

Anti-money laundering (AML) and Counter terrorist financing
policy

SORT SERVICES N.V.

I. PURPOSE

Sort Services N.V. (the “**Company**”) aims is to ensure that gambling activity is conducted in a fair and open way while making the utmost effort to prevent any use of the platform for fraudulent activities and money laundering. The Company recognizes the need to have in place systems and procedures to combat money laundering, terrorist financing and other criminal activity, to identify criminals and to protect the company, those employed by it and its business reputation.

The purpose of this Policy is to assist you to understand the obligations and responsibilities that arise from the anti-money laundering (“**AML**”) and counter terrorist financing (“**CTF**”) legislation and protect the Company from being the recipient of any proceeds relating to crime. The Company applies a risk-based approach to focus effort where it is most needed and will have the most impact. Our Policy underlines senior management commitment in this area, and the standards expected by employees.

This approach involves a number of steps to assess the most proportionate way to manage and mitigate the ML and TF risks faced by the Company:

- Identifying the ML and TF risks relevant to our operations;
- Designing and implementing policies, procedures, and processes to manage and mitigate the risks;
- Monitoring and improving the effective operation of these controls;
- Recording what has been done, and why.

The Company will take all reasonable measures and precautions to ensure that it is not used as a vehicle for illegal, illicit or criminal activities. The Company recognizes the need to have in place systems and procedures to combat money laundering, terrorist financing and other criminal activity, to deter criminals and to protect the company, those employed by it and its business reputation.

The Company will have a designated Money Laundering Reporting Officer (“**MLRO**”) or equivalent, (and to act in their absence a designated Compliance Officer).

All of the Company's activities must be managed in accordance with this policy, including but not limited to:

- Ensure that the Company does not assist in laundering the proceeds of crime;
- Report any knowledge or suspicion or any reasonable grounds for knowing or suspecting that the company is being used for money laundering or terrorist financing purposes to the MLRO (or Compliance Officer);
- Conduct ongoing monitoring of the relationship with existing clients and of transactions;
- Adherence to all applicable legal and regulatory obligations.

The Company approach to ML and TF is outlined as part of a **four-stage approach** for both our International operations. This includes:

- This **Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) Policy** which outlines at a high level internally our commitment to put in place robust measures to ensure that efforts to launder the proceeds of crime are prevented or, where efforts cannot be prevented, to report incidents in accordance with our legal obligations.
- Our **Risk Assessment**, which is an ongoing process with regard to how the company could be used for ML/TF. Our AML risk assessments provide the basis for designing and upholding processes and procedures to highlight potential risks for attention. The risk assessment takes account of the respective risk assessments made available.
- **AML Operations Guidance** for internal stakeholders, highlighting our AML organisation, legal obligations, suspicious activity reporting protocols, and a summary of the procedures put in place to detect and mitigate ML & TF risks.
- **AML Processes** which describe the practical processes and systems to monitor customer activity for the purpose of identifying concerning or suspicious activity and conducting further investigations.

II. ROLES AND RESPONSIBILITIES

1. Definition

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins.

There are essentially three stages in money laundering:

- **Placement:** the physical disposal of criminal proceeds where the money launderer attempts to place cash into the financial system (including via the use of 'smurfing' methods).
- **Layering:** the separation of criminal proceeds from their source by the creation of "layers" or a sequence of transactions designed to disguise the audit trail and provide the appearance of legitimacy.
- **Integration:** the conversion of the criminal proceeds, for example, into real estate, property or investments, so that they appear to be legitimate funds or assets.

These stages usually occur in sequence, but they may often overlap. It is an offence for a company to fail to establish adequate policies and procedures to identify and prevent money laundering.

2. Suspicion

There is no formal definition of the term "suspects", but guidance from the courts suggests that the individual must think that there is a possibility, which is "more than fanciful", that the relevant facts exist. A vague feeling of unease would not suffice.

There is no requirement for a suspicion to be clear or firmly grounded on specific facts. If you think a transaction is suspicious, you are not expected to know the exact nature of the criminal offence or that particular funds were definitely those arising from the crime. You may have noticed something unusual or unexpected and after making enquiries, the facts do not seem normal or make commercial sense. You do not have to have evidence that money laundering is taking place to have suspicion.

