD	Evidence of Identity at threshold		✓	✓
	Transaction monitoring from initial deposit (ongoing)	✓	✓	✓
	PEP, Sanctions and Negative Press / Adverse Media screening from first deposit (ongoing)	✓	✓	✓
	Country and IP screening upon registration	✓	✓	✓
	Risk rating	Standard	Medium	High/ Unusual activity

1.8 Enhanced Due Diligence

Enhanced due diligence (EDD) is the term used to describe measures that are required to be carried out for higher risk customers in addition to the CDD requirements required for standard risk customers. Due diligence should be risk-based therefore conducting enhanced measures in higher risk scenarios will focus AML/CFT measures on the customers that pose the highest risks.

In addition to collecting EDD for higher risk customers, EDD would also be applied in the event of the following:

Unusual activity

- The customer was identified as holding a prominent position within an international organisation;
- The customer is/was involved in professional sports; or
- The customer uses multiple sources to fund their gambling activity;
- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;

- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Any request for EDD must be completed within **30 days**. If a request is not satisfied within **30 days**, the MLRO must be informed and consideration given if a UTR is required in line with the reporting procedures.

In instances of unusual activity, EDD would not be applied if it would result in tipping off a customer that there was an investigation underway.

EDD Measures

Any player that is categorised as high risk must be subject to EDD.

EDD comprises of five elements in addition to standard CDD. Four of those five elements require "consideration" as each high risk customer must be treated on a case-by-case basis - risk factors reviewed, understood, and appropriate measures taken to address the risk posed by the customer.

The four elements to consider are as follows:

1 - Additional identification information (consider if)

Obtaining additional identification information would be appropriate where risks relate to the possibility of stolen or fake identity. It can also assist in confirming or discounting potential PEP, sanctions or negative press matches or when conducting open source research.

Examples of additional information include:

- Middle names
- Aliases
- Former names
- Nationality(ies)
- Gender
- Official person identification number
- Occupation
- Name of employer
- Previous address

2 - Additional verification (consider if)

Consideration should be given to carrying out additional measures to verify the customer's identification information as part of standard CDD and to verifying additional information provided as part of the EDD.

Examples of additional verification methods include:

Obtaining additional ID documents such as driver's licence, student card or bus pass

- A telephone or video call with the customer
- Request a selfie of the customer holding their ID or outside their home address (which can then be verified using google maps, etc.)
- Verify information supplied using internet searches and open source databases (e.g. Facebook, LinkedIn)

3 - Background research (consider if)

For high risk customers, particularly those with large or unusual transactions or where there are concerns over the SOW, Surewin B.V must make efforts to establish whether the customer has been accused or convicted of proceeds generating crime (e.g. theft, fraud).

This is achieved using open source information, name screening for negative press or by commissioning third party reports.

The MLRO is experienced in undertaking such research and will assist with any such circumstances.

4 - Additional ongoing monitoring (consider how)

The policy requires all ongoing monitoring to be risk-based, therefore monitoring of high risk customer should be conducted more frequently and comprise of more extensive checks.

The type of monitoring will depend on the relevant risk factors.

As a standard the following EDD measures are applied:

- Obtaining additional ID documents such as driver's licence, student card or bus pass that has not been used a standard proof of identity
- A video call with the customer
- Obtaining a selfie of the customer holding their ID or outside their home address (which can then be verified using google maps, etc.)
- Sending a document for signature by courier to the home address for it to be signed and returned by the customer with the journey being tracked
- Verify information supplied using internet searches and open source databases or social media (e.g. Facebook, LinkedIn)

EDD will be considered on a case by case basis. In some circumstances the MLRO may advise that additional measures be applied depending on the risk factors identified.

EDD must also be conducted in the case of any suspicious activity is identified – the MLRO will advise on what EDD is required in these circumstances.

A customer will have **30 days** from the initial request to provide EDD. Should EDD not be provided within that time frame, the customer's account will be immediately suspended and consideration given to the completion of a UTR.

5 - Source of Wealth

The fifth element of EDD is source of wealth. Unlike the other elements detailed above, SOW **must** be undertaken when EDD is triggered (high risk, PEP etc).

