FORTALEZA

Anti-Money Laundering
&
Counter Terrorist Financing Policy

Table of Contents

1.0 Version Control

Version	Author	Approved By	Date	Description
1.0	Fortaleza Compliance	Elvio Ciarla	December 2021	Initial Creation of document
2.0	Martin Verronneau	Elvio Ciarla	November 2025	PCMLTFA updates, EWRA considerations update, addition of BSA requirements, addition of payment gateway and prepaid product services, country acceptance policy refinement, reformatting and industry acceptance updates.

2.0 Overview

2.1 Document Objectives

Fortaleza's Anti-Money Laundering (AML) Policy and associated internal controls are designed to ensure compliance with the requirements set out in Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its associated regulations, as well as the obligations imposed under the United States Bank Secrecy Act (BSA) applicable to money services businesses (MSBs), including foreign MSBs with U.S. operations or exposure.

This policy outlines the foundational elements of Fortaleza's compliance program, including the mechanisms by which the company establishes and maintains a culture of compliance, executes day-to-day operational controls to identify, assess, and mitigate risks related to money laundering, terrorist financing, and sanctions evasion, and satisfies mandatory obligations relating to client due diligence, transaction monitoring, reporting, and recordkeeping. It further defines Fortaleza's strategy for maintaining regulatory alignment across its product and jurisdictional footprint, ensuring that the firm meets the expectations of relevant supervisory authorities.

2.2 Program Ownership

The Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) Compliance Program at Fortaleza is owned and overseen by the designated Compliance Officer, who holds ultimate accountability for its design, implementation, and ongoing effectiveness. The Compliance Officer is responsible for setting the strategic direction of the program, ensuring that it remains proportionate to the company's risk exposure and compliant with both Canadian and U.S. regulatory obligations, including those applicable under the PCMLTFA and the Bank Secrecy Act (BSA).

While the Compliance Officer provides overall leadership and oversight, the success and integrity of the AML/ATF Compliance Program rely on the active involvement of all Fortaleza employees. Compliance is a shared responsibility, and every staff member is expected to understand and apply relevant procedures, escalate concerns appropriately, and contribute to a culture of ethical conduct and regulatory vigilance.

Program ownership is underpinned by clearly defined roles and responsibilities, regular reporting to senior management, and mechanisms for ongoing review and enhancement. This structure ensures that the AML/CTF Compliance Program is fully embedded into Fortaleza's operational processes and remains responsive to both regulatory developments and business evolution.

2.3 Key Stakeholders

The effectiveness of Fortaleza's AML/CTF Compliance Program depends on the active engagement and coordinated contributions of multiple internal and external stakeholders. Each group plays a distinct and critical role in maintaining the integrity of the compliance framework and ensuring that the company meets its legal and regulatory obligations.

The Chief Compliance Officer holds overall responsibility for the design, oversight, and continuous improvement of the AML/CTF Compliance Program. This includes maintaining the policy suite, ensuring effective implementation of controls, monitoring program performance, and escalating material compliance risks to senior leadership and the Board, where appropriate.

Senior Management is responsible for supporting the program by ensuring that adequate human, technological, and financial resources are allocated to compliance functions. They champion a culture of compliance throughout the organization and are directly involved in assessing and responding to significant risk issues that may arise.

Directors and Board Members provide strategic oversight of the compliance framework and are expected to understand the firm's AML/CTF obligations and risk exposure. They are accountable for ensuring that appropriate governance, accountability, and reporting structures are in place.

Frontline and client-Facing Staff play a vital role in identifying and reporting unusual activity or potential red flags during onboarding, transactional interactions, and client service touchpoints. These staff members are trained to recognize suspicious indicators and are expected to escalate concerns through defined channels.

Compliance and Risk Personnel are responsible for the day-to-day execution of due diligence, transaction monitoring, sanctions screening, alert resolution, and internal reporting processes. Their responsibilities also include regulatory reporting, internal reviews, and keeping up to date with emerging threats and regulatory developments.

