

JX Group B.V.
B2B Gambling Provider

Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy

Contents

1.	Introduction.....	4
2.	Policy Statement	4
3.	Audience	5
4.	Definitions	5
5.	Policy Implementation	7
5.1.	Business Risk Assessment (BRA)	7
5.2.	Customer Risk Assessment (CRA).....	8
5.3.	Customer Acceptance Policy (CAP)	8
5.4.	Customer Due Diligence	9
5.4.1.	Standard CDD Requirements	9
5.4.2.	Verification and Screening Measures	9
5.4.3.	Failure to Complete CDD	10
5.5.	Ongoing Monitoring.....	10
5.5.1.	Document and Information Review	10
5.5.2.	Event-Based Updates	10
5.5.3.	Monitoring Responsibilities	10
5.6.	Reliance on Third Parties to perform Customer Due Diligence	11
5.7.	Reporting of Unusual Transactions	11
5.7.1.	Identification of Unusual Activity and Escalation	11
5.7.2.	Documentation and Recordkeeping	11
5.8.	Money Laundering Compliance Program.....	11
5.8.1.	Key Components.....	11
5.8.2.	Actions on Suspicion.....	12
5.8.3.	Review and Updates.....	12
6.	Compliance and Consequences of Non-Compliance	12
6.1.	Compliance Expectations.....	12
6.2.	Non-Compliance Consequences.....	12
6.3.	Oversight	12
7.	Related Information	12
7.1.	Legal and Regulatory References	13
7.2.	Internal Documents	13
7.3.	External Tools.....	13
8.	Contact Information.....	13
9.	Policy History	13
	<i>Annex I – General Business Risk Assessment Framework.....</i>	<i>14</i>

Purpose of the BRA	14
Key Elements of the BRA Framework.....	14

1. Introduction

JX Group B.V. (herein after referred as “**Company**”) is a gambling provider operating under the Curaçao law, specializing in the development of and distribution of iGaming content such as slot, online casino and crash games, and other certified gambling software. These products are integrated into licensed operator platforms, which are ultimately responsible for offering gaming services to end-users.

Although JX Group B.V. does not directly handle player accounts or process gambling transactions, it plays a significant role in the digital gambling ecosystem. As such, the Company recognizes its responsibility to support anti-money laundering (AML), counter-terrorist financing (CTF), and counter-proliferation financing (CPF) efforts by ensuring that its systems, services, and business relationships are not misused for illicit purposes.

This Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy (hereinafter referred as “**AML/CTF Policy**” or “**Policy**”) is designed to outline JX Group B.V.’s internal compliance framework in accordance with:

- The National Ordinance on the Identification when Rendering Services (**NOIS**);
- The National Ordinance on the Reporting of Unusual Transactions (**NORUT**);
- The Sanctions National Ordinance and the Kingdom Sanctions Act;
- The regulatory expectations and guidance provided by the Curaçao Gaming Control Board (**GCB**), effective from January 2025.

In addition, this Policy is informed by industry best practices and incorporates JX Group B.V.’s established **Customer Due Diligence (CDD)** standards as used during the onboarding of licensed operators and partners.

2. Policy Statement

The Company is fully committed to complying with all applicable AML/CTF/CPF laws, regulations, and international standards. The Company adopts a **risk-based approach** to prevent its services and business relationships from being exploited for money laundering, terrorist financing, or other financial crimes.

This policy applies to:

- All internal departments of JX Group B.V.;
- All employees, including management and compliance personnel;
- Any third parties or agents acting on behalf of the Company in onboarding or monitoring commercial partners.

By implementing this policy, JX Group B.V affirms its commitment to:

- Conducting thorough risk assessments of business partners;
- Performing appropriate due diligence prior to onboarding new clients or affiliates;
- Monitoring the AML-related documentation submitted by its clients and affiliates, and ensuring that such documentation is reviewed and re-screened every 3-6 months;
- Monitoring the AML-related documentation submitted by its clients and affiliates, and ensuring that such documentation is reviewed and re-screened every six (6) months
- Ensuring regular screening against international sanctions and PEP lists;
- Monitoring for unusual commercial behavior that may indicate illicit activity;
- Maintaining accurate records and cooperating with regulatory authorities.