In these circumstances, the policy sets out that Surewin B.V must reasonably establish and understand a customer's SOW.

SOW is distinct from source of funds and describes the origins of a person's financial standing or total net worth, i.e. what activities have generated the customer's funds.

The measures used to establish SOW will vary depending on the risks associated with the customer and the value of their transactions. When determining the appropriate measures the following factors will be considered:

- What factors resulted in the customer being classified as high risk;
- The value of the customer's transactions; and
- The period over which the transactions occurred and, if over a short period of time, consider what the value would be at that rate over the course of a year

Depending on the risk factors SOW will be considered using information available within the public domain, making use of social media such as LinkedIn and employee profiles on company websites. Such research will in all cases be undertaken and all considerations documented.

Surewin B.V is not required to contact a customer to establish SOW however, in this example, it would be appropriate to do so. In instances where information isn't available to source independently the following may be requested, on a case by case basis, as advised by the MLRO:

- An up to date CV
- A copy of recent bank statements
- Copies of pay slips and/or employment contract
- Details of any businesses owned
- Documentation to evidence inheritance or the sale of an asset

From the additional information provided further checks will be carried out in order to evidence if the SOW can now be verified.

In all instances, whether through independent checks or information provided by the customer, consideration will be given to:

- How reliable or independent the source of the information is;
- How plausible the information is; and
- How this compares to the customer's activity.

Source of Wealth vs Affordability

The majority of customers enjoy gambling as a leisurely activity making use of disposable income, however Surewin B.V recognises that gambling of significant portions of income should prompt interaction with the customer from a responsible gambling point of view.

Should SOW checks indicate that, when considered in line with betting activity, affordability is in question Surewin B.V will contact the customer in line with the responsible gambling policy.

Background research

During SOW verification, any information that raises any concerns or for high risk customers with large or unusual transactions Surewin B.V will conduct background research in order to establish, as far as possible, whether the customer has been accused or convicted of any crime that could have generated illicit funds such as fraud or theft.

Background research will be conducted by the Risk team who has been sufficiently trained to undertake this research.

The research will comprise of:

- Open source checks
- Name screening for negative press via screening tools
- Screening of any entity or person that forms part of their SOW

All research will be documented within the back office including any determinations made.

10.9 Simplified Due Diligence

Simplified Due Diligence (SDD) may be applied in low-risk situations where the likelihood of money laundering or terrorist financing is minimal and where permitted.

- The customer is resident in a jurisdiction with effective AML/CFT controls, not listed as high-risk by FATF or the EU.
- The product or account limits exposure to risk, e.g. low deposit limits, non-reloadable, no third-party payments, or strict withdrawal controls.
- There is no reason to suspect the customer is involved in money laundering or terrorist financing.
- The customer is not a politically exposed person (PEP).
- The customer relationship is non-anonymous, and there is no use of privacy-enhancing technologies that obscure identity (e.g., certain cryptocurrencies or VPN masking).
- Surewin B.V uses alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.).

1.10 Politically Exposed Persons

PEP's and Sanctions

Introduction

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Screening for PEPs and Sanctions

Upon first deposit customers are screened against PEP and Sanctions lists via Namescan (and thereafter ongoing screening throughout the duration of the customer relationship).

How to Perform a PEP & Sanction search on the Namescan Screening Tool

Step 1: Log In

- ✓ Go to the [Namescan website](#)
- ✓ Log in using your authorized username and password

Step 2: Navigate to the Search Section

- ✓ Once logged in, go to the Dashboard
- ✓ Click on "New Scan"

Step 3: Enter Search Details

- ✓ In the search form, enter the full name of the individual or entity
- ✓ Optional fields (if available):
- ✓ Date of Birth
- ✓ Country

Step 4: Start the Scan

- ✓ Click "Search" or "Submit" to initiate the scan
- ✓ Wait for the scan to complete—usually just a few seconds

