ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

1 Purpose And Scope

1.1 This Anti-Money Laundering and Counter-Terrorist Financing Policy (this "**Policy**") sets out the principles, standards, and controls adopted by Solitaire Prime Ltd. ("**Solitaire Prime**" or the "**Company**") to prevent the use of its products and services for money laundering, terrorist financing, sanctions evasion, proliferation financing, fraud, and related financial crimes (collectively, "**Financial Crime**").

1.2 This Policy applies to all business lines, products, and delivery channels of Solitaire Prime, including online trading, account onboarding, deposits/withdrawals, and any ancillary services offered via www.solitaireprime.com and associated mobile/web applications (the "**Platform**"). It applies to all employees, contractors, directors, and controlled affiliates (collectively, "**Personnel**") across all jurisdictions in which Solitaire Prime operates or markets its services.

1.3 Company will comply with applicable AML/CFT and sanctions laws and regulations in relevant jurisdictions, including (as applicable) the laws of Saint Lucia and other countries where services are offered or clients are onboarded, as well as relevant international standards, including the Financial Action Task Force ("**FATF**") Recommendations, the Wolfsberg Principles, and applicable guidance from competent authorities.

2 Governance And Responsibilities

2.1 The Board of Directors has ultimate responsibility for AML/CFT compliance, risk appetite, and oversight of the effectiveness of this Policy. The Board approves this Policy and receives at least annual reports on AML/CFT risks, control effectiveness, material incidents, and remedial actions.

2.2 Senior Management of the Company is responsible for implementing this Policy, allocating adequate resources, and fostering a culture of compliance. Senior Management will ensure the AML/CFT program keeps pace with the Company's growth, products, geographies, and risk profile.

2.3 Company will maintain an independent Compliance function with authority, resources, and expertise proportionate to its risk profile. The Compliance function will:

2.3.1 Develop and maintain AML/CFT policies, procedures, and controls.

2.3.2 Conduct enterprise-wide and product-level AML/CFT risk assessments.

2.3.3 Oversee KYC/CDD/EDD processes, sanctions screening, transaction monitoring, and reporting.

2.3.4 Deliver training, testing, and assurance activities.

2.3.5 Liaise with regulators and Financial Intelligence Units ("**FIU**").

2.4 Company appoints a Money Laundering Reporting Officer ("**MLRO**") with direct access to the Board. The MLRO is responsible for: (i) receiving and evaluating internal suspicious activity reports, (ii) directing investigations, (iii) filing external Suspicious Transaction/Activity Reports (STRs/SARs) with competent authorities, and (iv) maintaining required records. A Deputy MLRO will be appointed to ensure continuity.

3 Risk-Based Approach

3.1 **Enterprise-Wide Risk Assessment ("EWRA")**: Company will conduct an Enterprise-Wide Risk Assessment ("**EWRA**") at least annually and upon material changes (e.g., new products, geographies, delivery channels, or regulatory developments). The EWRA will evaluate inherent and residual risks across customer types, products/services, geographies, distribution channels, and transaction patterns, and inform control design and resource allocation.

3.2 **Customer Risk Rating**: Customers will be risk-rated (e.g., low, medium, high) based on factors including but not limited to customer type (natural person, corporate, trust), jurisdiction(s), Politically Exposed Person ("**PEP**") status, business activity, source of funds/wealth, product usage, and transactional behavior. Risk ratings will drive the level of due diligence, monitoring, and periodic review.

3.3 **Product and Channel Risk**: New products/features (e.g., leverage, new asset classes, payment rails, or third-party integrations) will undergo pre-launch AML/CFT risk assessment, with mitigating controls defined before go-live. Non-face-to-face onboarding and digital channels will include additional safeguards (e.g., biometric verification, liveness, device fingerprinting).

4 Customer Due Diligence and Know Your Customer

4.1 When Customer Due Diligence ("**CDD**") is Required. CDD is performed at onboarding, when conducting occasional transactions above applicable thresholds, upon suspicion of Financial Crime, or when doubts arise as to the veracity or adequacy of previously obtained customer information.

4.2 Natural Persons. At a minimum, Company will collect and verify:

4.2.1 Full legal name, date of birth, nationality/citizenship.

4.2.2 Residential address and contact details.

4.2.3 Occupation and employer name (or self-employment details).

4.2.4 Purpose and intended nature of the relationship.

4.2.5 *Source of funds and, where appropriate, source of wealth.*

4.3 *Acceptable documents include a valid government-issued photo ID (e.g., passport, national ID, driver's license) and recent proof of address (e.g., utility bill or bank statement not older than three months). Where permitted, electronic identity verification and trusted databases may be used. Liveness and biometric checks may be applied to mitigate impersonation and deepfake risks.*

4.4 *For corporate customers, Company will obtain and verify:*

4.4.1 *Legal name, incorporation/registration number, date, and country of incorporation.*

4.4.2 *Registered office and principal place of business.*

4.4.3 *Nature of business, ownership and control structure, directors and authorized signatories.*

4.4.4 *Purpose and intended nature of the relationship.*

4.4.5 *Source of funds and, where appropriate, source of wealth.*

4.5 *Documents may include Certificate of Incorporation, Memorandum and Articles/Constitution, Register of Directors and Shareholders, proof of registered address, board resolution authorizing the account, and identification and address verification for directors, authorized signatories, and beneficial owners.*

4.6 *Company will identify and verify the natural persons who ultimately own or control the customer, typically those owning or controlling, directly or indirectly, 25% or more of the equity or voting rights, or who otherwise exercise control through other means. Reasonable measures will be taken to verify Ultimate Beneficial Owners ("**UBO**") identities and to understand any complex or opaque ownership chains.*

4.7 *Company will screen customers, UBOs, and relevant connected parties for PEP status (domestic and foreign), as well as their close associates and family members. Enhanced Due Diligence ("**EDD**"), including Senior Management approval, will be required for PEP relationships.*

4.8 *At onboarding and on a continuous basis, customers and relevant parties will be screened against applicable sanctions lists (e.g., UN, OFAC, EU, UK) and relevant watchlists. Matches will be investigated and, where confirmed, the account will be blocked or restricted and reported as required by law.*

4.9 *Customer information will be reviewed periodically based on risk rating (e.g., low: every three years; medium: every two years; high: annually, or more frequently). Trigger events (e.g., change in ownership, unusual behavior, adverse media) will prompt an interim review and*

refresh.

4.10 If Company cannot complete CDD to a satisfactory standard, it will not open the account, will not execute transactions, or will terminate the relationship and consider filing an STR/SAR.

5 Enhanced Due Diligence

5.1 EDD will be applied to customers assessed as high risk, including but not limited to PEPs customers from high-risk or sanctioned jurisdictions; complex structures; correspondent or intermediary arrangements; non-resident clients; customers dealing in cash-intensive or high-risk sectors; adverse media exposure; or where the purpose/transaction pattern is unusual or unclear.

5.2 Measures may include deeper verification of identity and UBOs, independent verification of source of funds/wealth, gathering additional information on business activities and expected account activity, obtaining Senior Management approval, imposing lower transactional thresholds, and enhanced ongoing monitoring.

6 Transaction Monitoring and Controls

6.1 Company operates automated and manual post- and near-real-time monitoring, tailored to product and customer risk. Scenarios and typologies include: unusually large or rapid transactions, layering patterns, structuring/smurfing, velocity spikes, inconsistent behavior versus profile, use of third-party payment accounts, flows to/from high-risk jurisdictions, frequent deposits/withdrawals without commensurate trading activity, and misuse of promotional credits.

6.2 Examples include:

6.2.1 Sudden high-volume funding from unrelated third parties.

6.2.2 Multiple accounts controlled by the same device or IP/subnet, or frequent device changes.

6.2.3 Circular transfers between related accounts or brokers without economic rationale.

6.2.4 Immediate withdrawals after deposits without substantive trading.

6.2.5 Use of privacy-enhancing technologies to obfuscate identity or location.

6.2.6 Transactions involving sanctioned persons, embargoed jurisdictions, or high-risk payment intermediaries.

6.3 Compliance will document investigations, decisions, rationales, and supporting evidence. Where suspicion remains, the MLRO will determine whether to file an STR/SAR and whether to

restrict, freeze, or terminate the account.

6.4 When required by law or upon confirmed sanctions matches, relevant accounts or transactions will be blocked or frozen. Customers will not be notified where tipping-off prohibitions apply.

7 Recordkeeping

7.1 Company will maintain CDD records, UBO information, transaction data, monitoring and investigation files, STRs/SARs, training records, and policy/procedure versions for at least five years from the termination of the relationship or longer where required by law or in connection with investigations.

7.2 Records will be stored securely, be retrievable in a timely manner, and be made available to competent authorities upon lawful request. Access will be controlled and monitored in line with data protection laws.

8 Reporting and Cooperation

8.1 Personnel must promptly escalate any knowledge, suspicion, or reasonable grounds to suspect Financial Crime to the Compliance function or MLRO through designated internal channels.

8.2 The MLRO will assess internal reports and, where appropriate, file STRs/SARs with the competent FIU and cooperate with law enforcement, regulators, and other authorities as required.

8.3 Personnel are strictly prohibited from informing any person that an STR/SAR has been filed or that an investigation is contemplated or underway, except as permitted by law.

9 Sanctions Compliance

9.1 The Company will screen customers, UBOs, transactions, and, where feasible, counterparties against applicable sanctions lists at onboarding and on a continuous basis.

9.2 The Company will not onboard or transact with sanctioned persons, entities, or jurisdictions where such dealings would violate applicable sanctions laws. Where risk is high but legally permissible, additional controls and approvals will be required.

9.3 Payment rails, correspondent institutions, and processors will be risk-assessed and subject to appropriate due diligence, contractual undertakings, and ongoing oversight.

10 Third Parties and Outsourcing

10.1 Where Company relies on regulated third parties for elements of CDD or screening, it will ensure (i) the third party is competent and regulated, (ii) CDD information is available without delay, and (iii) ultimate responsibility remains with Solitaire Prime.

10.2 Introducers, referral partners, and affiliates are subject to due diligence and contractual

AML/CFT obligations, including audit rights, data sharing, training expectations, and termination for cause where AML/CFT non-compliance is identified.

10.3 Screening, KYC, and monitoring vendors will be assessed for data quality, model performance, coverage, latency, uptime, and information security. Vendor performance will be reviewed periodically.

11 Training and Awareness

11.1 All Personnel, particularly client-facing, operations, and product teams, will receive AML/CFT training at onboarding and at least annually thereafter. Training will be tailored by role and include emerging typologies (e.g., deepfake identity fraud, synthetic IDs, mule activity).

11.2 Knowledge checks and certifications will be required. Training completion rates will be tracked and reported to Senior Management. Failure to complete training may result in disciplinary measures.

12 Independent Testing and Internal Audit

12.1 The AML/CFT program will be subject to periodic independent testing by qualified internal audit or external assessors to evaluate design and operating effectiveness. Findings will be tracked to closure with deadlines and accountable owners.

12.2 Detection scenarios, thresholds, and screening/monitoring models will be calibrated, validated, and back-tested periodically. Changes will be documented and approved through a defined governance process.

13 Product and Change Management

13.1 New products, features, payment methods, geographic expansions, or material process changes require a New Product Approval ("**NPA**") review covering AML/CFT and sanctions risks, data, controls, and client communications before launch.

13.2 Marketing campaigns and incentives will be reviewed for AML/CFT risks (e.g., bonus abuse, mule recruitment) and appropriate mitigants applied.

14 Data Protection and Confidentiality

14.1 Personal data collected for AML/CFT purposes will be processed lawfully, fairly, and transparently, and used solely for compliance and risk management purposes in accordance with applicable data protection laws and the Company's Privacy Policy. Processing will be limited to what is necessary, with appropriate legal bases (including compliance with legal obligations and legitimate interests), data minimization, accuracy, and retention controls. Personal data will be retained only for as long as required by law or a legitimate regulatory need and then securely deleted or anonymized.

14.2 Customer information may be shared, as permitted or required by law, with regulators, Financial Intelligence Units ("**FIU**"), law enforcement, auditors, banking and payment partners, and vetted KYC/sanctions screening and transaction monitoring providers, subject to contractual confidentiality, purpose limitation, and security obligations. Cross-border transfers will occur only where adequate safeguards are in place (e.g., contractual clauses, recognized adequacy, or other lawful transfer mechanisms). The Company will implement technical and organizational measures to protect personal data against unauthorized access, alteration, or disclosure, including access controls, encryption in transit and at rest (where appropriate), logging, and periodic testing. Nothing in this Clause restricts disclosures prohibited from customer notification under tipping-off rules.

15 Customer Communication and Terms

15.1 Company's Terms and Conditions and Privacy Policy will describe AML/CFT obligations, potential requests for information, transaction limits, account restrictions, and the Company's right to refuse or terminate services where AML/CFT risk is unacceptable.

15.2 Customers must provide information and documents requested for CDD/EDD, ongoing monitoring, or investigations. Failure to cooperate may result in delayed transactions, restrictions, or termination.

16 Breach, Disciplinary Measures, and Whistleblowing

16.1 Breach of this Policy by any Personnel will be investigated promptly and may result in proportionate disciplinary action, up to and including termination of employment or contract, removal of access rights, reporting to regulators or law enforcement, and civil recovery where applicable. Disciplinary decisions will be documented and consistent with Company HR policies and applicable law.

16.2 The Company maintains confidential and, where permitted by law, anonymous channels for reporting suspected misconduct or breaches of this Policy, including direct reporting to the MLRO, Compliance, or via the whistleblowing hotline/email listed in Clause 18. Retaliation against any person who, in good faith, seeks guidance, raises a concern, or participates in an investigation is strictly prohibited and will itself be treated as a disciplinary offense. Reports will be acknowledged, triaged, and addressed in a timely manner, with outcomes recorded and, where required, escalated to Senior Management and/ or the Board.

17 Policy Maintenance

17.1 The Board will ensure this Policy is reviewed at least annually and upon any material change to the Company's business, products, delivery channels, geographic footprint, applicable laws/regulations, or risk profile. The Compliance function may propose interim updates; material amendments require Board approval, while immaterial clarifications may be approved

by the MLRO and reported to the Board at the next meeting. Each review will be documented with scope, participants, findings, and actions.

17.2 The MLRO owns document control, including version numbering, change logs summarizing amendments and rationale, maintenance of prior versions in an auditable archive, and controlled distribution of the current Policy to relevant stakeholders. The Policy will state its effective date, approval authority, and version number on the cover page and footer. Access to editable formats will be restricted; a read-only version will be made available on the Company's internal policy repository.

18 Contacts

For AML/CFT queries or to report suspicious activity, contact:

Email: info@solitaireprime.com

Registered Address: Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia.

MLRO: [insert]

19 Effective Date and Approval

This Policy is effective as of [insert] and has been approved by the Board of Directors of Solitaire Prime Ltd.

Approved by: [insert] Date: [insert] Version: [insert]