This policy shall be reviewed at least annually, or upon any material change in regulatory requirements or the business model. It serves as a guiding framework to protect the integrity of the Company and support global efforts in combating financial crime. Also, regular audits and reviews are conducted to assess the effectiveness of the Policy and identify areas for improvement.

3. Audience

This Policy applies to all individuals and entities who are involved in the execution, oversight, or support Company's business operations and compliance responsibilities. Specifically, this includes:

- all employees, regardless of their position, department, or level of seniority, including management and administrative staff;
- subsidiaries, agents, consultants and representatives acting on behalf of the Company in any business or regulatory capacity;
- third-party service providers, contractors, or partners engaged in customer due diligence (CDD), compliance support, risk assessment, or onboarding of operator clients;
- any other person or entities who, by virtue of their function, have access to sensitive client, financial, or compliance-related information.

All individuals and organizations within the scope of this Policy are expected to understand and adhere to the principles and requirements set out herein and to actively support Company's commitment to AML/CFT compliance.

4. Definitions

For the purposes of this internal AML/CFT Policy, the terms below are defined in accordance with the Company's operational context as B2B gambling provider under Curaçao law. These definitions are intended to ensure clarity and consistency in the application of this Policy by employees, departments, relevant third parties.

While aligned with the core principles of Curaçao's AML/CFT legal framework - such as the National Ordinance on the Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the CGA AML Guidelines (January 2025) – the definitions provided herein are specifically tailored for internal use and practical implementation by the Company.

Term	Abbreviation	Definition
Anti-Money Laundering	AML	A set of laws, regulations, and procedures intended to prevent criminals from disguising illegally obtained funds as legitimate income.
Counter-Terrorist Financing	CTF	Measures aimed at preventing the financing of terrorism or terrorist activities. Often regulated together with AML.
Counter-Proliferation Financing	CPF	Measures to prevent the financing of the development, acquisition, or proliferation of weapons of mass destruction.
Gambling Provider		A company that develops and supplies iGaming content (e.g., slot games, crash games, live casino software) to both licensed operator platforms and B2B intermediaries such as

		aggregators. JX Group B.V. operates in this capacity.
Operator/Client		A business entity, such as a licensed online casino (B2C) or gaming platform provider (B2B), that integrates JX Group B.V.'s games via API or similar systems.
Operator Client		refers collectively to both B2C license holders (such as online casinos) and B2B platforms or aggregators that integrate JX Group B.V. content.
Customer Due Diligence	CDD	The process of identifying, verifying, and assessing the risk level of Clients before onboarding and periodically thereafter. See Section 5.4.
Enhanced Due Diligence	EDD	Additional CDD measures applied in high-risk situations, including more detailed verification of ownership, source of funds, and risk factors.
Politically Exposed Person	PEP	An individual who currently holds or has previously held a prominent public function, along with their close associates and immediate family. PEPs are subject to enhanced screening.
Sanctioned Entity		Any person or organization appearing on sanctions lists issued by the UN, EU, OFAC, or Curaçao authorities. All clients are screened for sanctions risk.
Ultimate Beneficial Owner	UBO	A natural person who ultimately owns or controls more than 25% of a legal entity or otherwise exercises effective control.
Unusual Transaction	UTR	Any activity that deviates from the expected commercial behavior of a client, or raises suspicion of financial crime. JX Group B.V. monitors for such behavior in its partnerships.
Business Risk Assessment	BRA	An internal review of risks to the business related to money laundering, terrorism financing, or sanctions exposure. Updated at least annually.

Customer Risk Assessment	CRA	The evaluation of ML/TF risks specific to an individual client based on jurisdiction, structure, ownership, product use, and payment behavior.
National Ordinance on the Identification when Rendering Services	NOIS	Curaçao legislation requiring service providers to identify clients and verify their identity prior to providing services.
National Ordinance on the Reporting of Unusual Transactions	NORUT	Curaçao legislation requiring entities to report any suspicious or unusual transactions to the Financial Intelligence Unit (FIU).
Curaçao Gaming Control Board	GCB	The supervisory authority for AML/CFT compliance in the Curaçao gaming sector, including gambling providers and licensed operators.