Step 5: Review the Results

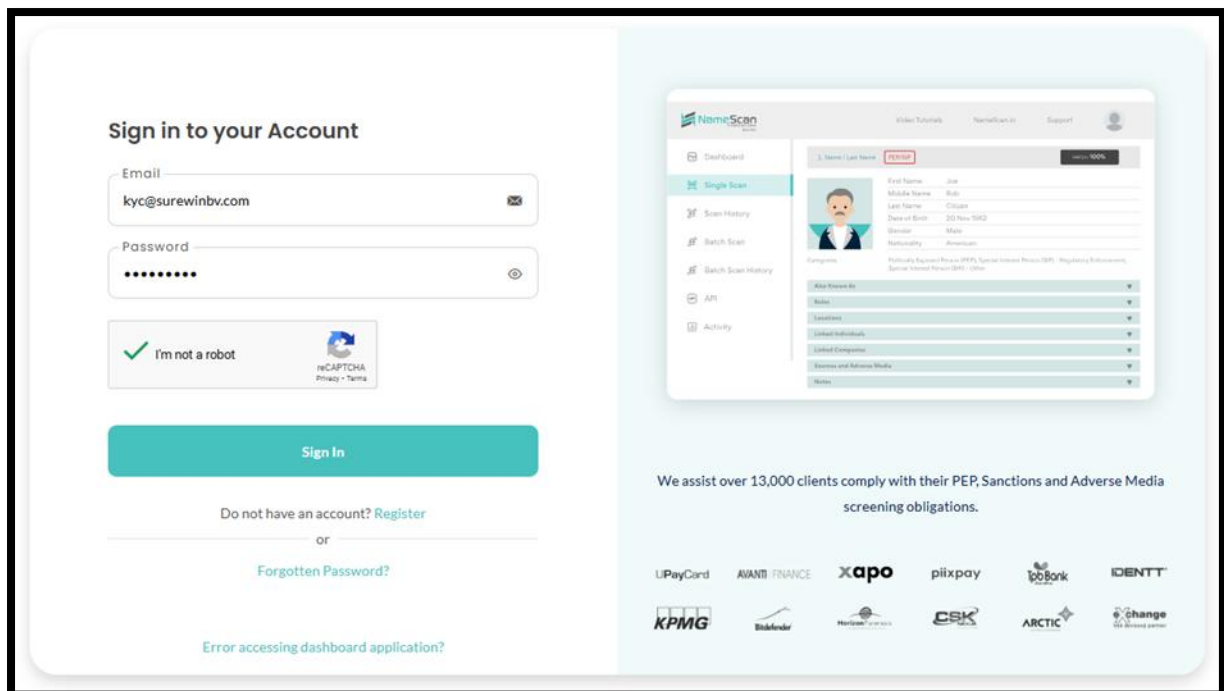
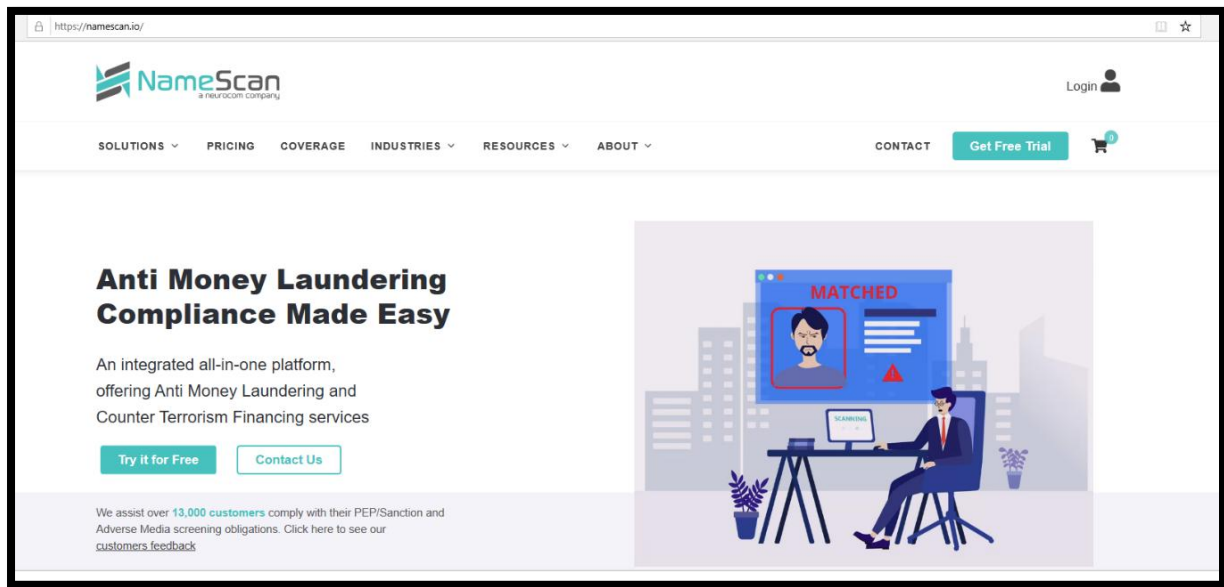
- ✓ Results will be categorized by relevance and risk level
- ✓ Review any matches carefully:
- ✓ False Positives: No action needed
- ✓ Potential Matches: Flag for further review or escalate to compliance