Having "reasonable grounds for knowing or suspecting" (as described above) that a person is engaged in money laundering is measured by assessing whether there are factual circumstances from which an honest and reasonable person, engaged in a business in the regulated sector (such as the Company) should have inferred or formed the suspicion that another was or could be engaged in money

laundering). It is therefore possible to commit an offence if you fail to make a report when you should have known, or suspected money laundering was taking place.

Failing to report knowledge, suspicion or grounds to suspect money laundering to the MLRO (or Compliance Officer) as soon as reasonably practicable after the information came to your attention is a criminal offence.

In case that the company has knowledge, suspicion or any grounds to suspect money laundering in relation to a potential customer, you must still report the knowledge, suspicion or grounds to suspect, even if a decision is made not to allow the customer to open an account.

3. Report a suspicion

As soon as you acquire knowledge, suspicion or grounds to suspect money laundering, you must contact the MLRO (or a Compliance officer), using an appropriate contact method. Speed is of the essence. You should advise the MLRO about what you know, who else you have spoken with, and who else you believe may also have information or knowledge about the matter.

The MLRO (or Compliance Officer) will give you instructions as to what further action to take, if any.

In appropriate cases, you will be asked to complete an internal suspicious activity report ("**SAR**") and send it by email to the MLRO (or Compliance Officer). The MLRO (or Compliance Officer) will maintain all the necessary records.

The MLRO is required to treat all information you provide as confidential.

By reporting your knowledge or suspicion and following the MLRO's (or Compliance Officer's) instructions, you will then have complied with this Policy and, where applicable, your obligations under the law.

Under no circumstance should you discuss the matter with anyone else unless specifically authorised to do so.

"Suspicious activity" is where there are circumstances that suggest that a person might be acting or behaving in an unusual manner. It can include any activity that seems odd or unusual to you or does not fit with the normal course of business (sometimes referred to as a "red flag"). Examples of red flags can include (but are not limited to) the following:

- where a potential customer is reluctant to provide supporting evidence to allow us to verify their identity and/or provide information on the entity we are potentially doing business with;
- where a potential customer presents unusual, inconsistent or suspicious identification documentation;
- where a customer or potential customer is reluctant to provide information in relation to the source of their wealth and/or funds;
- where a customer uses multiple debit cards to deposit money within a short period of time, also known as 'tumbling', especially when there are multiple rejected deposits attempt
- where a customer deposits a sum of money and makes a request to withdraw it having engaged in minimal or no gameplay;
- where a customer is situated in a higher-risk jurisdiction or is identified as being listed on the international sanctions list (subject to the special procedure for U.S. sanctions described below);
- where a customer is associated or linked with other customer accounts in any way (including active, dormant or suspended/terminated accounts)
- where a customer attempts to opens several accounts using either variations of their own or different names;
- where a customer's registered location and active IP address does not match;
- where the registered payment method details do not match the player's registered details;
- where there is a mismatch between the customer's country of residence and the location of their method of payment;
- where the customer logs into their account from multiple countries or attempts to circumvent geo-location controls to access the Company account from a prohibited jurisdiction;
- where a customer uses one payment method to make a deposit and requests a withdrawal to be made to a different account;
- where a customer deposits amounts which are just below reporting or recordkeeping limits (e.g., 2,000 Euro), or the Company's maximum transaction limits;

- where a customer attempts to hide the size of a large transaction by breaking it into multiple, smaller transactions;
- where a customer engages in unusual or inconsistent gameplay or financial activity;

The existence of a "red flag" leading to a suspicion that money laundering is taking place does not necessarily mean that money laundering is in fact taking place. It simply means that greater scrutiny is required to understand what is happening. If you are in any doubt as to whether a red flag exists, contact the MLRO (or Compliance Officer) in the way set out above.

III. CUSTOMER DUE DILIGENCE & ONGOING MONITORING

1. Verification

Checking our customers' identity and understanding where their funds come from as and are sent to. For customers utilising our services from Great Britain we have systems in place to meet requirements to verify the identity, address, and date of birth of customers in our regulated online gambling business prior to engaging in any gambling activity. Customer's identity is verified further where required by EU Money Laundering Regulations at certain thresholds to satisfactorily reduce the potential specific risk posed by non-face-to-face business. In order to complete CDD, the identity of customers must be verified on the basis of additional documents, data or information obtained from a reliable and independent source. Where considered necessary, the Company will use a commercial electronic data provider to verify these details for players.