5. Policy Implementation

This section outlines how JX Group B.V.'s Anti-Money Laundering and Counter-Terrorist Financing Policy is operationalized throughout the organization. It defines key responsibilities, explains core compliance procedures, and establishes the practical framework through which AML/CFT controls are embedded into the Company's day-to-day activities.

Where internal procedures are documented separately (e.g., internal onboarding manuals, risk classification guides, or CDD checklists), the Compliance Department shall be responsible for oversight, updates, and training to ensure full alignment with this Policy.

5.1. Business Risk Assessment (BRA)

JX Group B.V. conducts a comprehensive BRA at least annually, or more frequently if there are material changes to its products, services, markets, or client profile. The BRA is cornerstone of the Company's risk-based approach and it designates to identify, assess, and mitigate the specific risks related to money laundering, terrorist financing, and sanctions exposure within its operational environment.

The BRA evaluates among other factors:

- **The types of operator** clients with whom the Company established commercial relationships, including their business model and jurisdictional presence;
- **Jurisdictional risk exposure**, with particular attention to countries or regions identified as high-risk by the Financial Action Task Force (FATF) or subject to international sanctions;
- **Payment and integration methods**, including the use of alternative payment channels, digital wallets, and any cryptocurrency-related interfaces;
- **The quality and strength of regulatory oversight** in the client's licensing jurisdiction, including whether the client is regulated under a recognized AML/CFT regime.

Finding from the BRA directly inform JX Group B.V.'s client onboarding standards, risk classification system, due diligence measures, and ongoing monitoring procedures. All assessments are documented, approved by senior management and retained in accordance with the Company's record-keeping obligations. For a full overview of the Company's BRA structure and anticipated risk controls, please refer to Annex I – General Business Risk Assessment Framework.

5.2. Customer Risk Assessment (CRA)

The Company performs a Customer Risk-Assessment (CRA) prior to establishing a business relationship with new operator client. The CRA is designed to evaluate the specific risk exposure associated with the potential client, taking into consideration their structure, jurisdiction, business model and overall compliance posture.

This process supports the creation of documented risk profile for each customer, which informs the level of due diligence applied (standard or enhanced) and the ongoing monitoring requirements.

The CRA is conducted by the Compliance Department using information collected during the initial CDD process (see Section 5.4.) and internal KYC framework, which includes the Company's standard onboarding package.

Key risk indicators assessed during the CRA include:

- **Jurisdictional Risk:** Evaluation of the client's country of incorporation, licensing jurisdiction, and geographic reach. Countries considered high-risk by the FATF or subject to international sanctions increase the overall risk score.
- **Ownership and Control Structure:** Complexity of the group structure, transparency of the beneficial ownership chain, and presence of nominee or corporate shareholders.
- **PEP and Sanctions Exposure:** Identification of any directors, shareholders, or signatories who are Politically Exposed Persons (PEPs) or appear on global sanctions lists.
- **Regulatory Standing and Licensing Quality:** Verification of gaming licenses held, the scope of authority, and regulatory credibility of the licensing body.
- **Business Model and Client Type:** The nature of the gaming services offered by the operator (e.g., crypto-only casinos, unlicensed gaming platforms, affiliate-heavy business models) and their alignment with international AML standards.
- **Financial Behavior and Integration Model:** Proposed payment methods, frequency of transactions, and technical integration (e.g., API connection, revenue share setup, cryptocurrency support).

The outcome of the CRA is the assignment of a **risk rating** (Low, Medium, or High) to each customer. This risk rating determines the level of ongoing monitoring (see Section 5.5) and whether **Enhanced Due Diligence (EDD)** measures are required (see Section 5.6).

The CRA must be reviewed and, if necessary, updated:

- **Every 6 months** for high-risk clients;
- **Annually** for medium- and low-risk clients; or
- **Immediately** in case of significant changes in company structure, beneficial ownership, jurisdiction, or regulatory status.

All CRAs are documented, signed off by the Compliance Officer, and retained in accordance with the Company's record-keeping obligations.

5.3. Customer Acceptance Policy (CAP)

Based on the outcomes of the CRA, the Company determines whether a potential client may be accepted as a business partner and which level of due diligence measures be applied. This is done in accordance with the Company's Customer Acceptance Policy (CAP), which ensures that only clients who meet minimum risk, transparency and compliance standards and onboarded.