Step 6: Save or Export Results

- ✓ Save the report within the Back Office as a PDF - Ensure the report is linked to the account record for audit purposes.
- ✓ Account>KYC>Others>Choose file>
 - New Verification Status: vrfn_verified
 - Expiry: 31 - 12 - 9999
 - Document Id: NAMESCAN
 - Contact: select
- ✓ Make a note on the Back Office - NAMESCAN DONE AGAINST PEP AND SANCTIONS - NO MATCH - CERTIFICATE UPLOADED

Step 7: Update the PEP Tracker

Screenshots of the Namescan Screening Platform



Source

Please select the data source for this scan.

☒ Emerald ☐ Sapphire

> Scan Settings

List Type: All Sanction List: ALL FATF Jurisdiction Risk: On Adverse Media: On (Google, Bing) Match Rate: > 25

Name

Original Script (Non-latin/Roman based languages, such as Cyrillic, Arabic, Hebrew, Chinese, etc...) is acceptable

Please provide either 'First Name and Last Name' or 'Name' in the fields provided

First Name: ROBERT Middle Name: GABRIEL Last Name: MUGABE

Date of Birth: 21/02/1924 Country: Zimbabwe Gender: Male

Example: 24/03/1995 OR 1995

Email Address

☐ Record Due Diligence Decisions

Reference Number

Scan Clear

Program: ZIMBABWE

Identities

3) Robert Mugabe PEP

Name: Robert Mugabe

First Name: Robert

Last Name: Mugabe

Gender: male

Deceased: Yes

Deceased Date: 2019-09-06

Date of Birth: 1924-02-21

Place of Birth: Kutama, Zimbabwe

Update At: 2023-01-16

Reference: Consolidated PEP List

Father: Gabriel Mugabe Matibiri

Mother: Amal Bona Mugabe

Spouse: Grace Mugabe

Children: Bona Mugabe, Michael Nhamodzenyika Mugabe, Chatunga Bellamine Mugabe, Robert Peter Mugabe Jr.

Sibling: Sabina Mugabe

Citizenship: Zimbabwe

Occupations: politician

Other Names

Political Parties

Roles

Other Information

Surewin B.V recognises the increased risk in dealing with PEP's and their associates. In addition, Surewin B.V recognises the prohibition on dealing with sanctioned individuals and companies.

Politically Exposed Person (PEP) are entrusted with prominent public functions or are family members or close associates of such persons. These are people in power and could be susceptible to corruption.

Surewin B.V has a process by which all High-Risk customers are checked and screened against a PEPs/Sanctions database.

PEP and Sanctions checks consists of screening customers against Namescan to determine if they are known fraudsters, drug dealers, terrorists, money launderers or politically exposed persons.

The names of customers that match the names of known fraudsters, drug dealers, terrorists or money launderers are investigated by the Risk department and any accounts that are determined or suspected to be related or owned by a known fraudster, drug dealer, terrorist or money launderers

are escalated to the MLRO for review.

Surewin B.V through the application of risk variables, Surewin B.V will be able to mitigate the risks posed by the threat of being used for money laundering and/or terrorist financing.

Customers should not be able to log in, play, or request any deposits or withdrawals during the time the account is under review.