External Service Providers, Vendors, and Partners that perform or support AML/CTF-related functions are expected to operate in full alignment with Fortaleza's compliance policies and to meet applicable regulatory and contractual standards. Fortaleza exercises ongoing due diligence and oversight of these relationships to ensure accountability.

Agents and Mandataries, as defined under the PCMLTFA, are not currently used by Fortaleza and there are no immediate plans to appoint or engage any in the delivery of services. Should Fortaleza's business model evolve to include agents or mandataries in the future, their roles would be clearly defined, contractually bound to Fortaleza's AML/CTF standards, and subject to robust oversight, training, and due diligence.

3.0 Introduction

3.1 Business Model Overview

Fortaleza Digital LLC ("Fortaleza") is a limited liability company with its registered office at 1309 Coffeen Avenue Ste 1200, Sheridan, Wyoming 82801. Fortaleza uses ALT5 Sigma Canada Inc.'s services which is registered as a Money Services Business (MSB) with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) under registration number **M20608365** which is authorized to operate services under Dealing in Virtual Currencies and Payment Service Provider designations servicing entity clients worldwide.

Fortaleza uses ALT5 Sigma Canada Inc.'s services which is registered as a foreign Money Services Business with the United States Financial Crimes Enforcement Network (FinCEN), acknowledging its exposure to U.S. clients and transaction flows with FinCEN registration number **31000302468893**.

Fortaleza offers a diversified suite of financial technology, payments, and virtual asset services, currently comprising three distinct product lines:

- **Fortaleza Pay**: A crypto payment processing solution that enables merchants to accept virtual currency payments from their clients. This service facilitates seamless conversion of crypto to fiat where applicable and supports automated merchant settlement workflows.
- **Fortaleza Prime**: A full-stack over-the-counter (OTC) and white-label trading platform that allows institutional clients, financial institutions, and fintech firms to offer virtual asset trading capabilities under their own brand. Clients may use Fortaleza as a liquidity provider or opt to integrate external counterparties, making the platform adaptable as either a trading solution or pure infrastructure provider.
- **Fortaleza Card (MSwipe)**: A prepaid card issuing solution available exclusively to business clients, enabling corporate users to issue branded prepaid cards to their end users. These cards allow the conversion of digital asset-linked balances into fiat currency for seamless retail and online transactions. Fortaleza does not issue prepaid cards directly to individual consumers but provides business clients with infrastructure to support compliant crypto-to-fiat spending solutions.

3.2 Regulatory Overview

Fortaleza qualifies as a Money Services Business (MSB) under the definitions set forth by both Canadian and United States regulatory authorities, due to its activity involving virtual currencies and payment services.

In Canada, Fortaleza comply with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and is subject to the registration, reporting, recordkeeping, and compliance program obligations outlined in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its associated Regulations.

Fortaleza is also compliant to Canadian federal legislation governing anti-money laundering (AML), counter-terrorist financing (CTF), and sanctions compliance, including:

- The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)
- The Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations
- FINTRAC guidance applicable to Reporting Entities
- The Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)
- The United Nations Act
- The Special Economic Measures Act (SEMA)

In the United States, Fortaleza comply with the Financial Crimes Enforcement Network (FinCEN) and comply with the anti-money laundering and reporting obligations applicable to foreign-based virtual currency service providers engaging in activities with a U.S. nexus. Fortaleza comply to U.S. federal legislation and guidance, including:

- The Bank Secrecy Act (BSA)
- The USA PATRIOT Act of 2001
- The Anti-Money Laundering Act of 2020 (AMLA 2020)
- FinCEN's Guidance on Convertible Virtual Currency (FIN-2019-G001)
- The Client Due Diligence Rule (2016)
- Office of Foreign Assets Control (OFAC) Sanctions Programs

Fortaleza has implemented a comprehensive AML/CTF Compliance Program designed to satisfy the requirements set forth by both FINTRAC and FinCEN. This program incorporates risk-based internal controls, client due diligence, transaction monitoring, suspicious activity reporting, and sanctions screening procedures that are tailored to Fortaleza's operational footprint and service offerings as well as ongoing supervision, reviews, and audits by relevant regulatory authorities and is committed to maintaining full compliance with all applicable legal and regulatory standards.