The CAP includes the following key principles:

- Clients may only be accepted upon successful completion of a documented CRA and a full Customer Due Diligence (CDD) process, as outlined in Section 5.4.;
- Clients operating in or associated with FATF designated high-risk jurisdictions, or under international sanctions, are subject to automatic rejection or must undergo Enhanced Due Diligence (EDD);
- All clients must be screened for Politically Exposed Person (PEP) status and sanctions exposure using reputable screening databases prior to onboarding;
- No business relationship shall commence until the client has submitted complete and verifiable CDD documentation, including corporate registration, licensing, ownership structure and individual identification for UBOs and authorized signatories;
- If the client's structure includes nominee shareholders, bearer shares, or complex layering, additional verification measures must be applied and reviewed by the Compliance Officer.

Only clients who are classified as acceptable within the CRA and meet the CAP thresholds are approved for integration and contractual engagement. Exceptions to the policy may only be granted by senior management in consultation with the Compliance Department and must be justified in writing.

5.4. Customer Due Diligence

Customer Due Diligence (CDD) is a core control mechanism within the Company's AML/CFT framework and is applied to all operator clients prior to the establishment of a business relationship. The depth of the CDD process is determined by the risk assigned during the Customer Risk Assessment (CRA), in accordance with the Customer Acceptance Policy (CAP).

5.4.1. Standard CDD Requirements

As part of the standard onboarding, the Company requires all prospective operator clients to submit the following documentation and information, as reflected in the Company's CDD form:

- Certificate of Incorporation / Business Registration (for all legal entities in the ownership chain);
- Memorandum and Articles of Association;
- Director and Shareholder Registers;
- Group Shareholding Structure up to the Ultimate Beneficial Owner (UBO);
- Valid gaming licenses, including license numbers, jurisdiction(s), and scope of coverage;
- List of countries where the client is authorized to operate and/or targets its services;
- Identification documents (certified passport copies) and proof of address for all directors, UBOs (25%+ ownership), and account signatories;
- Disclosure of any PEPs or sanctions exposure, or ongoing or past legal proceedings.

All submitted documents must be:

- in English, or translated and certified by the authorized person;
- Certified as true copies, including the certifier's name, title, signature and contact details;
- No older than six (6) months for utility bills that is also used as proof of address.

5.4.2. Verification and Screening Measures

All clients and their associated individuals are subject to the following screening procedures:

- PEP screening using public databases, risk intelligence platforms and government watchlists;
- Sanctions screening against the UN sanctions lists, EU Sanctions Map, OFAC lists, and relevant local sources;
- Internal cross-checking against previous onboarding attempts or internal flags.

No business relationship may proceed if a match is found on sanctions lists unless explicitly cleared by the Compliance Officer and legal counsel. If a PEP is identified, Enhanced Due Diligence (see Section 5.6) is triggered.

5.4.3. Failure to Complete CDD

In line with AML requirements, the Company undertakes to:

- **Reject** any prospective client that fails to provide satisfactory documentation;
- **Suspend or terminate** a business relationship if updated CDD cannot be obtained during scheduled reviews;
- Document all interactions and retain them as evidence of due diligence and regulatory compliance.

If suspicions of money laundering, terrorism financing, or sanctions violations arise during the CDD process, the Compliance Officer will assess whether the client should be blocked and if a report to the **FIU Curaçao** is warranted (see Section 5.7).

5.5. Ongoing Monitoring

The Company applies an ongoing monitoring process to ensure that the information and documents provided by its clients remain current, accurate, and complete throughout the business relationship. This is an essential part of maintaining effective AML compliance and reflects the procedures set out here/

5.5.1. Document and Information Review

As part of the internal monitoring schedule:

- Clients are required to resubmit key CDD documents every six (6) months, including corporate registration, licenses and identification documents of directors and beneficial owners.
- Any changes in ownership, company structure, or licensing must be communicated by the client and reviewed by the Compliance Department.

The Compliance Department reviews:

- Validity of submitted documents (e.g., expired passports or licenses);
- Updated PEP and sanctions status through regular re-screening;
- Any changes to the client's risk profile.

5.5.2. Event-Based Updates

In addition to scheduled reviews, monitoring is also triggered when:

- There is a change in the client's legal structure or ownership;
- A new director, shareholder, or authorized signatory is appointed;
- A licensing update or jurisdiction expansion is detected;
- Irregularities or red flags are observed by internal teams (e.g., during communication or integration).