- **Where a potential PEP match can be discounted** as a false positive, details of the investigation and rationale for discounting must be recorded within the back office on the player profile and recorded on the discounted PEP log.
- The discounted PEP log is reviewed on a monthly basis by the Compliance Officer.
- **Where a potential PEP match cannot be discounted** as a false positive **or where the match is confirmed as positive PEP** must be subject to EDD including SOW.
- Upon receipt of EDD a PEP Assessment must be completed (this is detailed later in this Manual). Only when EDD including SOW and a successful PEP Assessment is completed can the approval of the relationship be considered
You leave the following note on the account:
 - Risk Management review complete. False positive from Namescan. (If all other checks are completed, no other fraud has occurred, and senior management has cleared the customer the account can be reopened).

PEP Risk Assessment

Upon identification of a PEP the level of risk that they pose must be assessed. In order to do so meaningfully the following factors will be taken into account:

- The level of influence that the individual holds;
- The scale of their public profile;
- The level of seniority within their organisation or Government;
- Authority over or access to state funds and assets, policies and operations;
- Control over regulatory approvals, awarding of licences and concessions.

Surewin B.V will complete a PEP Risk Assessment in each instance – the assessment template is included in this manual at Schedule 3. This is completed by the Risk team and sent to the Directors and/or The MLRO for review. All PEP relationships must be approved by the Directors and/or The MLRO.

1.10.1 Ongoing Monitoring of PEP Screening

Should a player who had not been identified as a PEP at on-boarding stage become one, Surewin B.V will implement measures described above within the thirty-day window of observing that the person is a PEP. Failing with these, shall result in Surewin B.V terminating the relationship with this customer.

1.10.2 Sanctions Match

Surewin B.V must ensure it does not transact with any person who is subject to sanctions. Specific actions taken regarding customers identified on sanctions lists:

- A record of customers on sanctions lists identified and reported is kept by the Compliance team.
- Any match will result in the customer's account being immediately frozen and details sent to the MLRO and Directors of Surewin B.V

Surewin B.V must ensure it does not transact with any person who is subject to sanctions. In order to monitor this all customers are screened against current sanctions upon deposit via Namescan and thereafter ongoing screening throughout the duration of the customer relationship against relevant sanctions lists.

1.11 Application of CDD measures to existing customers

Surewin B.V applies ongoing Customer Due Diligence (CDD) measures to existing customers in accordance with AML/CTF regulations. This ensures that customer information remains accurate, relevant, and up to date throughout the relationship lifecycle.

1.11.1 Risk-Based Review

- Customers are categorized by risk level (standard, medium, high), and CDD reviews are conducted accordingly.
- Review frequency:
 - **High-risk:** Annually
 - **Medium-risk:** Every 2–3 years
 - **Standard-risk:** Every 3–5 years

1.11.2. Trigger Events - CDD is reapplied if:

- There is a change in customer information
- Unusual or suspicious transactions occur.
- Regulatory or legal updates apply (e.g., sanctions).

1.11.3. Ongoing Monitoring

Customer activity is monitored continuously by Risk staff and at trigger events to detect deviations from expected behaviour. Any anomalies may prompt enhanced due diligence (EDD).

1.11.4. CDD Measures

For existing customers, the following must be reviewed and updated as needed:

- Identity and verification documents
- Business purpose and transaction patterns
- Source of funds or wealth (where applicable)
- Screening against sanctions and adverse media

1.11.5. Roles and Responsibilities

All customer-facing teams, compliance officers, and operations staff are responsible for ensuring timely CDD updates. Escalation procedures apply for high-risk or non-cooperative customers.

1.11.6. Recordkeeping

CDD documentation will be retained for at ten years.

