ANTI-MONEY LAUNDERING & COUNTER-TERRORIST FINANCING POLICY

FXCG Group Limited

EFFECTIVE DATE	June 2026
VERSION	2.0
REVIEW CYCLE	At least annually and upon material regulatory change
DOCUMENT STATUS	Public Policy

Company No. A000001395
No. 9 Cassius Webster Building, Grace Complex, PO Box 1330, The Valley, AI-2640, Anguilla
www.fxcg.com

Document Control

Document	Anti-Money Laundering & Counter-Terrorist Financing Policy
Entity	FXCG Group Limited
Effective Date	June 2026
Version	2.0
Review Cycle	At least annually and whenever there is a material change to law, regulation, risk profile, products, services or delivery channels
Policy Owner	Compliance function

PUBLIC POLICY NOTE
This document summarises FXCG's public AML/CFT principles. Confidential monitoring thresholds, detection rules, alert scenarios, investigation methods and internal reporting criteria are intentionally not disclosed. Internal procedures may impose stricter controls than those described here.

Contents

1. Purpose and Scope

FXCG Group Limited ("FXCG") is committed to maintaining proportionate and effective measures to prevent its products, services and payment channels from being used for money laundering, terrorist financing, proliferation financing or other financial crime.

This Policy applies to FXCG and, where adopted or required, to relevant officers, employees, contractors, agents and outsourced service providers involved in customer onboarding, account administration, payments, transaction monitoring, compliance or related activities.

FXCG applies a risk-based approach. The nature and extent of controls may vary according to the customer, beneficial owner, jurisdiction, product, transaction, delivery channel and other relevant risk factors. Where applicable law imposes a higher standard, the applicable law prevails.

Money laundering

Money laundering is the process of concealing or disguising the criminal origin, ownership or control of funds or other property so that they appear to have a legitimate source. It is commonly described in three stages:

Placement	Introducing criminal proceeds into the financial system or converting them into financial instruments or assets.
Layering	Moving or transforming funds through multiple transactions or accounts to obscure their origin, ownership or audit trail.
Integration	Reintroducing funds into the legitimate economy so that they appear to be lawful wealth or income.

2. Legal and Regulatory Framework

To the extent applicable to FXCG and its activities, this Policy is designed to support compliance with the AML/CFT legal framework in force in Anguilla, including:

- Proceeds of Crime Act, R.S.A. c. P98;
- Anti-Money Laundering and Terrorist Financing Regulations, R.R.A. P98-1, as amended, including the Anti-Money Laundering and Terrorist Financing (Amendment) Regulations, 2026 (R.A. 21/2026);
- Anti-Money Laundering and Terrorist Financing Code, R.R.A. P98-5, as amended, including the Anti-Money Laundering and Terrorist Financing (Amendment) Code, 2026 (R.A. 22/2026); and
- applicable anti-terrorism, sanctions, proliferation-financing and related laws, Orders in Council, directions and requirements in force from time to time.

FXCG may also take account of guidance, notices and risk information issued by competent authorities and relevant international standard-setting bodies when updating its controls.

3. AML/CFT Governance and Risk-Based Approach

3.1 Business-wide risk assessment and risk-based approach

FXCG maintains a documented assessment of the money-laundering and terrorist-financing risks relevant to its business and uses that assessment to design, maintain and update proportionate AML/CFT policies, procedures, systems and controls. The assessment takes account of the business structure and outsourcing model, customers, connected countries and territories, products and services, transaction types and delivery channels, and is reviewed when material changes occur.

Customer-level controls are calibrated to the assessed risk. Higher-risk relationships receive enhanced measures and closer monitoring, while simplified measures may be used only where permitted by law and supported by a documented low-risk assessment.

3.2 Governance oversight

Senior management and, where applicable, the board are responsible for ensuring that AML/CFT responsibilities are appropriately allocated, effective controls are implemented, material issues are escalated and sufficient authority and resources are available to the compliance function.

3.3 Money Laundering Compliance Officer

Where required by applicable law, FXCG will appoint an appropriately senior Money Laundering Compliance Officer (MLCO) with timely access to records and information necessary to oversee compliance with applicable AML/CFT obligations, policies, procedures, systems and controls.

3.4 Money Laundering Reporting Officer

Where required by applicable law, FXCG will appoint an appropriately senior Money Laundering Reporting Officer (MLRO) responsible for receiving and assessing internal disclosures and determining whether a suspicious activity report should be submitted to the competent authority. The MLCO and MLRO roles may be held by the same person where permitted and appropriately approved.

3.5 Group-level information sharing

Where relevant, lawful and proportionate, FXCG may share customer, account, transaction and financial-crime risk information within its group for compliance, audit, risk management and AML/CFT purposes. Any such sharing is subject to confidentiality, security, data-protection and applicable legal requirements.

4. Customer Due Diligence

FXCG will apply customer due diligence (CDD) before establishing a business relationship or carrying out a transaction where CDD is required, and at other times where required by applicable law or risk. The 2026 amendments to the Anguilla AML/CFT framework reinforce that suspicion-based CDD obligations apply regardless of otherwise applicable transaction thresholds or exemptions.

4.1 Core CDD measures

- identify the customer and verify identity using reliable, independent documents, data or information;
- identify and, where required, verify beneficial owners and persons exercising ownership or control;
- identify authorised representatives and verify their authority to act;
- understand the purpose and intended nature of the relationship and expected account activity;
- obtain source-of-funds information and, where appropriate or required, source-of-wealth information;
- screen relevant parties for sanctions, politically exposed person (PEP) status and other financial-crime risk indicators; and
- keep CDD information accurate, relevant and reasonably up to date.

4.2 Individual customers

Individual customers are generally required to provide their full legal name, date of birth, nationality or country of origin, residential address and other information reasonably required to establish and verify identity. FXCG may require a valid passport, national identity card, photographic driving licence, proof of residential address and other supporting evidence. Certified or notarised translations may be required where documents cannot be reliably reviewed in the language provided.

4.3 Corporate and other legal-person customers

For companies and other legal persons, FXCG will obtain sufficient information to identify and verify the entity, understand its legal form, ownership and control structure, identify beneficial owners, verify authorised persons, understand the nature of the business and establish the expected purpose and activity of the relationship.

4.4 Simplified due diligence

Simplified due diligence may be applied only where permitted by law and supported by a documented assessment that the relationship or transaction presents a low degree of money-laundering and terrorist-financing risk. Simplified due diligence does not remove the requirement for ongoing monitoring and will not be applied or continued where there is suspicion, material doubt about CDD information or an elevated risk that requires enhanced measures.

5. Customer Risk Assessment and Enhanced Due Diligence

FXCG may assign customers and relationships a risk classification and apply enhanced due diligence (EDD) and enhanced ongoing monitoring where a higher risk is identified. Relevant factors may include:

Customer risk	Complex ownership, opaque structures, unexplained use of intermediaries, unusual business profile or reluctance to provide information.
Geographic risk	Connections to jurisdictions associated with elevated money-laundering, terrorist-financing, sanctions, corruption or financial-crime risk.
Product / transaction risk	Unusual complexity, rapid movement of funds, activity inconsistent with the stated purpose, or transactions lacking an apparent economic rationale.
Delivery risk	Non-face-to-face onboarding, unusual payment methods or other delivery channels that may increase impersonation or concealment risk.
PEP risk	A customer, beneficial owner or connected person who is a foreign or domestic PEP, an international-organisation PEP, or a family member or close associate.
Source risk	Source of funds or source of wealth that is difficult to verify, inconsistent with the customer profile, unnecessarily layered or otherwise unclear.

5.1 Politically exposed persons

FXCG will take reasonable measures to identify PEPs and relevant family members or close associates. Where required by law or the assessed risk, FXCG may require senior management approval, establish source of wealth and source of funds, obtain additional supporting evidence and apply enhanced ongoing monitoring.

5.2 High-risk customers and jurisdictions

Customers, beneficial owners, transactions or payment flows connected to higher-risk countries or territories may be subject to enhanced verification, additional source-of-funds or source-of-wealth evidence, closer transaction review, restrictions or refusal. FXCG may also impose risk-based limits or controls beyond the minimum legal requirement where reasonably necessary.

6. Sanctions and Financial Crime Screening

FXCG may screen customers, beneficial owners, authorised persons, counterparties and transactions against applicable sanctions restrictions and other relevant financial-crime risk information. Screening may occur at onboarding, periodically during the relationship and when material customer or transaction information changes.

Where a potential match or restriction is identified, FXCG may pause or reject onboarding, delay or reject a transaction, request additional information, restrict account activity or take other measures permitted or required by law. Assets or funds will be frozen or blocked where required by applicable sanctions law, a competent authority or other legally binding measure.

7. Ongoing Monitoring and Periodic Review

FXCG monitors customer activity on an ongoing basis to identify activity that is inconsistent with the customer's known profile, stated purpose, expected transaction pattern or legitimate economic rationale. Monitoring may be automated, manual or a combination of both.

- review transactions and account behaviour against known customer and risk information;
- identify unusual, complex, high-risk or otherwise suspicious activity;
- refresh identity, beneficial ownership, source-of-funds, source-of-wealth or other KYC information when due or triggered by risk events;
- reassess the customer risk rating when material information changes; and
- escalate material concerns for compliance review and, where appropriate, MLRO assessment.

8. Suspicious Activity Reporting and Confidentiality

8.1 Internal escalation

Employees and relevant personnel must promptly escalate knowledge, suspicion or reasonable grounds for suspicion of money laundering, terrorist financing or related criminal activity through FXCG's internal reporting channel to the MLRO or designated compliance function. Internal reports must not be filtered or suppressed by line management.

8.2 MLRO assessment and external reporting

The MLRO will consider relevant information, document the assessment and determine whether a suspicious activity report (SAR) should be submitted to the competent Reporting Authority or Unit as required by applicable law. Attempted or refused transactions may also be reportable where they give rise to the required level of knowledge or suspicion.

8.3 No tipping off

Information concerning an internal or external SAR, an investigation or related law-enforcement engagement is confidential and must not be disclosed where doing so is prohibited. In line with the 2026 amendments, where continued CDD would reasonably risk tipping off a customer in a case involving suspicion and an intended or actual SAR, FXCG may cease further CDD steps to the extent permitted by law and will make the required report if one has not already been made.

9. Deposits and Withdrawals

CORE PAYMENT PRINCIPLE

FXCG does not accept or make cash payments. Customer funding and withdrawals are subject to source-of-funds, ownership and payment-channel verification. Third-party funding or withdrawals are not permitted unless expressly allowed by applicable law and FXCG's written payment procedures.

- Funds should originate from a bank account, payment card or other payment method approved by FXCG and held in the same name as the FXCG trading account, subject to verification and payment-provider rules.
- Withdrawals will normally be returned to the original funding source up to the amount originally received from that source, where the payment method supports refunds or withdrawals.
- Profits or amounts that cannot be returned to the original funding method may be paid to a verified bank account or other approved payment method in the same name as the trading account holder, subject to applicable law and provider capability.
- FXCG may request bank statements, payment-account evidence, proof of ownership, source-of-funds documentation or other supporting information before processing a deposit or withdrawal.
- FXCG may reject, delay, reverse or otherwise restrict a payment where ownership cannot be verified, the transaction is inconsistent with the customer profile, required information is not provided or a legal/compliance restriction applies.

10. Record Keeping and Data Retention

FXCG maintains records sufficient to evidence customer identification and verification, beneficial ownership, account activity, transactions, AML/CFT reviews, internal and external reporting decisions, training and other relevant compliance actions.

Applicable Anguilla AML/CFT Regulations prescribe a five-year baseline record-retention period for relevant AML/CFT records and permit a longer period to be required by the Commission or the Unit. As an internal policy standard, FXCG will generally retain relevant AML/CFT and transaction records for not less than seven years after the relevant transaction is completed or the business relationship ends, unless a longer or different period is required or permitted by applicable law, investigation, legal hold, regulatory direction or data-protection requirement.

Records will be maintained in a form that is reasonably retrievable, secure and sufficient to support transaction reconstruction, compliance review and lawful requests from competent authorities.

11. Employee Training and Control Testing

FXCG provides AML/CFT awareness and role-appropriate training to relevant personnel. Training is refreshed periodically and when material legal, regulatory, product or risk changes occur. Training may cover customer due diligence, beneficial ownership, PEPs, sanctions, source of funds and wealth, unusual activity, internal escalation, suspicious activity reporting, confidentiality and tipping-off restrictions.

FXCG will maintain procedures to monitor and test the effectiveness of its AML/CFT policies, procedures and training. Where weaknesses or inadequacies are identified, controls will be enhanced or remediated as necessary. Training and testing records will be retained in accordance with applicable requirements and FXCG's record-retention standards.

12. Reliance on Third Parties and Outsourcing

Where permitted by law, FXCG may rely on an introducer, intermediary, agent or outsourced service provider to perform specified elements of CDD, screening, record keeping or related operational activities. FXCG will apply due diligence to such arrangements and obtain required customer information without undue delay.

Reliance or outsourcing does not transfer FXCG's responsibility for compliance. FXCG remains responsible for ensuring that outsourced or relied-upon measures are adequate, appropriately governed and capable of producing records and information required by FXCG and competent authorities.

13. Restrictions, Refusals and Termination

FXCG may refuse to establish a relationship, decline or delay a transaction, request additional documents, restrict account functionality, suspend activity or terminate a customer relationship where reasonably necessary to manage financial-crime risk, comply with contractual rights or satisfy applicable legal and regulatory requirements.

Where a freeze, blocking measure or other restriction on access to funds is required by law, sanctions measures, court order or a competent authority, FXCG will act in accordance with the applicable requirement. Nothing in this Policy gives FXCG a right to confiscate customer property outside applicable law and contractual rights.

14. Policy Review and Updates

This Policy will be reviewed at least annually and earlier where there is a material change to applicable law, regulation, supervisory expectations, FXCG's risk profile, products, services, jurisdictions, payment methods or operating model. FXCG may update this Policy from time to time and publish the current version through its official channels.

INTERPRETATION
This Policy is a high-level statement of FXCG's AML/CFT approach and does not replace customer agreements, payment terms, internal compliance procedures or applicable law. Where there is any inconsistency, applicable law and legally binding requirements prevail.

Annex A - Indicative KYC and KYB Documentation

The documents below are indicative and not exhaustive. FXCG may request additional or alternative evidence depending on customer type, jurisdiction, risk, document quality, payment method and applicable law.

Customer type	Information / evidence	Examples
Individual	Identity	Valid passport; national identity card; photographic driving licence; other reliable government-issued identification accepted by FXCG.
Individual	Residential address	Utility bill; bank or financial-institution statement; government correspondence; other reliable proof of address, generally recent and normally not older than 3 months unless FXCG permits otherwise.
Individual	Source of funds / wealth	Bank statements; payslips; sale agreements; investment statements; tax or business records; inheritance or other evidence appropriate to the stated source.
Corporate / legal person	Existence and legal form	Certificate of incorporation or equivalent; constitutional documents; registered-office evidence; certificate of good standing or equivalent where relevant.
Corporate / legal person	Ownership and control	Shareholder register; beneficial ownership information; ownership chart; director register; partnership or trust information where applicable.
Corporate / legal person	Authority to act	Board resolution; authorised-signatory list; power of attorney or other authority; identification of persons operating the account.
Corporate / legal person	Business and expected activity	Nature of business; principal activities; expected funding and transaction profile; source of funds; financial statements or supporting commercial documentation where relevant.
All customers	Additional verification	Certified copies, notarisation, certified translation, video or electronic verification, liveness checks, database verification or other measures required by FXCG based on risk and legal requirements.