Verification of customer identity involves verifying the customer information based on documents or information (i.e. from 3rd party verification services) obtained from a reliable and independent source. Our Know Your Customer teams are responsible for this process.

Our international business seeks to establish customer identity on a risk-based approach in line with monitoring processes and regulatory guidance.

Ongoing monitoring involves our AML teams reviewing customer activity against prevailing procedures. This includes, for example, proactive risk-based customer spend threshold reviews, reviews following internal suspicious activity reports, and reactively investigating adverse media or law enforcement alerts. Further enhanced due diligence, including source of funds and wealth, is considered as appropriate in this framework, including ones in respect of PEPs. The frequency of ongoing customer review is determined

by the framework and on a risk-based approach and managed through relevant case management systems.

For those customers, rated as high risk either initially or later in the business relationship, the company will need to conduct mandatory enhanced customer due diligence. This means employing additional measures, including approval from senior management for the business relationship, and conducting enhanced ongoing monitoring.

Our Risk Operations function maintain rule sets to prevent and/or flag potential account risks in respect of geo-location, payment methods, and multiple accounts.

The verification process is part of the Know Your Customer (KYC) procedure. We need to complete the verification before the customer commences gambling. The verification process is completed on registration. The customers are informed of the verification procedures when they first register so that there is no misunderstanding at a later stage. All customers receive an email informing them about the stages of the verification process.

Identification process: name, address and date of birth of the client. The full verification requires a match on two separate data sources, which includes 2 matches on name, date of birth and address. The current GBG responses of the ID3 checks are: (i) Pass - Fully Verified; (ii) Fail; (iii) Refer - DOB fail, address verified; (iv) Refer - DOB pass, address fail. If the customer does not pass the ID3 check, a pop-up message with an explanation is presented to the customer (along with an email).

For any status different from Fully Verified, an ID and POA is being requested, in order to verify the customer with documents. The player is not allowed to deposit but can log in and upload the needed documents: ID & POA. The system blocks the bonuses in order to avoid giving any welcome bonus for not verified players.

- If verified by GBG, we request documents again at first deposit – pop-up and mail, reminder popup after login, withdrawal, total deposits exceed EUR 2 000.

2. Customer Due diligence (CDD)

The Company must apply CDD measures if they:

- establish a business;
- suspect money laundering or terrorist financing;

- doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification;
- carry out an occasional transaction that amounts to a transfer of funds which is more than EUR 1 000.

Regardless of whether they have established a business relationship with the customer, suspect money laundering or terrorist financing, or doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification, casino operators must also apply CDD measures in relation to any transaction that amounts to EUR 2 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

The best protection against abuse by money launderers is to know your customer – this is done through Customer Due Diligence (CDD). CDD refers to all processes and controls applied to ensure that at all stages of the business relationship we have a clear understanding of who the customer is and his behavioural pattern.

The main aim of CDD is to make sure that we have effective mechanisms in place in order to: (i) Identify a customer; (ii) Verify customer's identity; (iii) Establish the purpose and intended nature of the business relationship along with the customer's business and risk profile, and; (iv) Monitor customer's activity on an on-going basis to reduce fraudulent and ML/TF activity during the life cycle of a customer - based on internally developed triggers and constant monitoring by the appointed AML office.

For customers utilizing our services from Great Britain we have systems in place to meet requirements to verify the identity, address, and date of birth of customers in our regulated online gambling business prior to any gambling activity. Customer's identity is verified further where required by EU Money Laundering Regulations at certain thresholds to satisfactorily reduce the potential specific risk posed by non-face-to-face business. Verification of customer identity involves verifying the customer information against documents or information (i.e. from 3rd party verification services) obtained from a reliable and independent source. Our Know Your Customer teams are responsible for this process. Our EU retail business seeks to establish customer identity on a risk-based approach in line with monitoring processes and regulatory guidance.