3.3 Applicable Definitions

Money Laundering is the process of taking money obtained through illicit means and disguising the source to make it appear legitimate. Money laundering typically takes place in three stages:

- Placement – initial deposit of proceeds of crime into the financial system, placement may or may not include the predicate offence from which illicit funds were derived.
- Layering – conducting multiple transactions and/or transfers to convert illicit funds to another form and obfuscate the true source/original placement.
- Integration – withdrawal or conversion of the funds to a "clean" form. Money laundering may, or may not be, accompanied by a predicate criminal offence.

Terrorist Financing is the process of moving funds in relation to terrorist activities. The source of funds may come from legitimate sources and does not always involve additional illicit activity or money laundering. Terrorist financing is defined as the collection, provision or receipt of money or other property for the purpose of it being used, or in the knowledge that it is intended to be used to:

- To commit particularly serious crimes as referred to in section 74 of the PCMLTFA (every person or entity that knowingly contravenes any of the sections, subsections or the regulations listed, is guilty of an offence.)
- By a person or persons forming an association that commit such crime as referred to in section 3 of the PCMLTFA or is guilty of attempt, preparation, conspiracy or complicity in such crime, or

- For such travel as referred to in Criminal Responsibility for Public Provocation, Recruitment and Training concerning Terrorist Offences and other Particularly Serious Crimes.

A Money Service Business is a regulated entity that provides financial services such as money transmission, virtual currency transactions, or payment processing. Under Canadian law (PCMLTFA), MSBs must register with FINTRAC. Under U.S. law (BSA), foreign MSBs must register with FinCEN if serving U.S. clients or engaging in U.S.-linked transactions.

Financial Action Task Force (FATF) is an international and intergovernmental organization that aims to develop and promote policies focused on combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. FATF sets standards and provides recommendations that member countries are expected to implement. The organization's work includes monitoring the progress of member countries implementing these standards, reviewing measures taken, and promoting effective legislative, regulatory, and operational measures. FATF's recommendations are widely recognized as the global standard for compliance best practices in relation to anti-money laundering and counter-terrorist financing.

A Business Relationship is established between a Money Service Business and its Clients for financial transaction services. Money Service Business enters a business relationship under the following two conditions:

- A Client's identity is verified a second time within a 5-year period. This equates to a Client transacting equal to or greater than $1,000.00 CAD on two separate occasions.
- Engaging in a written service agreement with a Client for services related to financial transactions.

Once a business relationship is established, the MSB must fulfill additional obligations, including ongoing monitoring, recordkeeping, and updating client information, to ensure compliance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and to mitigate the risk of money laundering and terrorist financing.

A business relationship at Fortaleza ends five years after the date of the last transaction completed by the client.

Tipping Off is the unlawful act of alerting an individual or entity that they are the subject of a suspicious transaction report or an investigation by regulatory or law enforcement authorities. This practice is strictly prohibited under anti-money laundering and counter-terrorist financing laws in many jurisdictions, as it can compromise investigations, enable suspects to destroy evidence, alter behavior, or evade detection. Penalties for tipping off may include substantial fines and criminal prosecution.

Politically Exposed Persons and Heads of International Organizations are individuals who hold or have held senior public roles, such as heads of state, members of legislatures, senior government officials, judges, military officers, or executives of state-owned enterprises. Heads of International Organizations (HIOs) refer to individuals who lead institutions established by governments through formal agreements, such as the United Nations or World Bank.

Due to their positions and influence, PEPs and HIOs are considered higher risk from a money laundering and corruption perspective. As such, enhanced due diligence measures, including source of funds verification and senior management approval, may be required when establishing or maintaining business relationships with such individuals. This includes close associates and family members of PEPs and HIOs.

Under Canadian legislation, a domestic PEP or HIO ceases to be treated as such five years after the day on which they leave their qualifying position. However, foreign PEPs are considered high-risk indefinitely, regardless of how long ago they left office.

