iQuoto

LEGAL DOCUMENT

Financial Crime Policy.

Anti money laundering counter terrorist financing and sanctions

Version	Effective	Issued
1.0	12 October 2026	13 October 2026

iQuoto International Limited, trading as iQuoto Global
Registered in St Vincent and the Grenadines · 25708 BC 2019

iquoto.global

Financial Crime Policy.

This policy sets mandatory Company controls for preventing and detecting money laundering, terrorist financing, proliferation financing, sanctions breaches and related financial crime in the SVG Company's business. It applies to directors, employees, contractors and delegated functions. It is an internal policy. Compliance maintains the supporting procedures and evidence of implementation; failures must be recorded, escalated and remediated.

CONTENTS

1 Entity legal framework and governance
2 Business and client risk assessment
3 Identification and verification
4 Enhanced measures and politically exposed persons
5 Sanctions and proliferation financing
6 Funding withdrawals and crypto routes
7 Monitoring and escalation
8 Records privacy and outsourcing
9 Training assurance and management information
10 Adoption and source record
11 Supporting procedures and guidance

1 Entity legal framework and governance

1.1 iQuoto International Limited is SVG registration 25708 BC 2019. Registered office: The Financial Services Centre, P.O. Box 1823, Stoney Ground, Kingstown, St. Vincent & the Grenadines. It is distinct from iQuoto Limited Mauritius. Corporate registration and AML compliance do not establish forex brokerage authorisation.

1.2 Compliance must maintain an obligations register covering the current applicable SVG proceeds-of-crime framework, AML and Terrorist Financing Regulations and Code, terrorism legislation, sanctions implementation, reporting and registration requirements, and relevant client or service jurisdictions. Compliance obtains and maintains current enacted texts, records amendments, determines scope, competent authorities and deadlines, and assigns responsible owners. The obligations register must be checked before affected activity or an official filing; the absence of an internal entry does not suspend a legal obligation.

1.3 FATF recommendations inform the risk-based design but are international standards, not directly binding Company legislation. Provider-country duties do not automatically become the SVG Company's duties, and provider checks do not replace the Company's responsibility. Legal applicability of crypto payment routes must be assessed separately from crypto CFD dealing.

1.4 The Board approves risk appetite, resources and policy, appoints the responsible reporting officer, receives management information and ensures remediation. The Company has identified Kofi B. Addae-Duah as its reporting officer, appointed on 1 February 2026. Internal concerns are reported through compliance@iquoto.global with access restricted to authorised personnel. No deputy is appointed. The reporting officer must have sufficient authority, independence, expertise, access to records and direct Board access. Commercial staff cannot veto a legally required report. Compliance records and completes any legally required appointment notification and retains evidence.

1.5 During the reporting officer's absence, Support logs and triages concerns, preserves evidence and coordinates lawful protective steps. Critical matters and any risk of a missed deadline or prohibited activity are immediately escalated to the Board using directors' contact numbers held internally. Any director may coordinate the emergency response. This does not itself appoint a director or Support as statutory reporting officer: the Board must ensure the person making any official filing is legally authorised and any required appointment or notification is completed. Maintain restricted access to the current contact directory and filing credentials. The Board must maintain legally authorised emergency filing arrangements and accessible official reporting channels. Support has no authority to make a statutory filing solely by virtue of its triage role. A gap in cover must be escalated immediately and must not cause a required report to be delayed. Do not disclose a suspected report or investigation where prohibited.

2 Business and client risk assessment

2.1 Compliance owns, approves and maintains the documented business-wide financial-crime risk assessment. It covers customer types, countries, forex and CFDs, copy trading, payment channels, pooled funds, counterparty margin, intermediaries, remote onboarding and technology. Assess inherent risk, controls and residual risk before new activity begins. Compliance reviews the assessment annually and whenever products, countries, providers or payment channels materially change, records changes and escalates material risks to the Board.

2.2 Compliance assigns and maintains client risk ratings based on the Company's Countries Rating List. Record the list version, relevant countries, rating rationale and review date in the client file. Geographic rating is a starting point; Compliance must also assess client-specific ownership, control, PEP status, funding, business, channel and suspicious-activity indicators so country rating does not prevent enhanced measures required by the circumstances or law. Compliance documents rating rules and client-specific overrides in the controlled risk procedure; elevated client-specific risks must not be reduced solely by a lower country rating.

2.3 Compliance maintains and updates the restricted-country and eligibility list and the Countries Rating List. Keep their versions, approval dates and access locations controlled. Compliance retains the current lists, prohibited activities and client eligibility rules in the controlled internal repository and makes them available to onboarding and payment staff. Activity must not proceed where eligibility cannot be established. No anonymous, fictitious or inadequately verified relationship is permitted. Nationality alone is not conclusive evidence of wrongdoing, and AML eligibility does not establish product-marketing permission.

3 Identification and verification

3.1 Complete identity, beneficial ownership and authority verification before deposits or trading are enabled. The Company permits no exemptions or delayed-verification exceptions. Obtain individuals' identity, address, date of birth, residence, relevant tax residence, relationship purpose, expected funding and activity, and representatives' identity and authority. Use reliable independent evidence proportionate to risk. Failed or incomplete checks prevent activation and require Compliance assessment; no commercial override is permitted.

3.2 For companies, obtain legal name, registration, registered office, constitutional and current existence evidence, business purpose, directors and authorised persons. Under the Company's policy, identify all beneficiaries and beneficial owners regardless of ownership percentage; do not exclude someone merely for falling below a percentage threshold. Trace ownership to relevant natural persons and identify controlling individuals independently of ownership. Compliance maintains a documented control identification and verification procedure and applies the relevant legal definitions to companies, trusts and funds. Do not equate every legal shareholder with the ultimate natural-person beneficial owner.

3.3 For funds, trusts and fiduciary arrangements identify the contracting entity and capacity, governing documents, manager, trustee, settlor, protector, beneficiaries or beneficiary class and other controlling persons as relevant. Verify authorisation, mandate and investment powers where required. Regulated-fund status does not create automatic simplified due diligence.

3.4 Sumsub assists identity verification. Compliance must approve the exact contracting entity, enabled checks, data processing, retention, reliability and access to underlying evidence. Automated pass results do not replace assessment of inconsistencies. Staff must resolve document fraud, duplicate identity, liveness or sanctions alerts before approval and provide lawful human review where required.

4 Enhanced measures and politically exposed persons

4.1 Enhanced due diligence applies where required by law or justified by elevated risk, including complex unexplained structures, unusual funding, higher-risk geographic exposure, adverse information and politically exposed persons with relevant relatives or close associates. PEP status alone is not evidence of crime.

4.2 Compliance approves high-risk clients and politically exposed persons (PEPs), documenting the assessment and decision before accepting or continuing the relationship. The Company has designated Kofi B. Addae-Duah as the senior-management approver for PEP relationships where that approval is required. Record his approval and the supporting assessment in the client file, and satisfy any additional approval requirements under applicable law. Establish and corroborate source of wealth and source of funds, understand the relationship and apply enhanced monitoring. Source of funds explains the money used for the transaction; source of wealth explains how overall wealth was acquired. Use tax, income, business, sale, inheritance or other credible evidence as appropriate, avoiding excessive unrelated collection.

4.3 The Company does not use simplified due diligence. Full pre-activation verification applies to every client, with enhanced measures where required. The Compliance Team performs scheduled client KYC reviews at intervals not exceeding 12 months for high-risk clients, 18 months for medium-risk clients and 24 months for low-risk clients, measured from completion of onboarding or the latest completed KYC review. Ongoing monitoring applies to all clients between scheduled reviews. Material changes or suspicious activity trigger an earlier review without waiting for the scheduled date. Apply any shorter interval required by law or the circumstances, reassess the risk rating and record the evidence, outcome, approvals and next review date. Compliance records approval of high-risk clients and PEPs and any additional legally required approval in the client file.

5 Sanctions and proliferation financing

5.1 Compliance maintains screening coverage and assesses the sanctions regimes actually applicable to the Company or transaction, including relevant domestic implementation of UN measures and provider obligations. Company-confirmed screening sources comprise OFAC sanctions; UN Security Council sanctions; UK sanctions; the EU Consolidated Sanctions List; EU Most Wanted warnings; US Bureau of Industry and Security lists; US State Department Foreign Terrorist Organizations and non-proliferation lists; US DOJ sources including FBI, DEA and US Marshals; Interpol wanted-person sources; and India's Central Bureau of Investigation list. The Company's legacy reference to HM Treasury lists must be mapped to the current UK Sanctions List, the sole current UK designation source since 28 January 2026. Wanted-person, law-enforcement and export-control sources are not all financial-sanctions lists: assess the legal effect and identifiers of each result, not a generic automatic freeze. Compliance validates enabled Sumsub coverage and source freshness and assesses ownership and control under each applicable sanctions regime, including indirect ownership and relevant aggregation rules. Screening an additional foreign source does not establish universal application of its law.

5.2 The Company uses Sumsub's system to screen clients for sanctions, PEP status and adverse media. Ongoing screening is enabled for all clients and generates alerts when relevant screening information changes. Compliance reviews alerts immediately upon receipt, triages urgency, resolves possible matches using reliable identifiers and documents false-positive reasoning and approval decisions.

Immediate review means prompt assessment and protective action; it does not imply every investigation can be completed instantly. A system result does not replace the Company's assessment or approval. Screen before onboarding and relevant payments, on list changes and on material client changes. Escalate credible sanctions matches and financial-crime concerns immediately to the reporting officer and prevent prohibited activity while the applicable position is assessed. Maintain evidence of enabled settings, alert receipt and review times, and validate screening-list coverage and ownership and control checks against applicable requirements. Escalate any screening or alert-delivery failure promptly and apply appropriate contingency checks.

5.3 Where law requires freezing, prohibition or reporting, act without delay within the legal deadline. Do not return, move or release affected funds without a lawful basis or required permission. Obtain any required licence from the competent authority. Commercial approval cannot substitute for it. Review sanctions-evasion and proliferation indicators, including concealment of counterparties and unusual geographic or payment patterns.

6 Funding withdrawals and crypto routes

6.1 Third-party payments are prohibited. Verify that funding and withdrawal instruments belong to the verified client, including lawful entity authority. Third-party or incorrectly received payments are returned to the originating account with Compliance approval, subject to lawful freezes, directions, card or provider requirements and safe verification of the destination. Keep approval and return evidence. A withdrawal to a different verified account requires Board authorisation and Compliance execution following ownership verification and documented checks. An obligation to freeze or obtain permission prevails over routine return-to-source processing.

6.2 Bank wire, card, approved local APMs and supported crypto routes require approved providers and documented originator, beneficiary, currency and channel information. Client funds are pooled separately from operating funds; daily reconciliation by Risk, Compliance and Trading supports, but does not replace, monitoring of individual clients and funding provenance.

6.3 Crypto transactions are handled by Xoala Digital, the trading name of Xoala IOM Limited, Isle of Man company number 019808V. The Company identifies its Isle of Man Financial Services Authority Designated Business registration as ID 332; XOALA's public disclosure corroborates these identifiers. This is distinct from Steven AB's Swedish EMI cash-account service. Designated Business registration is not represented as a banking, investment-services or forex brokerage licence or a compensation guarantee. Compliance oversees wallet ownership or control, blockchain risk and sanctions checks. Apply supported asset and network controls and proportionate analysis of exchange, mixer, theft and sanctions risks with off-chain information. Board authority and Compliance execution govern unverifiable-payment handling, subject to legal restrictions: no payment is processed or returned in breach of a freeze or required direction. Required transfer information and travel-rule duties depend on applicable law and service classification. Maintain the actual provider agreement and service-scope evidence.

6.4 The Board authorises financial-crime holds and releases; Compliance executes those decisions working with Risk, with ongoing review and a recorded basis, scope and decision history. Mandatory prohibitions or freezes must be observed promptly and cannot await discretionary approval. Explain permitted information without tipping off. Complete verified withdrawals retain the agreed 12 operating-hour processing requirement, subject to lawful restrictions. AML does not authorise indefinite discretionary withdrawal restriction or forfeiture.

7 Monitoring and escalation

7.1 Ongoing monitoring applies to all clients and covers funding, trading, withdrawals, copy relationships and changes against the client's profile. It continues between scheduled KYC reviews and is not replaced by them. Indicators include repeated deposits followed by little trading and rapid withdrawal, inconsistent funding, splitting to evade controls, linked accounts, identity anomalies, opaque structures, collusive trading, unexplained transfers of value and activity inconsistent with the business purpose. Material changes or suspicious activity trigger an earlier Compliance Team KYC review and any necessary escalation. An indicator requires assessment; profitable trading, latency concerns or a complaint alone are not evidence of money laundering.

7.2 The Company continuously monitors deposits, trading and withdrawals using Risk Team-built systems and Sumsub. Monitoring rules and thresholds are documented internally; Compliance approves changes and maintains a controlled change record. Confidential threshold values need not appear in this policy. Risk and Compliance jointly investigate transaction alerts, beginning review within a few hours of receipt. Record receipt, investigators, assessment, actions and outcome. Critical concerns, prohibited-activity risks and reporting deadlines require immediate triage and lawful protective action. This timing describes the start of review, not guaranteed completion. Compliance reviews screening alerts immediately under clause 5.2. Financial-crime concerns go promptly to Kofi through compliance@iquoto.global; do not wait for proof or tip off the client.

7.3 Kofi B. Addae-Duah, as reporting officer, independently assesses internal disclosures, preserves evidence and records the reasons for reporting or not reporting. Where the applicable legal test is met, he submits the required report directly through the competent authority's official channel, including SVGFIU where applicable, within the applicable legal deadline and retains submission evidence and any acknowledgment. Sumsub supports case management, record storage and report preparation. It is treated as a submission route only where delivery to the competent authority is confirmed and evidence is retained. Generating a report or adding information to a screening or shared database does not constitute statutory filing. Reports cover attempted as well as completed activity where required. Obtain required consent or directions before proceeding where law requires them. Compliance maintains the current official channels, forms, deadlines, access credentials and emergency arrangements in a restricted reporting procedure and verifies them before use. The Board ensures authorised cover during absence under clause 1.5. Any external database sharing requires a separate lawful basis and assessment of confidentiality, accuracy and data protection.

7.3A Depending on the applicable reporting obligation and jurisdiction, potential overseas recipients include FinCEN, UKFIU, FINTRAC, FIU-IND, Tracfin, Germany's FIU, UAE FIU, QFIU, EMLCU, South Africa FIC, NFIU, Ghana FIC and Kenya FRC. This is a routing reference, not an instruction to report every case to every authority. Compliance determines the actual legal nexus, recipient, filing eligibility and channel; the location of activity alone does not establish every foreign reporting duty.

7.4 Restrict knowledge of reports and investigations to authorised personnel. Do not disclose a report, suspected report or investigation where prohibited. Seek guidance before asking questions that could tip off. Legal confidentiality restrictions do not permit false statements to clients or unnecessary disclosure to providers. Board reporting uses restricted or anonymised information as appropriate.

8 Records privacy and outsourcing

8.1 The Company has confirmed a seven-year retention period for KYC files, transaction records and AML investigation and report records, measured from the inception of each relevant action. Record that inception date for each record or case. KYC files are also retained throughout the client relationship, including where the relationship lasts longer than seven years. KYC files are retained for a further seven years after account closure. For KYC files, this relationship-based period supplements the inception-based period and prevents earlier disposal. Keep records retrievable and sufficient to reconstruct identity, beneficial ownership, risk assessments, approvals, transactions, alerts, reports and decisions. The Company period does not authorise disposal before an applicable statutory period expires, while the record is needed for ongoing due diligence, or while a lawful hold applies. If law measures retention from relationship termination, transaction completion or another later event, that applicable requirement prevails. Assess any applicable limits on retention, including sensitive data. Communications remain retained seven years from the event under the existing policy. Compliance maintains a retention schedule defining category inception dates, applicable statutory triggers, legal bases and access rules, including open investigations that extend beyond the original inception date.

8.2 Company records are stored on the Company's servers; directors have access and supervisory responsibility. Sumsub also holds relevant case and report records under clause 7.3. Maintain documented access permissions, secure transmission, backups and audit trails, and restrict report and investigation access to authorised personnel with a need to know. The Board authorises record deletion and Compliance executes it after retention and hold checks. Compliance maintains documented permissions for each operational role; access to reports and investigations is restricted to authorised personnel with a need to know. Use proportionate collection and lawful provider sharing and international transfers under the Privacy Notice. Preserve records needed for open investigations, actual or anticipated proceedings and lawful holds; seven years does not authorise disposal while those needs remain. Dispose securely when retention is no longer justified.

8.3 Compliance oversees Sumsub and other outsourced AML functions. Manual verification by Compliance is the fallback for screening or monitoring failures, subject to adequate evidence and lawful restrictions where checks cannot be completed. Record the outage, scope, fallback checks and recovery reconciliation. Outsourcing does not transfer accountability. Compliance validates and retains provider contract and settings review evidence covering access to evidence, confidentiality, audit, incidents, continuity, retention and data handling. Statutory third-party reliance requires its actual legal conditions; ordinary outsourcing is not automatically such reliance.

9 Training assurance and management information

9.1 Compliance delivers and records induction and at least annual staff AML refresh training as an adopted Company requirement. Keep attendance and competence evidence and provide role-specific training for directors, onboarding, payments, Support, Trading and technology staff on escalation, sanctions, fraud, privacy and tipping-off. Assess suitability of staff in sensitive roles lawfully and proportionately.

9.2 Compliance coordinates assurance and testing of controls, files, alert handling, payment checks and provider oversight. An independent review takes place at least annually. Directors and other personnel involved in designing, operating or approving the controls under review are excluded from performing that review or determining its findings. The reviewer must be suitably qualified, independent of the

activities reviewed and able to report findings directly to the Board. The Board appoints an external reviewer where sufficient internal independence or expertise is unavailable. Record the scope, independence assessment, findings, owners, deadlines and evidence of remediation. The Board retains oversight and responsibility for corrective action; that oversight does not substitute for the independent review.

9.3 The Board receives at least quarterly risk and control reporting as an adopted Company requirement, covering high-risk relationships, overdue reviews, alerts, reports in permitted form, sanctions issues, training, provider failures and remediation. Escalate significant failures immediately. Record breaches and required notifications; staff concerns must have a protected internal escalation route.

10 Adoption and source record

10.1 Policy owner: Compliance. Company-confirmed Board approval date and effective date: 12 October 2026. This final issue incorporates Company instructions confirmed through 13 October 2026. Compliance retains the approval record and final text in the controlled policy register and records subsequent amendments. Compliance reviews the policy quarterly and upon material change. The next scheduled review is 12 January 2027. Quarterly policy review is separate from the annual business risk assessment and independent review. Compliance verifies and records the Company's applicable SVG AML/CFT supervisory, registration and reporting obligations and supporting evidence. Corporate registration or an FSA forex letter does not establish a brokerage licence, an AML registration or an official reporting route.

11 Supporting procedures and guidance

11.1 Compliance maintains controlled procedures for client and business risk assessments, country and eligibility lists, ownership and control verification, enhanced due diligence, screening, monitoring thresholds, payment checks, statutory reporting, retention, access permissions, outsourcing, contingency arrangements and independent review. These procedures must implement this policy and applicable law. Missing evidence or an incomplete procedure must be logged, escalated and addressed; activity requiring an uncompleted control must not proceed.

11.2 The Source of Wealth and Funds Guidance supports evidence collection for salary and savings, investments, property and company sales, inheritance, loans, gifts, winnings, compensation and other funds. Compliance assesses authenticity, plausibility, amounts and the funding trail; documents alone do not establish approval. Source of funds and overall source of wealth are separate assessments. Any reference in supporting guidance to payment directly by a solicitor, accountant or other third party is subject to the prohibition in clause 6.1. Gift, loan or estate evidence does not permit third-party funding. Compliance controls updates to the guidance, including company identity, version and contact information.

iQuoto

Questions about this document?

Support

support@iquoto.global

Compliance and complaints

compliance@iquoto.global

Website

iquoto.global

Client portal

secure.iquoto.global

---

iQuoto International Limited, trading as iQuoto Global. An International Business Company incorporated in St Vincent and the Grenadines, registration number 25708 BC 2019.

Registered office and correspondence address: The Financial Services Centre, P.O. Box 1823, Stoney Ground, Kingstown, St. Vincent & the Grenadines.

Risk warning. FX and CFDs are complex, leveraged financial products which carry a high level of risk to your capital. Trading on margin can result in losses that exceed your deposits, and these products are not suitable for all investors. You should ensure you fully understand the risks involved, and seek independent advice if necessary, before opening an account. Past performance is not a reliable indicator of future results.

© 2026 iQuoto International Limited