5.5.3. Monitoring Responsibilities

The Compliance Department is responsible for:

- Requesting and reviewing updated documentation;
- Keeping internal CDD records up to date;
- Adjusting the client's risk rating if new information warrants reclassification.

All actions related to ongoing monitoring are recorded and stored in accordance with the Company's recordkeeping obligations.

5.6. Reliance on Third Parties to perform Customer Due Diligence

The Company may rely on third-party sources to support the collection or verification of certain CDD information during the onboarding of clients. However, such reliance is limited to specific aspects of the process and does not transfer responsibility for risk assessment or final approval.

Third Parties may include:

- External service providers or platforms that supply public corporate records or screen for PEP/sanctions;
- Professional advisors (e.g. legal or compliance consultants) assisting in document preparation or translation.

The Compliance Department remains fully responsible for assessing the accuracy of the information received, conducting the Customer Risk Assessment and making final onboarding decision. The use of third parties does not diminish the Company's accountability under Curaçao AML/CFT regulations.

5.7. Reporting of Unusual Transactions

While the Company does not engage in direct transactions with individual players, it remains alert to any unusual or suspicious activity involving its operator clients. In accordance with the Curaçao AML framework, the Company has internal procedures to identify, document, and escalate such cases.

5.7.1. Identification of Unusual Activity and Escalation

Unusual activity may include:

- Refusal to submit CDD documents;
- Sudden changes in company ownership or structure;
- Clients linked to high-risk jurisdictions or negative media;
- Technical integration requests inconsistent with standard practice.

If unusual behavior is observed, it must be reported internally to the Compliance Officer, who will:

- Review and assess the case;
- Decide whether it should be escalated to the Financial Intelligence Unit (FIU Curaçao);
- Document the outcome and keep a record of the report.

The Company strictly prohibits any form of tipping-off - clients must not be informed if a report is made or under review. Breach of this rule may result in disciplinary action and potential legal liability.

5.7.2. Documentation and Recordkeeping

All unusual transaction reports are documented and retained for a minimum period as required by applicable regulations. This includes:

- All CDD documentation (e.g., client IDs, corporate records);
- Internal risk assessments;
- Records of suspicious activity reports (even if not submitted externally);
- Communications related to onboarding and monitoring.

5.8. Money Laundering Compliance Program

The Company maintains a risk-based AML/CFT Compliance Program to help prevent its services from being used for money laundering, terrorist financing, or related crimes. The program follows the legal requirements Curaçao, including NOIS, NORUT, guidance issued by GCB.

5.8.1. Key Components

The Program includes:

- Clear internal policies and onboarding procedures;
- A designated **Compliance Officer** with the authority to manage AML efforts;
- **CDD and EDD measures** based on client risk level (see Sections 5.4–5.6);

- Ongoing monitoring of client documentation and activity (see Section 5.5);
- A procedure for reporting unusual transactions to the **FIU Curaçao** (see Section 5.7);
- **Recordkeeping** of CDD and monitoring documents for at least **five (5) years**;
- Regular AML **training** for relevant staff;
- Independent reviews or audits of the AML Program, conducted at least **once per year**.

5.8.2. Actions on Suspicion

If a client is suspected of being involved in financial crime, the Compliance Officer may:

- Freeze access to games or integrations;
- Suspend or end the business relationship;
- Block further onboarding;
- File a report with the FIU Curaçao or another authority.

These decisions are reviewed on a case-by-case basis and fully documented, while ensuring no tipping-off occurs.

5.8.3. Review and Updates

The AML Program is reviewed **annually or after major legal or business changes**. The Compliance Officer is responsible for proposing updates, which must be approved by senior management and shared with relevant teams.

6. Compliance and Consequences of Non-Compliance

The Company requires all employees, departments and associated third-parties to comply fully within this Policy. Compliance is essential to maintain legal obligations under Curaçao law and to protect the Company's reputation.

6.1. Compliance Expectations

All relevant personnel and partners must:

- Follow the AML/CFT procedures outlined in this Policy;
- Participate in AML training when required;
- Cooperate with internal and external audits;
- Report any suspicious activity to the Compliance Officer.

6.2. Non-Compliance Consequences

Failure to comply may result in:

- Disciplinary action (e.g., warnings, retraining, termination);
- Suspension or termination of business relationships;
- Legal action or regulatory reporting;
- Financial penalties or reputational damage to the Company.

6.3. Oversight

The Compliance Officer is responsible for handling violations, maintaining records, advising management, and reporting to authorities when necessary. The Company enforces a **zero-tolerance approach** toward financial crime.

7. Related Information

This Policy follows the key AML/CFT legal requirements in Curaçao and reflects the Company's internal procedures for onboarding and monitoring its **operator clients**. As a gambling provider offering B2B

services, the Company is responsible for verifying its clients (not end users), screening for risks, and reporting any suspicious activity.

7.1. Legal and Regulatory References

- **NOIS** – Requires the Company to identify and verify its clients and their key individuals;
- **NORUT** – Requires reporting of unusual or suspicious activity involving clients;
- **Sanctions Laws** – Require screening clients and owners against international sanctions lists;
- **GCB AML Guidelines (2025)** – Outline AML rules for the gaming sector, including game providers.

7.2. Internal Documents

- CDD Form (used for onboarding);
- Internal KYC review procedures;
- AML training materials;
- Reporting templates and internal escalation steps;
- Risk rating and client approval procedures.

7.3. External Tools

- UN, EU, OFAC sanctions lists;
- FATF list of high-risk countries.

All internal documents are available through the Compliance Department upon request.

8. Contact Information

For any questions regarding this policy, please contact.

eMoore N.V.

Legalcompliance Department

Groot Kwartierweg 10, Livestrong Building

Willemstad, Curaçao

Telephone: +599 9 7471401

Email: legalcompliance@the-emgroup.com

9. Policy History

This section Provides a summary of the revision history of the Company's AML/CFT Policy. Any updates to the Policy - whether driven by regulatory changes, audit finding, or internal process updates - must be recorded in this log and approved by senior management.

Initial Implementation	Version Date	Description of Change	Policy Owner	Change Authors	Approved by

17/04/2025	1	--	Compliance Department	--	Compliance Department
------------	---	----	-----------------------	----	-----------------------

Annex I – General Business Risk Assessment Framework

This Annex I provides an overview of the Business Risk Assessment (BRA) framework that JX Group B.V. will implement under the updates Curaçao AML/CFT legal framework effective January 2025. While the Company has previously operated under the former licensing structure, it is currently in a transitional phase and does not have active client relationships at this time. As such, no current risk-based findings can be provided. The following outlines the risk methodology that should be applied prospectively, once operations resume under the new license.

Purpose of the BRA

The purpose of the BRA is to identify, evaluate, and mitigate the money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks JX Group B.V. may face in its role as a B2B gambling provider. The BRA ensures that controls are proportionate to the risk exposure and supports the application of a risk-based approach throughout onboarding and monitoring procedures.

Key Elements of the BRA Framework

Risk Area	Assessment Focus	Planned Controls
<i>Jurisdictional Risk</i>	Assessment of client countries of incorporation, licensing, or operation, particularly if listed by FATF as high-risk.	(a) Restrict onboarding from high-risk jurisdictions; (b) Apply EDD where required.
<i>Business Model Risk</i>	Evaluate of whether the client operates a crypto-only, unlicensed, or unregulated gaming business.	(a) Required valid licenses; (b) Escalate crypto-heavy operators for enhanced review.
<i>Ownership and Control Risk</i>	Analysis of corporate structure, UBO transparency, and use of nominees or bearer shares.	(a) Demand certified UBO declarations and full ownership documentation.
<i>Regulatory Risk</i>	Review of the client's licensing authority and the level of AML/CFT supervision in that jurisdiction.	(a) Accept clients only from recognized regulatory frameworks with equivalent AML standards.
<i>Product and Integration Risk</i>	Assessment of API integration requests, unusual revenue models, or technical setups.	(a) Standardize API onboarding and monitor early-stage activity patterns.

The BRA will be conducted prior to the onboarding of any new client and reviewed at least annually or when significant business changes occur. All assessments and decisions made under this framework will be documented and retained in accordance with Curaçao's AML/CFT obligations.