ROLODEX TECHNOLOGIES

KNOW YOUR CUSTOMER (KYC)

AML POLICY

- BANK SECRECY ACT (BSA),
- ANTI-MONEY LAUNDERING (AML),
- COUNTER-TERRORIST FINANCING (CTF),
- SANCTIONS COMPLIANCE,
- CUSTOMER IDENTIFICATION PROGRAM (CIP),
- CUSTOMER DUE DILIGENCE (CDD),

- FINANCIAL CRIME PREVENTION MANUAL

ARTICLE I

DEFINITIONS, INTERPRETATION, AND REGULATORY CONSTRUCTION

Section 1.01 Purpose

This Bank Secrecy Act, Anti-Money Laundering, Counter-Terrorist Financing, Economic Sanctions, Customer Identification, Customer Due Diligence, and Financial Crime Prevention Program (the "Program") establishes the mandatory enterprise-wide framework adopted by Rolodex Technologies ("Rolodex," the "Company," "Institution," "Platform," or "Firm") for the identification, assessment, mitigation, monitoring, escalation, investigation, reporting, and prevention of money laundering, terrorist financing, sanctions violations, fraud, corruption, tax evasion, cyber-enabled financial crime, and other illicit financial activities.

This Program shall constitute the official compliance standard governing all personnel, operations, products, services, technologies, third-party relationships, subsidiaries, affiliates, and jurisdictions in which Rolodex operates.

Section 1.02 Regulatory Intent

This Program is designed to ensure that Rolodex maintains controls reasonably designed to:

(**a**) **Prevent**

Prevent the use of Rolodex ’s products, systems, services, infrastructure, software, payment rails, virtual asset services, and financial networks for unlawful purposes.

(**b**) **Detect**

Identify suspicious conduct, abnormal transactions, sanctions exposure, criminal typologies, fraud indicators, terrorist financing patterns, and other forms of financial misconduct.

(**c**) **Report**

Timely report suspicious activities, sanctions matters, regulatory violations, and other reportable events to competent governmental authorities.

(**d**) **Cooperate**

Cooperate with lawful investigations, regulatory examinations, subpoenas, court orders, production requests, and law enforcement inquiries.

Section 1.03 Regulatory Framework

This Program shall be interpreted and administered in accordance with applicable laws including, without limitation:

United States Authorities

(a) The Bank Secrecy Act (31 U.S.C. §5311 et seq.);

(b) The USA PATRIOT Act;

(c) The Anti-Money Laundering Act of 2020;

(d) FinCEN regulations;

(e) OFAC regulations;

(f) Federal Trade Commission regulations;

(g) State money transmission laws;

(h) State consumer financial protection laws;

(i) Securities laws where applicable;

(j) Virtual asset regulations where applicable.

International Authorities

(a) FATF Recommendations;

(b) Wolfsberg Principles;

(c) Basel AML Guidelines;

(d) United Nations sanctions regimes;

(e) European AML Directives;

(f) Applicable international financial crime regulations.

Section 1.04 Interpretation

The provisions of this Program shall be interpreted broadly to promote regulatory compliance, financial system integrity, and the prevention of financial crime.

Where a conflict exists between local law and this Program, Rolodex shall apply the stricter standard unless prohibited by law.

ARTICLE II

ENTERPRISE AML GOVERNANCE FRAMEWORK

Section 2.01 Board Responsibility

The Board of Directors shall bear ultimate responsibility for the effectiveness of Rolodex ′s AML and Financial Crime Compliance Program.

The Board shall:

(**a**) **Oversight**

Exercise active oversight over compliance operations.

(**b**) **Risk Appetite**

Approve Rolodex ′s AML risk appetite framework.

(**c**) **Compliance Independence**

Ensure independence of the Compliance Function.

(**d**) **Resource Allocation**

Provide sufficient financial, technological, and human resources.

(**e**) **Annual Review**

Review the effectiveness of the Program no less than annually.

Section 2.02 Chief Compliance Officer

Rolodex shall appoint a Chief Compliance Officer (“CCO”) possessing appropriate experience, qualifications, authority, and independence.

The CCO shall have unrestricted access to:

- The Board of Directors;
- Senior Management;
- Compliance records;
- Monitoring systems;
- Customer records;
- Investigation files.

Section 2.03 Authority of the CCO

The CCO shall have authority to:

(**a**)

Suspend transactions;

(**b**)

Block payments;

(**c**)

Freeze accounts;

(**d**)

Escalate suspicious activity;

(**e**)

File regulatory reports;

(**f**)

Recommend termination of customer relationships;

(**g**)

Implement emergency controls where necessary to mitigate financial crime risks.

Section 2.04 Compliance Independence

No employee, officer, shareholder, investor, director, or executive shall interfere with, obstruct, influence, compromise, or improperly direct compliance decisions.

Any attempt to do so shall constitute a material violation of Company policy.

ARTICLE III

THREE LINES OF DEFENSE FRAMEWORK

Section 3.01 First Line of Defense

Business units shall own and manage financial crime risks arising from their operations.

Responsibilities include:

(a) Customer onboarding;

(b) Data collection;

(c) Initial risk identification;

(d) Escalation of suspicious conduct;

(e) Compliance with operational procedures.

Section 3.02 Second Line of Defense

The Compliance Department shall provide:

(a) Independent oversight;

(b) Risk assessment;

(c) Monitoring;

(d) Sanctions screening;

(e) Investigations;

(f) Regulatory reporting.

Section 3.03 Third Line of Defense

Internal Audit shall independently evaluate:

(a) Program effectiveness;

(b) Regulatory compliance;

(c) Control design;

(d) Operational effectiveness;

(e) Governance maturity.

Section 3.04 Audit Independence

Internal Audit shall maintain complete independence from business operations and Compliance management.

Audit findings shall be reported directly to the Board Audit Committee.

ARTICLE IV

CUSTOMER IDENTIFICATION PROGRAM (CIP)

Section 4.01 Purpose

The Customer Identification Program ("CIP") is established to ensure that Rolodex Technologies reasonably knows the true identity of each customer, beneficial owner, authorized representative, merchant, institutional client, and counterparty with whom Rolodex establishes a business relationship.

The CIP shall constitute the first line of defense against money laundering, terrorist financing, sanctions evasion, fraud, identity theft, cyber-enabled crime, corruption, and other forms of financial misconduct.

No customer relationship shall be established unless Rolodex has obtained and verified customer identity information to the extent required under applicable laws, regulations, and internal risk management standards.

Section 4.02 Prohibition on Anonymous Accounts

Rolodex shall not knowingly:

(a) establish anonymous accounts;

(b) establish fictitious accounts;

(c) permit the use of false identities;

(d) facilitate transactions for unidentified persons;

(e) process transactions through shell identities;

(f) maintain customer relationships where identity verification cannot be completed.

Any account determined to contain false, misleading, fraudulent, or materially inaccurate identifying information may be suspended, restricted, frozen, or terminated without prior notice.

Section 4.03 Required Information – Natural Persons

Prior to account activation, Rolodex shall collect, at minimum:

(a) Identity Information

i. Full legal name;

ii. Date of birth;

iii. Nationality;

iv. Residential address;

v. Country of residence;

vi. Email address;

vii. Telephone number;

viii. Taxpayer Identification Number where required.

(b) Identification Documents

One or more valid government-issued documents including:

i. Passport;

ii. Driver's License;

iii. National Identification Card;

iv. Permanent Residence Card;

v. Government-issued identity credential acceptable to Rolodex .

Section 4.04 Documentary Verification

Rolodex may utilize documentary verification methods including:

(a) Optical character recognition;

(b) Document authenticity verification;

(c) Security feature analysis;

(d) Hologram verification;

(e) Machine-readable zone validation;

(f) Government database verification;

(g) Third-party identity verification services.

Section 4.05 Non-Documentary Verification

Rolodex may utilize non-documentary verification methods including:

(a) Biometric authentication;

(b) Facial recognition technology;

(c) Liveness detection;

(d) Device intelligence;

(e) Geolocation verification;

(f) Behavioral analytics;

(g) Public records review;

(h) Credit bureau verification;

(i) Banking relationship validation.

Section 4.06 Failure of Verification

Where Rolodex cannot reasonably verify a customer's identity, Rolodex may:

(a) deny account creation;

(b) suspend onboarding;

(c) require supplemental documentation;

(d) escalate the customer for Enhanced Due Diligence;

(e) terminate the onboarding process;

(f) report suspicious activity where required.

ARTICLE V

IDENTITY VERIFICATION STANDARDS

Section 5.01 Verification Standard

Rolodex shall maintain verification procedures reasonably designed to establish a high degree of confidence that the individual or entity seeking to establish a relationship is the true and lawful owner of the identity presented.

Verification procedures shall be risk-based and proportionate to:

(a) customer type;

(b) geographic exposure;

(c) product risk;

(d) transaction risk;

(e) delivery channel risk;

(f) sanctions risk.

Section 5.02 Biometric Verification

Where permitted by law, Rolodex may require:

(a) facial recognition matching;

(b) selfie verification;

(c) liveness testing;

(d) biometric authentication controls.

Rolodex reserves the right to reject identity submissions where biometric confidence thresholds are not satisfied.

Section 5.03 Device and Digital Identity Controls

Rolodex may collect and analyze:

(a) device identifiers;

(b) IP addresses;

(c) browser fingerprints;

(d) operating system data;

(e) network intelligence;

(f) location information;

(g) behavioral indicators.

The purpose of such controls shall be fraud prevention, identity assurance, sanctions compliance, and security monitoring.

Section 5.04 Re-Verification Requirements

Rolodex may require re-verification where:

(a) suspicious activity is detected;

(b) customer information changes materially;

(c) regulatory requirements change;

(d) account risk increases;

(e) periodic review obligations arise.

Section 5.05 Identity Fraud Escalation

Accounts presenting indicators of identity fraud shall be immediately escalated to Compliance for investigation.

Indicators may include:

(a) synthetic identities;

(b) stolen identities;

(c) forged documentation;

(d) inconsistent information;

(e) duplicate customer records;

(f) suspicious device usage.

Rolodex may immediately suspend account functionality during such investigation.

ARTICLE VI

BENEFICIAL OWNERSHIP VERIFICATION

Section 6.01 Purpose

Rolodex shall identify and verify the natural persons who ultimately own, control, or benefit from legal entities seeking access to Company services.

The purpose of beneficial ownership verification is to prevent misuse of legal structures for:

(a) money laundering;

(b) terrorist financing;

(c) sanctions evasion;

(d) tax evasion;

(e) corruption;

(f) concealment of criminal proceeds.

Section 6.02 Ownership Threshold

Unless a stricter standard is required by law, Rolodex shall identify each natural person who:

(a) directly owns twenty-five percent (25%) or more of a legal entity; or

(b) indirectly owns twenty-five percent (25%) or more of a legal entity; or

(c) exercises substantial control over the legal entity.

Rolodex may apply lower ownership thresholds where risk considerations warrant.

Section 6.03 Beneficial Ownership Information

Rolodex may require:

(a) ownership charts;

(b) shareholder registers;

(c) articles of incorporation;

(d) certificates of formation;

(e) partnership agreements;

(f) trust documentation;

(g) operating agreements;

(h) board resolutions.

Section 6.04 Complex Ownership Structures

Enhanced review shall be required where ownership structures involve:

(a) offshore entities;

(b) nominee shareholders;

(c) bearer shares;

(d) trusts;

(e) foundations;

(f) layered ownership arrangements;

(g) shell companies.

Rolodex reserves the right to reject ownership structures that prevent transparent identification of ultimate beneficial owners.

Section 6.05 Ongoing Ownership Monitoring

Customers shall promptly notify Rolodex of material changes in ownership or control.

Rolodex may periodically request updated ownership documentation.

Failure to cooperate may result in account restriction or termination.

ARTICLE VII

CUSTOMER DUE DILIGENCE (CDD)

Section 7.01 General Requirement

Rolodex shall conduct Customer Due Diligence sufficient to understand:

(a) customer identity;

(b) business purpose;

(c) expected account activity;

(d) source of funds;

(e) source of wealth where applicable;

(f) customer risk profile.

Section 7.02 Nature and Purpose of Relationship

Rolodex shall seek to understand:

(a) reasons for account opening;

(b) expected transaction activity;

(c) anticipated transaction volumes;

(d) anticipated transaction frequency;

(e) geographic activity;

(f) intended products and services.

Section 7.03 Customer Risk Assessment

Each customer shall be assigned a risk rating.

Risk classifications may include:

Low Risk

Customers presenting minimal financial crime exposure.

Medium Risk

Customers presenting moderate financial crime exposure.

High Risk

Customers presenting elevated financial crime exposure.

Prohibited Risk

Customers presenting unacceptable risk.

Rolodex reserves sole discretion in assigning risk classifications.

Section 7.04 Source of Funds

Rolodex may require evidence demonstrating the lawful origin of funds including:

(a) payroll records;

(b) tax filings;

(c) bank statements;

(d) business revenue reports;

(e) investment records;

(f) inheritance records;

(g) property sale records.

Section 7.05 Ongoing Due Diligence

Rolodex shall conduct ongoing due diligence throughout the customer relationship.

Monitoring may include:

(a) transaction reviews;

(b) sanctions screening;

(c) adverse media screening;

(d) behavioral analysis;

(e) periodic KYC refreshes.

Section 7.06 Periodic Reviews

Customer reviews shall occur according to risk level.

Low Risk

At intervals determined by Compliance.

Medium Risk

More frequent review cycles.

High Risk

Enhanced periodic review schedules.

Compliance may accelerate review requirements where warranted.

ARTICLE VIII

ENHANCED DUE DILIGENCE AND POLITICALLY EXPOSED PERSONS (PEPs)

Section 8.01 Enhanced Due Diligence Requirement

Enhanced Due Diligence ("EDD") shall be applied where elevated financial crime risks are identified.

EDD shall supplement, and not replace, standard Customer Due Diligence procedures.

Section 8.02 High-Risk Customer Categories

EDD may be required for:

(a) Politically Exposed Persons;

(b) senior government officials;

(c) state-owned enterprise executives;

(d) family members of PEPs;

(e) close associates of PEPs;

(f) customers from high-risk jurisdictions;

(g) cryptocurrency-intensive businesses;

(h) money service businesses;

(i) correspondent relationships;

(j) cash-intensive businesses.

Section 8.03 Politically Exposed Persons

For purposes of this Program, a Politically Exposed Person includes:

(a) current heads of state;

(b) current heads of government;

(c) cabinet ministers;

(d) senior military officials;

(e) senior judicial officials;

(f) senior political party officials;

(g) executives of state-owned enterprises;

(h) equivalent foreign officials.

Section 8.04 PEP Risk Assessment

Rolodex shall evaluate:

(a) political exposure;

(b) corruption risk;

(c) geographic risk;

(d) source of wealth;

(e) source of funds;

(f) sanctions exposure;

(g) adverse media findings.

Section 8.05 Additional EDD Measures

Rolodex may require:

(a) senior management approval;

(b) enhanced identity verification;

(c) detailed source of wealth analysis;

(d) tax documentation;

(e) independent intelligence reports;

(f) enhanced transaction monitoring;

(g) recurring reviews.

Section 8.06 Source of Wealth Verification

Where deemed necessary, customers may be required to provide evidence demonstrating the legitimate origin of accumulated wealth.

Documentation may include:

(a) audited financial statements;

(b) business ownership records;

(c) inheritance documentation;

(d) investment records;

(e) employment contracts;

(f) asset sale agreements.

Section 8.07 Exit and Relationship Termination

Rolodex reserves the unrestricted right to decline, suspend, restrict, freeze, or terminate any customer relationship where:

(a) risks cannot be adequately mitigated;

(b) beneficial ownership cannot be determined;

(c) source of funds cannot be verified;

(d) sanctions concerns arise;

(e) regulatory obligations require action;

(f) financial crime risks exceed Rolodex ′s approved risk appetite.

Such action may be taken without prior notice where legally permissible.

ARTICLE IX

CUSTOMER RISK RATING METHODOLOGY

Section 9.01 Purpose

Rolodex shall maintain a documented, risk-based Customer Risk Rating Methodology designed to identify, assess, quantify, monitor, and mitigate financial crime risks associated with each customer relationship.

The Risk Rating Program shall form a core component of Rolodex ′s Enterprise-Wide Anti-Money Laundering, Counter-Terrorist Financing, Sanctions Compliance, and Financial Crime Risk Management Framework.

Section 9.02 Risk-Based Approach

Rolodex shall apply a risk-based approach consistent with regulatory expectations and international best practices.

Risk classifications shall be assigned based upon the totality of information available to Rolodex .

Risk assessments shall consider both quantitative and qualitative factors.

Section 9.03 Customer Risk Factors

Rolodex shall evaluate multiple risk indicators including:

(a) Customer Type Risk

Including:

i. Individual customers;

ii. Business customers;

iii. Trusts;

iv. Foundations;

v. Non-profit organizations;

vi. Money services businesses;

vii. Financial institutions;

viii. Virtual asset service providers.

(b) Geographic Risk

Including:

i. Country of residence;

ii. Country of incorporation;

iii. Transaction corridors;

iv. Jurisdictions subject to sanctions;

v. High-risk jurisdictions identified by international authorities.

(c) Product Risk

Including:

i. Cryptocurrency services;

ii. Stablecoin services;

iii. International remittances;

iv. Cross-border payments;

v. Peer-to-peer transfers;

vi. High-value payment services.

(d) Transaction Risk

Including:

i. Expected transaction volumes;

ii. Transaction frequency;

iii. Velocity indicators;

iv. Unusual activity patterns.

Section 9.04 Risk Classifications

Customers shall be assigned one of the following classifications:

Tier I – Low Risk

Customers presenting minimal exposure to financial crime.

Tier II – Moderate Risk

Customers presenting manageable financial crime exposure.

Tier III – High Risk

Customers presenting elevated financial crime exposure requiring Enhanced Due Diligence.

Tier IV – Prohibited Risk

Customers presenting unacceptable risk exposure.

Relationships classified as Prohibited Risk shall not be onboarded or maintained.

Section 9.05 Dynamic Risk Reassessment

Customer risk ratings shall be reviewed and updated whenever:

(a) material information changes;

(b) suspicious activity is detected;

(c) ownership changes occur;

(d) sanctions concerns arise;

(e) adverse media emerges;

(f) regulatory requirements change.

Section 9.06 Compliance Authority

Compliance shall possess sole authority to:

(a) assign risk ratings;

(b) elevate risk classifications;

(c) impose restrictions;

(d) require Enhanced Due Diligence;

(e) recommend relationship termination.

Business units shall not override compliance risk determinations.

ARTICLE X

SANCTIONS COMPLIANCE PROGRAM

Section 10.01 Purpose

Rolodex shall maintain a comprehensive Economic Sanctions Compliance Program designed to prevent the use of Company products, services, platforms, systems, technologies, and infrastructure by sanctioned individuals, entities, vessels, jurisdictions, organizations, or networks.

Section 10.02 Zero-Tolerance Standard

Rolodex maintains a zero-tolerance policy regarding violations of applicable sanctions laws.

No employee, officer, contractor, affiliate, customer, vendor, or third party may knowingly engage in conduct intended to evade sanctions controls.

Section 10.03 Sanctions Authorities

Rolodex's sanctions framework shall consider restrictions issued by:

United States

(a) Office of Foreign Assets Control (OFAC);

International Authorities

(b) United Nations;

(c) European Union;

(d) United Kingdom;

(e) Other applicable governmental authorities.

Section 10.04 Sanctions Risk Management

Rolodex shall maintain controls reasonably designed to identify:

(a) sanctioned persons;

(b) sanctioned entities;

(c) blocked property;

(d) embargoed jurisdictions;

(e) sanctioned virtual asset addresses;

(f) sanctions evasion schemes.

Section 10.05 Enterprise Screening Obligation

Rolodex shall screen:

(a) customers;

(b) beneficial owners;

(c) authorized signatories;

(d) counterparties;

(e) merchants;

(f) vendors;

(g) employees;

(h) directors.

Screening shall occur prior to establishing a relationship and periodically thereafter.

Section 10.06 Sanctions Escalation

Potential sanctions matches shall be escalated immediately to Compliance for review.

No transaction shall proceed while a sanctions investigation remains unresolved.

ARTICLE XI

OFAC COMPLIANCE PROCEDURES

Section 11.01 OFAC Program

Rolodex shall maintain procedures reasonably designed to comply with regulations administered by the Office of Foreign Assets Control.

Section 11.02 Blocking and Rejection Authority

Where required by law, Rolodex may:

(a) block assets;

(b) reject transactions;

(c) suspend accounts;

(d) freeze funds;

(e) restrict platform access.

Rolodex may implement such measures without prior notice.

Section 11.03 Restricted Jurisdictions

Rolodex reserves the right to prohibit activity involving jurisdictions deemed:

(a) comprehensively sanctioned;

(b) embargoed;

(c) prohibited by law;

(d) otherwise unacceptable from a sanctions risk perspective.

Section 11.04 OFAC Investigations

Compliance shall investigate potential sanctions matters by reviewing:

(a) customer records;

(b) beneficial ownership information;

(c) transaction history;

(d) blockchain analytics;

(e) geolocation data;

(f) adverse media.

Section 11.05 Reporting Obligations

Where legally required, Rolodex shall submit reports to appropriate authorities regarding:

(a) blocked property;

(b) rejected transactions;

(c) sanctions-related activity;

(d) other reportable matters.

Section 11.06 Voluntary Self-Disclosure

Rolodex reserves the right to voluntarily disclose potential sanctions violations to applicable authorities where deemed appropriate by Compliance and legal counsel.

ARTICLE XII

WATCHLIST SCREENING CONTROLS

Section 12.01 Screening Framework

Rolodex shall maintain automated screening systems designed to identify potential matches against:

(a) sanctions lists;

(b) terrorist lists;

(c) law enforcement lists;

(d) politically exposed persons databases;

(e) adverse media sources;

(f) internal watchlists.

Section 12.02 Screening Frequency

Screening may occur:

(a) at onboarding;

(b) daily;

(c) in real time;

(d) before transactions;

(e) after profile changes;

(f) during periodic reviews.

Section 12.03 Fuzzy Matching Controls

Rolodex may utilize advanced matching methodologies including:

(a) exact matching;

(b) phonetic matching;

(c) transliteration matching;

(d) fuzzy logic screening;

(e) artificial intelligence-assisted screening.

Section 12.04 Alert Review Procedures

Potential matches shall be reviewed by qualified compliance personnel.

Investigations shall consider:

(a) date of birth;

(b) nationality;

(c) geographic indicators;

(d) ownership information;

(e) transaction data;

(f) supporting documentation.

Section 12.05 False Positive Resolution

Where a potential match is determined not to represent a true match:

(a) the basis for resolution shall be documented;

(b) evidence supporting the determination shall be retained;

(c) approval shall be obtained from authorized compliance personnel.

Section 12.06 True Match Escalation

Where a true match is identified:

(a) Compliance shall immediately escalate the matter;

(b) account restrictions may be imposed;

(c) transactions may be blocked;

(d) reporting obligations shall be evaluated.

ARTICLE XIII

HIGH-RISK JURISDICTIONS, ANTI-BRIBERY, AND ANTI-CORRUPTION CONTROLS

Section 13.01 High-Risk Jurisdictions

Rolodex shall maintain a risk-based framework for identifying jurisdictions presenting elevated exposure to:

(a) money laundering;

(b) terrorist financing;

(c) corruption;

(d) sanctions evasion;

(e) organized crime;

(f) regulatory deficiencies.

Section 13.02 Jurisdictional Risk Assessment

Risk assessments shall consider:

(a) FATF findings;

(b) sanctions exposure;

(c) corruption indices;

(d) law enforcement cooperation levels;

(e) financial transparency standards.

Section 13.03 Enhanced Controls

Customers connected to high-risk jurisdictions may be subject to:

(a) Enhanced Due Diligence;

(b) source-of-funds verification;

(c) source-of-wealth verification;

(d) transaction restrictions;

(e) senior management approval.

Section 13.04 Anti-Bribery Commitment

Rolodex prohibits bribery, corruption, kickbacks, facilitation payments, improper inducements, and any conduct intended to improperly influence decision-making.

This prohibition applies globally regardless of local custom or business practice.

Section 13.05 Prohibited Conduct

No employee, officer, contractor, consultant, agent, representative, or third party acting on behalf of Rolodex shall:

(a) offer bribes;

(b) solicit bribes;

(c) authorize bribes;

(d) receive bribes;

(e) disguise improper payments;

(f) create false records.

Section 13.06 Gifts and Entertainment

Gifts, hospitality, travel, entertainment, sponsorships, and charitable contributions shall be:

(a) lawful;

(b) reasonable;

(c) proportionate;

(d) accurately recorded;

(e) approved where required.

Any item capable of creating an appearance of impropriety shall be prohibited.

Section 13.07 Third-Party Due Diligence

Rolodex shall conduct risk-based due diligence on:

(a) agents;

(b) consultants;

(c) intermediaries;

(d) business partners;

(e) vendors;

(f) referral partners.

Rolodex reserves the right to terminate relationships presenting unacceptable corruption risks.

Section 13.08 Books and Records Controls

Rolodex shall maintain complete and accurate books, records, and accounts.

No person may:

(a) create false entries;

(b) conceal transactions;

(c) maintain off-book accounts;

(d) falsify documentation.

Section 13.09 Reporting and Whistleblower Protection

Employees shall promptly report suspected violations.

Rolodex prohibits retaliation against any individual who, in good faith:

(a) reports misconduct;

(b) participates in an investigation;

(c) cooperates with compliance reviews.

Section 13.10 Enforcement Authority

Violations of this Article may result in:

(a) disciplinary action;

(b) suspension;

(c) termination of employment;

(d) termination of business relationships;

(e) referral to regulatory authorities;

(f) referral to law enforcement agencies.

Rolodex reserves all rights available under law to pursue corrective, remedial, and enforcement actions.

ARTICLE XIV

TRANSACTION MONITORING PROGRAM

Section 14.01 Purpose

Rolodex shall maintain a comprehensive Transaction Monitoring Program ("TMP") reasonably designed to detect, investigate, escalate, and report potentially suspicious, unusual, fraudulent, prohibited, or unlawful activity occurring through Rolodex ′s products, services, systems, platforms, payment networks, and virtual asset infrastructure.

The Transaction Monitoring Program shall operate on a risk-based basis and shall form a core component of Rolodex ′s enterprise-wide financial crime compliance framework.

Section 14.02 Monitoring Framework

Rolodex shall maintain automated and manual monitoring controls designed to identify:

(a) money laundering indicators;

(b) terrorist financing indicators;

(c) sanctions evasion activity;

(d) fraud typologies;

(e) suspicious cryptocurrency activity;

(f) structuring behavior;

(g) unusual transaction patterns;

(h) account takeover activity;

(i) mule account activity;

(j) cybercrime proceeds.

Section 14.03 Monitoring Coverage

Monitoring controls shall apply to:

(a) deposits;

(b) withdrawals;

(c) peer-to-peer transfers;

(d) remittances;

(e) merchant payments;

(f) cryptocurrency transfers;

(g) stablecoin transactions;

(h) fiat currency transactions;

(i) internal transfers;

(j) cross-border transactions.

Section 14.04 Automated Monitoring Systems

Rolodex may utilize automated transaction monitoring systems incorporating:

(a) rules-based detection;

(b) behavioral analytics;

(c) machine learning models;

(d) risk scoring methodologies;

(e) anomaly detection technologies;

(f) artificial intelligence-assisted investigations.

Section 14.05 Alert Generation

Transaction monitoring alerts may be generated based upon:

(a) transaction size;

(b) transaction frequency;

(c) velocity thresholds;

(d) geographic exposure;

(e) customer risk classification;

(f) sanctions exposure;

(g) blockchain intelligence indicators;

(h) typology detection rules.

Section 14.06 Alert Review Procedures

All alerts shall be reviewed by appropriately trained personnel.

Reviews shall consider:

(a) customer profile information;

(b) transaction history;

(c) source of funds information;

(d) prior investigations;

(e) adverse media findings;

(f) sanctions screening results.

Section 14.07 Escalation Matrix

Where suspicious activity is identified, alerts shall be escalated according to established escalation procedures.

Escalation levels may include:

Level I

Compliance Analyst Review

Level II

Senior Compliance Review

Level III

Financial Crime Investigation

Level IV

Chief Compliance Officer Review

Level V

Regulatory Reporting Determination

Section 14.08 Risk-Based Restrictions

Rolodex may impose:

(a) transaction limits;

(b) withdrawal restrictions;

(c) account freezes;

(d) enhanced monitoring requirements;

(e) relationship termination measures.

ARTICLE XV

CRYPTOCURRENCY AND BLOCKCHAIN AML CONTROLS

Section 15.01 Purpose

Rolodex shall maintain specialized controls addressing risks associated with virtual assets, cryptocurrencies, stablecoins, decentralized finance exposure, blockchain networks, and digital asset transactions.

Section 15.02 Blockchain Analytics Program

Rolodex may utilize blockchain intelligence solutions to identify:

(a) darknet market exposure;

(b) sanctioned wallet activity;

(c) ransomware proceeds;

(d) fraud schemes;

(e) stolen asset activity;

(f) mixer usage;

(g) tumbling services;

(h) terrorist financing indicators;

(i) illicit marketplace exposure.

Section 15.03 Wallet Screening Controls

Rolodex shall screen blockchain addresses prior to processing transactions where technologically feasible.

Screening may include:

(a) sender wallet review;

(b) beneficiary wallet review;

(c) intermediary wallet review;

(d) transaction path analysis.

Section 15.04 Blockchain Risk Scoring

Rolodex may assign risk ratings to:

(a) blockchain addresses;

(b) counterparties;

(c) token transactions;

(d) smart contract interactions.

Risk scoring may consider:

(i) historical activity;

(ii) sanctions exposure;

(iii) illicit activity indicators;

(iv) transaction patterns.

Section 15.05 Prohibited Blockchain Activity

Rolodex may prohibit transactions involving:

(a) sanctioned wallets;

(b) terrorist financing indicators;

(c) ransomware wallets;

(d) stolen funds;

(e) darknet marketplaces;

(f) criminal organizations.

Section 15.06 Stablecoin Controls

Rolodex may implement enhanced controls for stablecoin transactions involving:

(a) high-risk jurisdictions;

(b) large-value transfers;

(c) rapid movement of funds;

(d) layering indicators.

Section 15.07 Decentralized Finance Exposure

Rolodex reserves the right to restrict, limit, review, or prohibit activity involving decentralized finance protocols where compliance risks cannot be adequately assessed or mitigated.

ARTICLE XVI

TRAVEL RULE COMPLIANCE PROGRAM

Section 16.01 Purpose

Rolodex shall maintain policies, procedures, systems, and controls designed to comply with applicable funds transfer, virtual asset transfer, and Travel Rule obligations.

Section 16.02 Information Collection

Where required by law, Rolodex shall collect and transmit information concerning:

(a) originators;

(b) beneficiaries;

(c) account identifiers;

(d) wallet identifiers;

(e) transaction details.

Section 16.03 Verification Standards

Rolodex shall take reasonable steps to verify the accuracy of Travel Rule information prior to transmission.

Section 16.04 Counterparty Compliance Assessment

Rolodex may assess whether counterpart institutions maintain adequate Travel Rule controls.

Factors may include:

(a) regulatory status;

(b) compliance maturity;

(c) licensing status;

(d) jurisdictional risk.

Section 16.05 Incomplete Information

Rolodex reserves the right to:

(a) reject transfers;

(b) delay transfers;

(c) suspend processing;

(d) request additional information;

(e) report suspicious activity.

where required information is missing, incomplete, inaccurate, or unverifiable.

Section 16.06 Recordkeeping

Travel Rule records shall be retained in accordance with applicable legal and regulatory requirements.

ARTICLE XVII

SUSPICIOUS ACTIVITY REPORTING (SAR)

Section 17.01 Policy Statement

Rolodex shall maintain procedures reasonably designed to identify, investigate, document, escalate, and report suspicious activity in accordance with applicable laws and regulations.

Section 17.02 Reportable Activity

Potentially reportable activity may include:

(a) money laundering;

(b) terrorist financing;

(c) sanctions evasion;

(d) fraud;

(e) cybercrime proceeds;

(f) corruption;

(g) tax evasion;

(h) identity theft;

(i) structuring;

(j) suspicious cryptocurrency activity.

Section 17.03 Internal Escalation

Employees shall immediately report suspicious conduct to Compliance.

Failure to report known suspicious activity may constitute a violation of Company policy.

Section 17.04 SAR Investigation Procedures

Compliance personnel shall evaluate:

(a) customer information;

(b) transaction history;

(c) source of funds information;

(d) blockchain intelligence;

(e) sanctions screening results;

(f) adverse media findings.

Section 17.05 SAR Determination Authority

Only authorized compliance personnel designated by the Chief Compliance Officer may determine whether a SAR filing is warranted.

Section 17.06 Confidentiality

Information concerning SAR investigations shall be strictly confidential.

No employee shall disclose:

(a) the existence of a SAR;

(b) the possibility of a SAR filing;

(c) an ongoing SAR investigation.

Unauthorized disclosure may result in disciplinary action and legal consequences.

Section 17.07 Documentation Requirements

Rolodex shall maintain records supporting:

(a) investigative findings;

(b) analytical conclusions;

(c) escalation decisions;

(d) filing determinations.

Section 17.08 Relationship Management

The filing of a SAR shall not automatically require account closure.

Rolodex shall evaluate:

(a) legal obligations;

(b) regulatory expectations;

(c) financial crime risks;

(d) operational considerations.

when determining whether a relationship should continue.

ARTICLE XVIII

CURRENCY TRANSACTION REPORTING AND FINANCIAL CRIME INVESTIGATIONS

Section 18.01 Currency Transaction Reporting Program

Rolodex shall maintain procedures designed to identify and report currency transactions where reporting obligations arise under applicable law.

Section 18.02 Structuring Detection

Rolodex shall maintain controls designed to identify:

(a) structuring;

(b) smurfing;

(c) threshold avoidance behavior;

(d) unusual cash activity.

Indicators may include multiple transactions conducted for the apparent purpose of evading reporting requirements.

Section 18.03 Financial Crime Investigations Unit

Rolodex shall maintain a Financial Crime Investigations Function responsible for:

(a) complex investigations;

(b) suspicious activity analysis;

(c) fraud investigations;

(d) sanctions investigations;

(e) cryptocurrency investigations;

(f) law enforcement coordination.

Section 18.04 Investigation Authority

Investigators may review:

(a) account records;

(b) transaction records;

(c) customer communications;

(d) blockchain analytics;

(e) device intelligence;

(f) identity documentation.

subject to applicable law and internal controls.

Section 18.05 Investigation Case Management

Each investigation shall be documented within an approved case management system.

Records shall include:

(a) allegations;

(b) evidence reviewed;

(c) investigative actions;

(d) findings;

(e) recommendations;

(f) disposition.

Section 18.06 Law Enforcement Cooperation

Rolodex may cooperate with:

(a) law enforcement agencies;

(b) regulatory authorities;

(c) financial intelligence units;

(d) judicial authorities.

to the extent permitted or required by law.

Section 18.07 Legal Holds

Where appropriate, Rolodex may preserve records, accounts, transactions, and evidence relevant to ongoing investigations.

Section 18.08 Account Freezes and Restrictions

Rolodex reserves the right to:

(a) restrict transactions;

(b) freeze assets;

(c) suspend services;

(d) terminate accounts;

(e) reject payments.

where necessary to comply with legal obligations or mitigate financial crime risk.

Section 18.09 Enterprise Reporting

The Chief Compliance Officer shall periodically provide reports to senior management and the Board concerning:

(a) monitoring activity;

(b) investigations;

(c) SAR filings;

(d) sanctions matters;

(e) emerging risks;

(f) program effectiveness.

Section 18.10 Regulatory Cooperation

Nothing in this Program shall prohibit Rolodex from voluntarily cooperating with governmental authorities regarding actual or suspected violations of law.

Such cooperation may include information sharing, reporting, production of records, and participation in lawful investigations.

ARTICLE XIX

CORRESPONDENT BANKING, PAYMENT PARTNER, AND THIRD-PARTY DUE DILIGENCE PROGRAM

Section 19.01 Purpose

Rolodex shall maintain a comprehensive Correspondent Banking, Payment Partner, Banking-as-a-Service ("BaaS"), Financial Institution, Virtual Asset Service Provider ("VASP"), and Third-Party Due Diligence Program designed to identify, assess, monitor, and mitigate financial crime, sanctions, operational, regulatory, legal, and reputational risks associated with third-party relationships.

No third-party relationship shall be established without completion of risk-based due diligence procedures.

Section 19.02 Risk Assessment Requirements

Prior to onboarding a third party, Rolodex shall evaluate:

(a) regulatory status;

(b) licensing status;

(c) ownership structure;

(d) beneficial ownership;

(e) AML program maturity;

(f) sanctions controls;

(g) fraud controls;

(h) cybersecurity posture;

(i) geographic exposure;

(j) financial condition.

Section 19.03 Prohibited Relationships

Rolodex shall not knowingly establish or maintain relationships with:

(a) shell banks;

(b) unlicensed financial institutions;

(c) sanctioned entities;

(d) prohibited virtual asset service providers;

(e) organizations lacking adequate compliance controls.

Section 19.04 Enhanced Due Diligence

Enhanced Due Diligence shall be required for:

(a) correspondent banking relationships;

(b) foreign financial institutions;

(c) cryptocurrency exchanges;

(d) payment aggregators;

(e) remittance partners;

(f) high-risk jurisdictions.

Section 19.05 Ongoing Monitoring

Third-party relationships shall be subject to periodic review.

Monitoring may include:

(a) sanctions screening;

(b) adverse media review;

(c) regulatory action monitoring;

(d) licensing verification;

(e) transaction reviews;

(f) compliance certifications.

Section 19.06 Right to Audit

Rolodex reserves the right to conduct compliance audits, request certifications, obtain supporting documentation, and terminate relationships where risk levels become unacceptable.

ARTICLE XX

MERCHANT RISK MANAGEMENT PROGRAM

Section 20.01 Purpose

Rolodex shall maintain a Merchant Risk Management Program reasonably designed to identify, evaluate, mitigate, and monitor risks associated with merchant customers and commercial payment activity.

Section 20.02 Merchant Due Diligence

Prior to onboarding, Rolodex shall assess:

(a) ownership structure;

(b) business model;

(c) products and services;

(d) expected transaction activity;

(e) customer base;

(f) jurisdictions served;

(g) compliance history.

Section 20.03 High-Risk Merchant Categories

Enhanced review may be required for merchants operating in sectors presenting elevated risk.

Such categories may include:

(a) money services;

(b) virtual asset businesses;

(c) cross-border commerce;

(d) high-volume digital services;

(e) industries identified by Compliance as elevated risk.

Section 20.04 Merchant Monitoring

Merchant activity shall be monitored for:

(a) unusual transaction patterns;

(b) excessive chargebacks;

(c) fraud indicators;

(d) sanctions concerns;

(e) suspicious customer behavior.

Section 20.05 Merchant Restrictions

Rolodex reserves the right to:

(a) impose reserve requirements;

(b) establish transaction limits;

(c) delay settlements;

(d) suspend payment processing;

(e) terminate merchant services.

ARTICLE XXI

ENTERPRISE FRAUD PREVENTION PROGRAM

Section 21.01 Purpose

Rolodex shall maintain a comprehensive Enterprise Fraud Prevention Program designed to detect, prevent, investigate, and mitigate fraud across all products, services, systems, customers, employees, and third-party relationships.

Section 21.02 Fraud Risk Categories

Rolodex shall maintain controls addressing:

(a) identity fraud;

(b) account takeover fraud;

(c) payment fraud;

(d) synthetic identity fraud;

(e) insider fraud;

(f) merchant fraud;

(g) cyber-enabled fraud;

(h) cryptocurrency fraud;

(i) social engineering schemes.

Section 21.03 Fraud Detection Controls

Rolodex may utilize:

(a) device intelligence;

(b) behavioral analytics;

(c) geolocation monitoring;

(d) transaction monitoring;

(e) biometric authentication;

(f) machine learning models;

(g) fraud scoring systems.

Section 21.04 Multi-Factor Authentication

Rolodex may require multi-factor authentication for:

(a) account access;

(b) password changes;

(c) withdrawals;

(d) profile modifications;

(e) high-risk transactions.

Section 21.05 Fraud Investigations

Fraud investigations shall be documented and conducted by qualified personnel.

Investigations may include:

(a) account reviews;

(b) device analysis;

(c) transaction tracing;

(d) blockchain analytics;

(e) customer interviews.

Section 21.06 Fraud Escalation Authority

Rolodex may:

(a) freeze accounts;

(b) block transactions;

(c) suspend access;

(d) recover assets where lawful;

(e) refer matters to law enforcement.

ARTICLE XXII

RECORDKEEPING AND RECORD RETENTION PROGRAM

Section 22.01 Policy Statement

Rolodex shall maintain complete, accurate, reliable, and accessible records sufficient to demonstrate compliance with applicable laws, regulations, contractual obligations, and internal policies.

Section 22.02 Records Subject to Retention

Records may include:

(a) customer identification records;

(b) due diligence documentation;

(c) transaction records;

(d) sanctions investigations;

(e) SAR-related documentation;

(f) fraud investigations;

(g) audit reports;

(h) compliance certifications;

(i) training records.

Section 22.03 Retention Period

Records shall be retained for the period required by applicable law and regulatory requirements.

Where multiple retention periods apply, the longest applicable period shall govern.

Section 22.04 Integrity Controls

Rolodex shall maintain controls designed to ensure:

(a) completeness;

(b) accuracy;

(c) authenticity;

(d) accessibility;

(e) recoverability.

Section 22.05 Legal Holds

Rolodex may suspend routine destruction schedules where records become relevant to:

(a) litigation;

(b) investigations;

(c) regulatory examinations;

(d) enforcement proceedings.

Section 22.06 Destruction Standards

When destruction is permitted, records shall be destroyed securely and in accordance with approved retention procedures.

ARTICLE XXIII

EMPLOYEE SCREENING, TRAINING, AND COMPLIANCE CERTIFICATION

Section 23.01 Employment Screening Program

Rolodex shall maintain a risk-based employee screening program.

Screening may include:

(a) identity verification;

(b) employment verification;

(c) education verification;

(d) professional licensing review;

(e) sanctions screening;

(f) criminal background checks where permitted by law.

Section 23.02 Fitness and Integrity Requirements

Employees occupying compliance-sensitive positions shall demonstrate integrity, competence, professionalism, and fitness for assigned responsibilities.

Section 23.03 Mandatory Compliance Training

Employees shall complete mandatory training:

(a) upon hire;

(b) annually thereafter;

(c) following material regulatory changes;

(d) upon reassignment to compliance-sensitive functions.

Section 23.04 Training Topics

Training may include:

(a) AML requirements;

(b) sanctions compliance;

(c) fraud prevention;

(d) anti-corruption obligations;

(e) cybersecurity awareness;

(f) suspicious activity reporting;

(g) data privacy requirements.

Section 23.05 Role-Based Training

Additional specialized training shall be provided to:

(a) compliance personnel;

(b) executives;

(c) investigators;

(d) customer support personnel;

(e) merchant operations teams;

(f) technology personnel.

Section 23.06 Employee Certifications

Employees may be required to certify periodically that they:

(a) understand Company policies;

(b) completed required training;

(c) complied with applicable obligations;

(d) disclosed conflicts of interest.

ARTICLE XXIV

INDEPENDENT TESTING, INTERNAL AUDIT, AND REGULATORY EXAMINATION MANAGEMENT

Section 24.01 Independent Testing Requirement

Rolodex shall maintain an independent testing function designed to evaluate the adequacy and effectiveness of the AML, sanctions, fraud prevention, and compliance programs.

Section 24.02 Scope of Independent Testing

Reviews may evaluate:

(a) governance effectiveness;

(b) policy compliance;

(c) transaction monitoring controls;

(d) sanctions screening controls;

(e) investigation procedures;

(f) reporting obligations;

(g) third-party risk controls.

Section 24.03 Auditor Independence

Independent testing shall be conducted by personnel possessing sufficient expertise, authority, and independence from the functions being reviewed.

Section 24.04 Internal Audit Authority

Internal Audit shall have unrestricted access to:

(a) records;

(b) systems;

(c) personnel;

(d) investigations;

(e) compliance files;

(f) Board-approved policies.

Section 24.05 Findings and Remediation

Audit findings shall be:

(a) documented;

(b) risk-rated;

(c) communicated to management;

(d) tracked to resolution.

Management shall implement timely corrective action plans.

Section 24.06 Audit Committee Reporting

Material audit findings shall be reported to the Board Audit Committee.

Reports may include:

(a) significant deficiencies;

(b) control failures;

(c) regulatory concerns;

(d) remediation progress.

Section 24.07 Model Validation

Rolodex shall maintain governance controls over compliance models, risk scoring systems, fraud detection engines, and monitoring systems.

Validation may assess:

(a) effectiveness;

(b) accuracy;

(c) calibration;

(d) performance;

(e) reliability.

Section 24.08 Regulatory Examination Readiness

Rolodex shall maintain procedures designed to facilitate regulatory examinations, inspections, audits, and inquiries.

Such procedures may include:

(a) document management protocols;

(b) examination response teams;

(c) regulatory communication procedures;

(d) evidence preservation requirements.

Section 24.09 Regulatory Cooperation

Rolodex shall cooperate with lawful examinations conducted by competent regulatory authorities.

Such cooperation may include:

(a) production of records;

(b) management interviews;

(c) system demonstrations;

(d) remediation reporting.

Section 24.10 Board Oversight

The Board of Directors shall receive periodic reports regarding:

(a) audit results;

(b) regulatory examinations;

(c) remediation status;

(d) control effectiveness;

(e) emerging compliance risks.

The Board shall exercise oversight sufficient to ensure the continued effectiveness of Rolodex ′s compliance framework.

ARTICLE XXV

REGULATORY REPORTING, GOVERNMENT REQUESTS, INFORMATION SHARING, AND LEGAL PROCESS MANAGEMENT

Section 25.01 Policy Statement

Rolodex shall maintain policies, procedures, systems, controls, governance standards, and reporting mechanisms reasonably designed to ensure timely, accurate, complete, and legally compliant responses to regulatory obligations, governmental inquiries, supervisory requests, law

enforcement investigations, judicial proceedings, and other legally authorized information requests.

Rolodex shall cooperate with competent authorities to the extent required or permitted by applicable law while preserving customer privacy rights, legal privileges, confidentiality obligations, and data protection requirements.

Section 25.02 Regulatory Reporting Obligations

Rolodex shall maintain procedures governing the identification, preparation, approval, submission, correction, and retention of regulatory reports including but not limited to:

(**a**)

Suspicious Activity Reports;

(**b**)

Currency Transaction Reports;

(**c**)

Sanctions-related reports;

(**d**)

Blocked property reports;

(**e**)

Money transmitter reports;

(**f**)

Virtual asset reporting obligations;

(**g**)

Regulatory examination responses;

(**h**)

Consumer protection reports;

(**i**)

Financial crime disclosures;

(**j**)

Other legally mandated submissions.

Section 25.03 Government Requests

Government requests may include:

(a) subpoenas;

(b) summonses;

(c) court orders;

(d) search warrants;

(e) administrative requests;

(f) regulatory inquiries;

(g) production demands;

(h) law enforcement requests.

All requests shall be reviewed by Compliance and Legal before response unless immediate action is required by law.

Section 25.04 Information Sharing

Rolodex may participate in lawful information-sharing programs designed to combat:

(a) money laundering;

(b) terrorist financing;

(c) sanctions evasion;

(d) fraud;

(e) cybercrime;

(f) organized crime;

(g) human trafficking.

Section 25.05 Preservation Requirements

Upon receipt of notice of investigation, examination, litigation, enforcement action, or governmental inquiry, Rolodex may implement immediate legal hold procedures.

No employee may alter, conceal, destroy, modify, delete, remove, or otherwise compromise information subject to a legal hold.

Section 25.06 Regulatory Notification Events

The Chief Compliance Officer shall determine whether material events require notification to regulators.

Events may include:

(a) material compliance failures;

(b) significant sanctions violations;

(c) data breaches;

(d) financial crime events;

(e) enforcement actions;

(f) licensing matters.

ARTICLE XXVI

DATA PROTECTION, PRIVACY, CONFIDENTIALITY, AND INFORMATION SECURITY

Section 26.01 Policy Statement

Rolodex shall maintain comprehensive administrative, technical, operational, organizational, and physical safeguards designed to protect customer information, Company information, confidential information, proprietary information, regulated data, and sensitive records from

unauthorized access, misuse, disclosure, alteration, destruction, loss, theft, compromise, or corruption.

Section 26.02 Confidential Information

Confidential Information includes:

(a) customer information;

(b) transaction data;

(c) compliance records;

(d) investigation records;

(e) sanctions reviews;

(f) proprietary business information;

(g) source code;

(h) security architecture;

(i) regulatory correspondence.

Section 26.03 Access Restrictions

Access to Confidential Information shall be granted solely on a legitimate business need-to-know basis.

Access rights shall be:

(a) role-based;

(b) risk-based;

(c) periodically reviewed;

(d) subject to monitoring.

Section 26.04 Information Security Controls

Rolodex may implement:

(a) encryption controls;

(b) access management systems;

(c) multi-factor authentication;

(d) intrusion detection systems;

(e) security monitoring systems;

(f) endpoint protection systems;

(g) network security controls.

Section 26.05 Confidentiality Obligations

Employees, officers, directors, contractors, consultants, agents, and third parties shall maintain strict confidentiality concerning:

(a) customer information;

(b) investigations;

(c) sanctions matters;

(d) suspicious activity reviews;

(e) regulatory examinations.

Section 26.06 Unauthorized Disclosure

Unauthorized disclosure of confidential information constitutes a material violation of Company policy and may result in:

(a) termination;

(b) civil liability;

(c) criminal referral;

(d) regulatory reporting.

Section 26.07 Survival of Confidentiality

Confidentiality obligations shall survive:

(a) termination of employment;

(b) termination of contracts;

(c) termination of customer relationships;

(d) expiration of this Program.

ARTICLE XXVII

CORPORATE GOVERNANCE, BOARD REPORTING, AND COMPLIANCE OVERSIGHT

Section 27.01 Governance Framework

Rolodex shall maintain a governance framework designed to ensure effective oversight of compliance, risk management, financial crime prevention, operational resilience, and regulatory compliance.

Section 27.02 Board Responsibility

The Board of Directors bears ultimate responsibility for oversight of Rolodex ′s compliance framework.

The Board shall:

(a) approve policies;

(b) establish risk appetite;

(c) oversee remediation efforts;

(d) review compliance reports;

(e) evaluate emerging risks.

Section 27.03 Compliance Committee

Rolodex may establish a Compliance Committee responsible for:

(a) governance oversight;

(b) compliance reviews;

(c) risk assessments;

(d) policy approvals;

(e) escalation review.

Section 27.04 Reporting Obligations

The Chief Compliance Officer shall periodically report to the Board concerning:

(a) AML program effectiveness;

(b) sanctions matters;

(c) investigations;

(d) audit findings;

(e) regulatory examinations;

(f) remediation efforts.

Section 27.05 Escalation Authority

The Board shall possess authority to require:

(a) independent investigations;

(b) external audits;

(c) enhanced controls;

(d) corrective actions;

(e) executive accountability measures.

Section 27.06 Compliance Independence

The Compliance Function shall operate independently from revenue-generating business activities.

No employee, executive, shareholder, investor, director, or third party shall improperly influence compliance decisions.

ARTICLE XXVIII

ENFORCEMENT, DISCIPLINARY ACTIONS, REMEDIATION, AND ACCOUNTABILITY

Section 28.01 Policy Enforcement

Violations of this Program shall be subject to disciplinary, contractual, civil, administrative, regulatory, and legal consequences.

Section 28.02 Employee Accountability

Employees shall be personally responsible for compliance with:

(a) applicable laws;

(b) regulatory obligations;

(c) Company policies;

(d) ethical standards.

Section 28.03 Categories of Violations

Violations may include:

(a) failure to report suspicious activity;

(b) sanctions violations;

(c) falsification of records;

(d) obstruction of investigations;

(e) unauthorized disclosures;

(f) conflicts of interest;

(g) fraud;

(h) corruption.

Section 28.04 Available Disciplinary Measures

Rolodex may impose:

(a) counseling;

(b) written warnings;

(c) suspension;

(d) demotion;

(e) compensation forfeiture;

(f) termination;

(g) legal action.

Section 28.05 Management Accountability

Managers shall be responsible for maintaining effective compliance controls within areas under their supervision.

Failure to exercise reasonable oversight may constitute a policy violation.

Section 28.06 Remediation Requirements

Where deficiencies are identified, corrective action plans shall include

(a) root cause analysis;

(b) remediation timelines;

(c) responsible parties;

(d) validation procedures;

(e) Board reporting.

Section 28.07 Regulatory Referrals

Rolodex reserves the right to refer matters to:

(a) law enforcement;

(b) regulators;

(c) licensing authorities;

(d) governmental agencies.

ARTICLE XXIX

POLICY ADMINISTRATION, DOCUMENT CONTROL, AMENDMENTS, AND COMPLIANCE ATTESTATIONS

Section 29.01 Ownership

This Program shall be owned and administered by the Chief Compliance Officer.

Section 29.02 Document Governance

Rolodex shall maintain formal document control procedures addressing:

(a) version control;

(b) approval workflows;

(c) revision histories;

(d) retention requirements;

(e) publication procedures.

Section 29.03 Review Requirements

This Program shall be reviewed:

(a) at least annually;

(b) following regulatory changes;

(c) following material business changes;

(d) following significant compliance events.

Section 29.04 Amendment Authority

The Board of Directors, Compliance Committee, or Chief Compliance Officer may recommend amendments.

Material amendments shall require appropriate approval in accordance with governance procedures.

Section 29.05 Compliance Attestations

Employees, officers, directors, and designated third parties may be required to provide periodic certifications confirming:

(a) policy compliance;

(b) completion of training;

(c) disclosure of conflicts;

(d) adherence to regulatory obligations.

Section 29.06 Regulatory Supremacy

Where applicable law imposes stricter requirements than this Program, the stricter requirement shall govern.

Section 29.07 Severability

If any provision of this Program is determined to be invalid, illegal, unenforceable, or ineffective, all remaining provisions shall remain in full force and effect.

Section 29.08 Survival

The following obligations shall survive termination:

(a) confidentiality;

(b) record retention;

(c) investigations;

(d) cooperation requirements;

(e) legal holds;

(f) reporting obligations.

ARTICLE XXX

DEFINITIONS, INTERPRETATION, REGULATORY APPENDICES, AND GENERAL PROVISIONS

Section 30.01 Definitions

For purposes of this Program:

"AML"

Means Anti-Money Laundering.

"Board"

Means the Board of Directors of Rolodex .

"Compliance"

Means Rolodex ′s Compliance Department.

“Customer”

Means any individual or entity utilizing Company products or services.

“EDD”

Means Enhanced Due Diligence.

“Financial Crime”

Includes money laundering, terrorist financing, sanctions violations, fraud, corruption, cybercrime, tax evasion, and related unlawful conduct.

“OFAC”

Means the Office of Foreign Assets Control.

“PEP”

Means Politically Exposed Person.

“SAR”

Means Suspicious Activity Report.

“Sanctions”

Means economic, trade, financial, or related restrictions imposed by governmental authorities.

“Travel Rule”

Means applicable information-sharing obligations relating to financial and virtual asset transfers.

Section 30.02 Construction

This Program shall be interpreted broadly to advance:

(a) regulatory compliance;

(b) financial system integrity;

(c) consumer protection;

(d) financial crime prevention.

Section 30.03 Regulatory Appendices

Rolodex may maintain supporting appendices including:

Appendix A

Enterprise AML Risk Assessment Methodology

Appendix B

Customer Risk Scoring Framework

Appendix C

Sanctions Compliance Procedures

Appendix D

Transaction Monitoring Rules

Appendix E

Travel Rule Procedures

Appendix F

Suspicious Activity Reporting Procedures

Appendix G

Fraud Investigation Procedures

Appendix H

Record Retention Schedule

Appendix I

Training Standards

Appendix J

Regulatory Reporting Matrix

Section 30.04 Good Faith Reliance

Employees acting in good faith and in accordance with Company policy shall be entitled to appropriate institutional support in connection with lawful compliance activities.

Section 30.05 No Waiver

Failure by Rolodex to enforce any provision of this Program shall not constitute a waiver of any rights, remedies, authorities, obligations, or enforcement powers.

Section 30.06 Reservation of Rights

Rolodex expressly reserves all rights necessary to:

(a) protect its customers;

(b) protect its systems;

(c) satisfy legal obligations;

(d) prevent financial crime;

(e) preserve regulatory compliance;

(f) mitigate operational, legal, financial, reputational, and compliance risks.

Section 30.07 Effective Date

This Program shall become effective upon approval by the Board of Directors and shall remain in force unless amended, superseded, or rescinded pursuant to approved governance procedures.

Contact Information

ROLODEX TECHNOLOGIES

14321 Winter Breeze Drive

Suite 323

Midlothian, Virginia 23113

United States

Legal Department

BOARD CERTIFICATION

The Board of Directors hereby adopts this Anti-Money Laundering, Counter-Terrorist Financing, Sanctions Compliance, Customer Identification, Financial Crime Prevention, and Compliance Program as the official enterprise compliance framework of Rolodex Technologies.

The Board further directs all officers, employees, contractors, agents, subsidiaries, affiliates, and representatives of Rolodex to comply fully with the requirements set forth herein.

Failure to comply with this Program may result in disciplinary action, contractual remedies, regulatory reporting, legal proceedings, and any other remedies available under applicable law.

ROLODEX TECHNOLOGIES, LLC.