CDD report

Name		
Aliases		
OSN	-	
Date of birth		
Nationality	British	
Current address		
ID number		
Education		

Type of asset	Estimated value	Remarks	Adverse media
Salary	Not available	No professional occupation identified.	Not available
Estimated Total Worth			

Source of Wealth

Player was not found across the social media websites. No matches also found in LinkedIn, Beta Companies House and Insolvency Register. No professional occupation identified. As per Zoopla, [player's](#) estimated house value is GBP 220K which is lower than the average for the area, GBP 366,203.

Business Interests

Name of Business	Type of Interest
Not available	Not available

Personal and Professional Associations

Name of Associate	Type of Association
Not available	Not available

Potential Red Flags

No issues found at this stage. No need of [SOF](#) for now. Player's activity will be monitored in case it continues to grow

Sources

URL

3. Ongoing monitoring

Ongoing monitoring involves our AML teams reviewing customer's activity against prevailing procedures. This includes, for example, proactive risk-based customer's spent threshold reviews, reviews following internal suspicious activity reports, and reactively investigating adverse media or law enforcement alerts. Further enhanced due diligence, including source of funds and wealth are considered as appropriate in this framework, including ones in respect of PEPs. The frequency of ongoing customer review is determined by the framework and risk-based approach and managed through relevant case management systems.

Our Risk Operations function maintain rule sets to prevent and/or flag potential account risks in respect of geolocation, payment methods, and multiple accounts. The Company has a continuing duty to conduct ongoing monitoring of all customer relationships and to be vigilant with regard to money laundering and terrorist financing at all times and to report any suspicious transactions or circumstances.

The Company will monitor all customer transactions and activity in accordance with industry best practice, international recommendations and guidelines (IMF, FATF MoneyVal) including but not limited to:

- Player identity; player due diligence and identification data;
- Player financial habits and behaviors, to ensure that the transactions are consistent with the licensee's knowledge of the player's risk profile;
- Player gaming habits and behaviors to ensure that the transactions are consistent with the Company's knowledge of the player's risk profile;
- Individual or linked transactions which are complex or unusually large with no apparent economic or lawful purpose;
- Unusual patterns of transactions with no apparent economic or lawful purpose;
- Transactions which exceed certain limits with no apparent economic or lawful purpose;
- Very high account turnover inconsistent with the balance;
- Transactions or behaviours which are outside of the player's regular activity pattern;
- Any other pattern of transactions or other customer activity identified as a red flag under the "Suspicious Activity" sections of this policy.

4. Customer risk

Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. Categories of customers whose activities may indicate a higher risk include:

- customers who are PEPs;
- high spenders – the level of spending which will be considered to be high for an individual customer will vary among casino operators, and among casinos managed by the same operator;
- disproportionate spenders – we should obtain information about customers' financial resources so that they can determine whether customers' spending is proportionate to their income or wealth;
- casual customers – this includes tourists, participants in junkets and local customers who are infrequent visitors;
- regular customers with changing or unusual spending patterns;

- improper use of third parties – criminals may use third parties or agents to avoid CDD undertaken at the threshold or to buy chips, or they may be used to gamble so as to break up large amounts of cash;
- junkets – junkets can pose several higher risks, including criminal control of the junket operator or participants, the movement of funds across borders which obscures the source and ownership of the money gambled by participants and their identities, and structuring, refining and currency exchange risks;
- multiple player accounts – some customers will open multiple player accounts under different names to hide their spending levels or to avoid breaching the CDD threshold;
- unknown or anonymous customers – these customers may purchase large amounts of chips with cash at casino tables, and then redeem the chips for large denomination notes after minimal or no play;

5. Transaction risk (including means of payment)

We have the following potential transaction risks:

- proceeds of crime – there is a risk that the money used by a customer has been gained through criminal activity, so greater monitoring of high spenders will help to mitigate the risk
- transfers between customers – customers may transfer money between themselves or may borrow money from unconventional sources, including other customers, which can offer criminals an opportunity to introduce criminal proceeds into the legitimate financial system through the casino
- use of casino deposit accounts – criminals may use accounts to deposit criminal proceeds and then withdraw funds with little or no play
- redemption of chips, tickets or tokens for cash or cheque, particularly after minimal or no play
- particularly in remote casinos:
- multiple gambling accounts or wallets – customers may open multiple accounts or wallets with an operator in order to obscure their spending levels or to avoid CDD threshold checks