1.12 The termination of the business

A customer might not be willing to provide Surewin B.V with the necessary information or documentation even though Surewin B.V may have repeatedly solicited him/her to forward said information or documentation. In this case, in addition to keeping a record of all the attempts made, the following needs to be followed:

- a) If the requested information and documentation is not received within **30 days** from the moment the threshold/trigger event was reached. Surewin B.V will terminate its business relationship with the customer, i.e., it is not to allow service to the customer. To this end, Surewin B.V may decide to either close the account or to keep it blocked and suspended in its entirety. In the latter case, we ensure that the account has a NIL balance at the time it is blocked and suspended, with any funds standing to the credit of any such account being disposed of as set out hereunder. If the customer makes the requested information and/or documentation available to Surewin B.V following the closure or the suspension and blocking of the gaming account, Surewin B.V will consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given customer.
- b) Surewin B.V considers whether there are any grounds giving rise to suspicion of ML/FT. The reluctance of the customer to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/FT. Surewin B.V also considers all factors and information it has at its disposal, including for example the payment method used, the played, and the customers playing trends and patterns, any information on the customer already held, including his/her jurisdiction of residence, and information which can be obtained through sources such as the internet etc. If there are grounds to suspect ML/FT, then the team will submit an Unusual Transaction Report (“UTR”) to the FIU. Should there be grounds to suspect ML/FT, then the MLRO is informed promptly, and an UTR is to be filed at the earliest possible even though the thirty days allowed for the collection of the necessary CDD information or documentation may not have lapsed or the customer may not have approached Surewin B.V to carry out any further transactions.
- c) Where there are no grounds to suspect ML/FT or the transaction has not been suspended by the FIU or by operation of the law, nor is there an attachment or freezing order, Surewin B.V would have no reason rooted in the AML/CFT regime justifying the retention of any such funds.

d) Thus, where funds are to be remitted back, Surewin B.V should:

- Consider whether there is any other legal impediment to the remittance of the funds; and
- Remit the funds to the same source through the same channels used to receive the funds.

If Surewin B.V is unable to remit the funds to the same source through the same channels, it will inevitably have to request fresh instructions from the customer. If these instructions give rise to suspicion, this should be raised with the MLRO as a potential UTR and suspend the remittance pending the FIU expressing its opposition or otherwise to the said transaction.

Whenever funds are remitted, it is also, to the extent that this may be possible, indicated in script/instructions accompanying the funds that these are being remitted due to the customers' inability to complete CDD.

1.13 Reliance on third parties to perform customer due diligence

- The third party must be regulated, supervised, or monitored for AML compliance in a jurisdiction with equivalent standards.
- The third party must retain all relevant documents and information for at least 10 years.
- Surewin B.V remains ultimately responsible for the adequacy and accuracy of the CDD performed.
- Surewin B.V will monitor the performance and reliability of the third party.
- Periodic audits or reviews may be conducted to ensure ongoing compliance with CDD requirements.

Recordkeeping and Documentation

- A record of all reliance arrangements must be maintained, including:
 - Identity of the third party
 - Jurisdiction and regulatory status
 - Date and scope of reliance
 - Access logs to CDD documentation

Schedule 3 – PEP Assessment Form

PEP Assessment Form

Notes:

- This form MUST be completed when potential PEP Status is indicated for any customer
- No account activity can be undertaken until a PEP relationship has senior sign off

Date of this assessment/review:	
Name of person under assessment/review:	
Customer ID	

Search findings

Background information leading to the PEP classification:	
PEP status (per the AML/CFT Policy):	PEP PEP (family member) PEP (close associate)
Screening findings (attach copy obtained for this review):	PEP status confirmed / Not confirmed
Sanctions list checks (attach copy of report obtained for this review):	Findings / No Findings
Google (attach copy of search results)	Findings / No findings
Details of any other research or information obtained which indicates or evidences PEP status:	
EDD	Confirm what EDD has been sourced (attach copies)
Proof of identity	
Proof of residential address	
SOW	
Other	
Any betting activity (if a change in status since registration)	
Country of residence	
Any other observations or concerns?	

Director / MLRO Recommendation

PEP relationship approved?	Yes	No
Recommended steps to monitor risk:		
Any further EDD required? If yes, list	Yes	No
Director / MLRO's Name, signature and date		

*Return to customer service team	
----------------------------------	--

Customer Service Team - Action points

Update PEP register Added to PEP register date:	Next review date: *diary for annual review
Confirm ongoing monitoring in place	Yes No
Signed by person preparing form:	Date: