AML/ATF and Sanctions Compliance Statement

Public statement on financial crime prevention controls

EFFECTIVE DATE	16 July 2026
COMPANY	NOVARC FINANCIAL LTD.
INCORPORATION NO.	BC1579964
REGISTERED OFFICE	C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada

1. Commitment

NOVARC FINANCIAL LTD. is committed to conducting business with integrity and to preventing its products, systems and services from being used for money laundering, terrorist financing, sanctions evasion, fraud, proliferation financing or other criminal activity.

NOVARC maintains a risk-based AML/ATF, sanctions and fraud-prevention framework designed for its business model, customers, products, delivery channels, transaction activity and geographic exposure.

2. Legal and Regulatory Framework

Our framework is designed to meet the requirements applicable to NOVARC under Canadian law, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), its regulations, applicable Canadian sanctions legislation, terrorist property requirements and guidance issued by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

Where an activity requires registration as a money services business or another authorization, NOVARC offers that activity only while the applicable requirement has been satisfied and remains in effect. The current status of any FINTRAC registration should be verified in the official FINTRAC MSB Registry.

FINTRAC registration is an anti-money laundering registration. It is not a banking licence, deposit guarantee, investment approval or endorsement of NOVARC, any customer, transaction or crypto asset. This Statement addresses financial crime controls and does not describe every regulatory obligation that may apply to NOVARC.

3. Business Model

NOVARC provides or arranges digital asset liquidity and transaction services, including negotiated over-the-counter (OTC), fiat-to-crypto and crypto-to-fiat transactions for approved customers. Services are delivered remotely through digital channels and approved banking, payment, liquidity, technology and compliance providers.

Unless expressly stated in a separate written agreement, NOVARC operates on a non-custodial, transaction-by-transaction basis. It does not maintain customer deposit accounts or store customer private keys and does not accept anonymous cash transactions through physical branches.

The remote, cross-border and virtual asset nature of the business may present elevated financial crime risks. NOVARC therefore tailors its controls to legal entity customers, beneficial ownership, wallet activity, source of funds, counterparties and cross-border settlement.

4. Core Compliance Program

Subject to the requirements applicable to the business, the compliance framework includes:

- an appointed Compliance Officer with appropriate authority, knowledge, resources and access to senior management;
- written policies and procedures that are approved, maintained and updated as required;
- a documented assessment of money laundering, terrorist financing, sanctions evasion and related financial crime risks;
- risk-based customer due diligence, ongoing monitoring and enhanced measures for higher-risk relationships;
- ongoing training for relevant employees, agents, contractors and authorized persons;
- record keeping, transaction monitoring, escalation and regulatory reporting procedures;
- a review of the effectiveness of the compliance program at least every two years, or more frequently where required by law or risk.

5. Risk-Based Approach

The level of due diligence and monitoring applied to a relationship or transaction depends on the risks presented. Relevant factors may include:

- customer type, business activity, regulatory status, reputation and expected use of the Services;
- ownership, control, management and organizational complexity;
- countries of residence, incorporation, operation, payment, settlement and counterparty location;
- products, crypto assets, networks, delivery channels and use of hosted or unhosted wallets;
- expected and actual transaction value, frequency, velocity, purpose and counterparties;
- source of funds, source of wealth and the economic rationale for activity;
- sanctions, PEP/HIO, adverse-media, fraud, law-enforcement and regulatory indicators;
- use of new technologies, privacy-enhancing tools, mixers, bridges or other high-risk protocols.

Customers and relationships may be assigned risk ratings at onboarding and reviewed throughout the relationship. Higher-risk relationships may be subject to enhanced verification, additional evidence, transaction restrictions, more frequent review and senior approval.

6. Customer Identification and Verification

NOVARC identifies and verifies customers and persons acting on their behalf using methods permitted by applicable law. Verification may involve government-issued identification, reliable electronic methods, credit-file or dual-process methods, trusted identity providers and independent documentary or database checks.

NOVARC will not establish or continue a relationship where identity, authority, intended activity or other required information cannot be adequately verified. Use of a third-party verification provider does not remove NOVARC's responsibility for obligations legally assigned to it.

7. Corporate Customers, Authority and Beneficial Ownership

For corporations, partnerships, trusts and other entities, NOVARC may obtain and verify:

- legal and trade names, registration number, jurisdiction and registered or principal addresses;
- nature of business, intended use, expected activity and regulatory or licensing status;
- directors, officers, partners, trustees, authorized representatives and signing authority;
- ownership and control information, including natural persons who directly or indirectly own or control 25% or more, and persons who otherwise exercise control;
- corporate records, shareholder registers, organization charts, agreements and other evidence needed to understand ownership, control and authority.

NOVARC takes reasonable measures to confirm the accuracy of beneficial ownership information. Complex, layered, opaque or multi-jurisdictional structures may require enhanced due diligence, and NOVARC may decline a relationship where ultimate ownership or control cannot be reasonably established.

8. Politically Exposed Persons and Higher-Risk Relationships

NOVARC screens relevant customers, beneficial owners and authorized persons for politically exposed person (PEP), head of an international organization (HIO), family-member and close-associate status where required by law or appropriate to risk.

Where elevated risk is identified, controls may include additional identity checks, source-of-funds and source-of-wealth evidence, senior management approval, transaction limits, enhanced ongoing monitoring and more frequent review.

9. Sanctions and Geographic Controls

NOVARC screens customers, beneficial owners, authorized persons, counterparties and, where relevant, wallet addresses against sanctions and restricted-party information applicable to the business. NOVARC also considers Canadian ministerial directives, geographic restrictions and the requirements of banking and payment partners.

NOVARC does not knowingly provide Services to sanctioned persons, prohibited jurisdictions or transactions intended to evade sanctions. It may block, freeze, reject, restrict, report or terminate activity where required by law or where sanctions exposure or evasion risk is identified.

10. Source of Funds, Source of Wealth and Purpose

NOVARC may request information and evidence regarding the origin of fiat currency or crypto assets, the customer's source of wealth, the purpose and expected nature of the relationship, and the economic rationale for a transaction.

Evidence may include bank statements, audited accounts, tax documents, sale agreements, investment records, payroll records, wallet history, exchange statements or other reliable documentation. Failure to provide satisfactory evidence may result in delay, restriction, rejection or termination.

11. Virtual Currency and Wallet Screening

NOVARC may collect wallet addresses, determine whether a wallet is hosted or unhosted, request proof of ownership or control, and use blockchain analytics to assess transaction history and exposure.

Particular attention may be given to:

- sanctioned, illicit, stolen or otherwise restricted addresses, assets and services;
- mixers, tumblers, darknet markets, ransomware, scams, fraud and illicit marketplaces;
- rapid, circular, layered or unexplained movement through multiple wallets or platforms;
- cross-chain bridges, privacy-enhancing technologies, unsupported assets or high-risk protocols;
- activity inconsistent with the customer profile, stated purpose or expected transaction pattern;
- exposure to jurisdictions, counterparties or services presenting unacceptable risk.

Where concerns are identified, NOVARC may pause, reject, return, restrict or terminate a transaction or relationship and may make any report or disclosure required or permitted by law.

12. Ongoing Monitoring

Customer relationships and transaction activity may be monitored throughout the relationship to identify activity inconsistent with the customer's known profile, stated purpose, expected activity, risk rating or prior behaviour.

Reviews may consider transaction value, frequency, velocity, counterparties, geography, wallet exposure, changes in ownership or control, sanctions updates, adverse media, regulatory status and requests from Service Providers or authorities.

Customer information and risk assessments are updated periodically and when material changes, trigger events or new risk information arise.

13. Travel Rule and Transfer Information

Where the Canadian Travel Rule or related transfer-information requirements apply, NOVARC collects, transmits and retains prescribed originator and beneficiary information. NOVARC uses reasonable measures to obtain missing information and may suspend, reject or return a transfer where required information cannot be obtained or verified.

14. Suspicious Activity and Regulatory Reporting

NOVARC maintains procedures to identify, assess, escalate and report suspicious or otherwise reportable activity. Where the applicable legal threshold is met, NOVARC may submit suspicious transaction reports, large virtual currency transaction reports, electronic funds transfer reports, terrorist property reports, sanctions-related reports or other prescribed reports to FINTRAC or another competent authority.

NOVARC may respond to lawful production orders, court orders, regulatory examinations, sanctions obligations and law-enforcement requests. Applicable law may prohibit NOVARC from disclosing that a report, review or investigation exists.

15. Record Keeping

NOVARC retains customer identification, beneficial ownership, transaction, due diligence, monitoring, reporting, training and compliance records for the periods prescribed by law. Many AML/ATF records must be retained for at least five years, and longer retention may apply due to an investigation, litigation hold, audit or other legal requirement.

16. Prohibited and Restricted Activity

NOVARC prohibits or restricts customers, transactions and activities presenting unacceptable legal, sanctions, fraud, financial crime or reputational risk. This may include:

- anonymous, fictitious, inadequately verified or impersonated customers;
- undisclosed third-party, pass-through, nested or unapproved money services activity;
- criminal proceeds, terrorist financing, proliferation financing, sanctions evasion and tax evasion;
- fraud, scams, ransomware, trafficking, illicit gambling, corruption and stolen assets;
- mixers, darknet markets and high-risk anonymity- or privacy-enhancing services;
- counterfeit goods, unauthorized financial services, deceptive practices and prohibited sectors;
- any transaction lacking a credible lawful purpose or adequate supporting information.

17. Third-Party Providers and Outsourcing

NOVARC may use qualified third parties for identity verification, screening, blockchain analytics, payment processing, banking, liquidity, technology and other operational functions. Outsourcing does not remove NOVARC's responsibility for obligations that remain legally assigned to NOVARC.

NOVARC applies risk-based vendor due diligence, contractual controls, information-security requirements, access limitations, monitoring and oversight appropriate to the function, data sensitivity and regulatory risk.

18. Training and Effectiveness Testing

Relevant personnel receive ongoing training appropriate to their duties and exposure to financial crime risk. Training may cover customer identification, beneficial ownership, PEP/HIO and sanctions screening, suspicious activity, reporting, record keeping, wallet risk, fraud, escalation and confidentiality.

The compliance program is reviewed and tested periodically and at least every two years where required. Findings are documented, reported to senior management and addressed through proportionate corrective action plans.

19. Customer Responsibilities

Customers must provide accurate, complete and current information, cooperate with due diligence and monitoring requests, use only approved accounts and wallets, disclose any person for whom they act, and promptly report material changes or suspected unauthorized activity.

Providing false information, structuring transactions to avoid controls, refusing required information or attempting to circumvent compliance measures may result in refusal, restriction, termination and reporting to competent authorities.

20. Privacy and Confidentiality

Personal information processed for AML/ATF, sanctions and fraud prevention is handled in accordance with the NOVARC Privacy Policy and applicable law. Information may be shared with Service Providers, financial institutions, FINTRAC, regulators, law enforcement and other competent bodies where required or permitted.

NOVARC does not publish or disclose confidential monitoring thresholds, investigation methods, alert logic, internal risk models or regulatory reports where disclosure could compromise controls or violate law.

21. Governance and Updates

Senior management supports the compliance function, and the Compliance Officer has authority to escalate concerns, restrict activity and recommend termination. The framework is updated to reflect changes in law, guidance, products, technology, risk exposure and operational arrangements.

This Statement may be updated from time to time. The current version will be made available on the NOVARC Canada website.

22. Contact

COMPLIANCE	compliance@novarc.global
LEGAL INQUIRIES	legal@novarc.global
WEBSITE	https://novarc.global/canada
REGISTERED OFFICE	C/O INCORP PRO, 170-422 Richards Street, Vancouver, British Columbia V6B 2Z4, Canada

This Statement is informational only and does not create rights beyond those provided by applicable law or a written agreement with NOVARC.