- changes to bank accounts – customers may hold a number of bank accounts and regularly change the bank account they use for the remote casino operator
- identity fraud – details of bank accounts may be stolen and used on remote gambling websites, or stolen identities may be used to open bank accounts or remote gambling accounts
- pre-paid cards – these cards pose the same risks as cash, as remote casino operators normally cannot perform the same level of checks on the cards as they can on bank accounts
- e-wallets – some e-wallets accept cash on deposit or cryptocurrencies, which pose a higher risk, and some customers may use e-wallets to disguise their gambling
- games involving multiple operators – for example, poker games often take place on platforms shared by a number of remote gambling operators, which can facilitate money laundering by customers, such as chip dumping.

6. Product risk

Product risk includes the consideration of the vulnerabilities associated with the particular products offered by the casino operator. Products which may pose a money laundering risk include:

- peer to peer gaming
- gaming where two or more persons place opposite, equivalent stakes on even, or close to even, stakes (for example, the same stake on red and on black in a game of roulette, including electronic roulette)
- gaming machines, which can be used to launder stained or fraudulent bank notes.

Deciding that a customer presents a higher risk of money laundering or terrorist financing does not automatically mean that the person is a criminal, money launderer or financier of terrorism. Similarly, identifying a customer as presenting a low risk of money laundering or terrorist financing does not mean that the customer is definitely not laundering money or engaging in criminal spend. We therefore need to remain vigilant and use our experience and common sense in applying the Company's risk-based criteria and rules, seeking guidance from our nominated officer as appropriate.

7. AML automated triggers

(i) more than 5 transactions of at least 20 EUR within 72 hours ; **(ii)** Deposit of EUR 1000 using a pre-paid card within 24 hours; **(iii)** Deposit of EUR 1500 using a pre-paid card within 72 hours; **(iv)** A deposit amount

of at least EUR 1500 is reached and the withdrawal/deposit ratio within 7 days is 70% (Withdrawal ratio calculated – total approved, paid & pending withdrawals/total approved deposits);

Logic: if 2 triggers are being hit within 30 days or less, the AML risk is being automatically set to medium; if 3 or more triggers are being hit for the same time period, the AML risk level is being automatically set to high.

IV. Enhanced customer due diligence measures (EDD)

1. Enhanced customer due diligence measures (EDD)

Where the risk associated with a business relationship is increased, we must apply enhanced customer due diligence measures (EDD) to manage and mitigate those high risks appropriately (e.g., where transactions are complex, unusually large or conducted in an unusual pattern). We apply enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks, especially in the following cases:

- in any case identified by the operator or in information provided by the Commission to the operator where there is a high risk of money laundering or terrorist financing;
- in any business relationship with a customer situated in a high-risk country identified by the European Commission or in relation to any transaction for which the operator is required to apply CDD measures, where either of the parties to the transaction is resident in a high-risk country;
- if the operator has determined that a customer or potential customer is a PEP, a family member or a known close associate of a PEP;
- in any case where the operator discovers that a customer has provided false or stolen identification documentation or information and the operator proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose;
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

In the case of business relationships with customers situated in high-risk countries or transactions where either of the parties to the transaction are resident in a high-risk country, the enhanced measures undertaken includes:

- obtaining additional information on the customer and on the customer's beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
- obtaining information on the reasons for the transactions;
- obtaining approval of senior management for establishing or continuing the business relationship;
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

Examining the background and purpose of the transaction is one of the measures that we, as a responsible gaming operator, should take. We also must increase the degree and nature of monitoring of the business relationship in which the transaction is made and to determine whether the transaction or the relationship appear to be suspicious. Depending on the requirements of the case we should:

- seek additional independent, reliable sources to verify information provided to us;
- take additional measures to better understand the ownership and financial situation of the customer;
- increase the monitoring of the business relationship, including greater scrutiny of the transactions.

When assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate the risk, we must take into account following risk factors:

- the business relationship is conducted in unusual circumstances ;
- the customer is resident in a geographical area of high risk ;
- the product or transaction might favour anonymity ;

- the situation involves non-face-to-face business relationships or transactions (as in the case of remote casinos), without certain safeguards such as electronic signatures ;
- payments will be received from unknown or unassociated third parties of the customer ;
- new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies (such as virtual currencies) for both existing and new products .

the business relationship or transaction involves countries:

- identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing
- identified by credible sources as having significant levels of corruption or other criminal activity, such as money laundering, terrorism, and the production and supply of illicit drugs
- subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations
- providing funding or support for terrorism
- that have organisations operating within their territory which have been designated, , as proscribed organisations under the Terrorist Act or, by other countries,international organisations or the European Union as terrorist organisations
- identified by credible sources (such as evaluations, detailed assessment reports or follow-up reports published by FATF, the International Monetary Fund, the World Bank, the organisation for Economic Cooperation and Development or other international bodies or non-governmental organisations) as not implementing requirements to counter money laundering and terrorist financing that are consistent with the FATF recommendations.

How should we assess whether there is a high risk of money laundering or terrorist financing? If:

- the customer transacts with significant amounts of cash
- the customer provides false, forged or stolen identification documentation upon establishing a business relationship

- the customer transacts with multiple remote gambling operators, particularly where this occurs across multiple geographical areas
- the product, service or transaction involves peer-to-peer gaming
- the product is electronic roulette/live games
- the product, service or transaction involves Ticket In/Ticket Out (TITO) or similar technology.

In any case where a customer indicates one of the risks listed above, a detailed check of the customer's relationship should be made (including double checking the following processes: identification, verification, data research, social media research and requesting financial evidence of source of funds) and a future monitoring of their transactions should be appointed.

2. Adverse Information Checks - PEPs, Sanctions & Terrorism

Searches will be made against politically exposed person ("PEP"), sanctions and enforcement lists during the course of CDD and whenever EDD (defined below) is triggered. In so doing, the Company will identify those customers who present a higher risk, which will include, without limitation, those:

- Who are identified as a PEP;
- Who are subject to sanctions;
- Who reside in, or are citizens of, high-risk countries (being those that are on the list of Financial Action Task Force high risk and non-cooperative jurisdictions; countries that are subject to EU, and UN financial sanctions;

Formal searches to identify whether customers are subject to sanctions, are Politically Exposed Persons, or linked to terrorism. Company's active customer base is frequently screened using third party software in line with the EU requirements. The software compares the registered details of our customers against lists of PEPs, their relatives or close associates, sanctioned individuals and lists of known criminals. Identified Politically Exposed Persons lead to further risk assessment and an appropriate level of due diligence based on that assessment; ongoing relationships require Group MLRO approval. The MLRO retains a record of identified PEP customers, and ongoing monitoring is managed through prevailing case management systems.

Governance processes operate across the Group, and in the EU, for example, includes MLRO sign off of decision making in respect of next steps for perceived potential higher risk customers.

V. RECORD KEEPING

For the purpose of performing our AML & CTF obligations, Company preserves documents and information as required by prevailing legislation and local requirements. This comprises, for example, customer due diligence, ongoing monitoring and governance records as detailed above, including the reasons for decisions and actions taken from an AML and CTF perspective. Employee training records and internal periodic/annual reports are also retained in addition to records pertaining to internal and external suspicious activity reports. All documents, data and information collected to identify the client and to verify identity are retained for at least 7 years from the date on which the business relationship ends. Records must be maintained that are sufficient to allow a competent third party to assess the effectiveness of AML/CTF policies and procedures, including transaction records, due diligence information, suspicious transaction reports and AML/CTF training records.

All employees, regardless of seniority, are required to undertake AML e-learning which includes a short assessment. This is refreshed on an annual basis, and includes background information on money laundering, potential offences, the role of colleagues in detecting potential risk triggers and escalating their detection, alongside case studies.

AML teams are trained by existing analysts at induction, and all AML colleagues are required to be familiar with our AML policies. Face-to-face training is also conducted by AML managers with our AML analyst and customer management teams.

AML colleagues are further provided with relevant face-to-face 3rd party training where available and relevant. This includes, for example, our AML analysts covering our international operations and undertaking a special AML certificate in betting and gaming. Senior AML Managers attend and participate in industry and regulatory workshops to keep their knowledge up to date.