Global Affairs Canada (GAC) is the federal department responsible for the administration and enforcement of Canadian sanctions laws and regulations, including those issued under the United Nations Act, the Special Economic Measures Act (SEMA), and the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law). GAC oversees the imposition of sanctions measures such as asset freezes, prohibitions on dealings, and travel bans, and provides interpretive guidance to reporting entities and the public regarding their obligations under Canadian sanctions programs.

Ministerial Directives and associated transaction restrictions are issued by the Minister of Finance to require reporting entities to implement specific countermeasures in response to elevated money laundering and terrorist financing risks. These directives apply to transactions originating from, or destined for, jurisdictions or entities identified as high-risk. They are intended to protect the integrity of Canada's financial system and support Money Services Businesses in mitigating threats associated with international financial flows.

Each directive outlines countermeasures to either enhance or expand upon current obligations that exist under existing obligations for Money Service Businesses. The directives specify the effective date and will remain active until they are officially revoked, suspended, or amended. Current Ministerial Directives issued by Canada as of June 8th, 2025 include:

- February 24, 2024: Russia (updated March 22, 2025)
- July 25, 2020: Islamic Republic of Iran (updated February 24, 2024)
- December 9, 2017: Democratic People’s Republic of Korea (DPRK) (updated March 22, 2025)

Compliance with Ministerial Directives and transaction restrictions is mandatory. FINTRAC monitors and assesses compliance with AML directives under the PCMLTFA and may examine records or inquire into the business activities of entities covered under the Act. Compliance activities, such as on-site or desk-based examinations, may now include reviewing adherence to Ministerial Directives.

The Office of Foreign Assets Control (OFAC) is a division of the U.S. Department of the Treasury responsible for administering and enforcing economic and trade sanctions against targeted foreign countries, regimes, individuals, entities, and practices that threaten national security, foreign policy, or economic interests of the United States. OFAC maintains and publishes the Specially Designated Nationals and Blocked Persons (SDN) List, as well as sectoral sanctions and country-based restrictions. U.S. persons, including Money Services Businesses, are prohibited from engaging in or facilitating transactions with any individual or entity listed by OFAC or located in comprehensively sanctioned jurisdictions.

Third-Party Relationships and Determination exist when a client conducts a transaction or establishes a business relationship on behalf of another individual or entity who is not explicitly identified as the account holder, beneficial owner, or authorized user. Identifying such relationships is essential for effective anti-money laundering and counter-terrorist financing controls, as they may obscure the true ownership or purpose of a transaction.

Fortaleza considers undisclosed third-party involvement a risk factor and applies appropriate due diligence measures to detect, assess, and document such activity. Failure to disclose a third party may result in escalation to the Compliance function and, where appropriate, the filing of a suspicious transaction or activity report in accordance with applicable law.

4.0 Money Service Business Requirements

4.1 FINTRAC MSB Registration

Money Service Businesses (MSB) must register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), Canada's Financial Intelligence Unit (FIU) and maintain an active registration while offering money services including:

- Remain active while offering money services;
- List the appropriate money service designations;
- Be current with director, officer, ownership and associated financial institutions;
- Respond to clarification requests in the prescribed form and manner;
- Renew the registration before the expiry date; and
- Notify FINTRAC within 30 days if money service activities cease to offer.

4.2 FinCEN MSB Registration

Fortaleza must maintain an active FinCEN registration when servicing US based clients and is required to renew its Money Services Business registration with FinCEN every two years, with the renewal filing due no later than December 31 of the second calendar year following the initial registration. Any material change to the company's ownership structure, legal name, management control, or core business activities must be reported to FinCEN by submitting an updated registration within 180 days of the change.

4.3 Travel Rule

The Travel Rule is an international anti-money laundering requirement that obligates financial institutions and virtual asset service providers (VASPs) to collect, transmit, and retain identifying information about the originator and beneficiary of certain transactions. This rule is designed to enhance transparency and traceability of funds, helping to prevent the misuse of financial systems for money laundering, terrorist financing, and sanctions evasion. Compliance with the Travel Rule requires effective procedures and technologies to ensure that required data is securely shared between obliged entities and available for regulatory review.

In Canada, this includes obligations under the PCMLTFR related to Electronic Funds Transfers (EFTs), which require reporting entities to collect and retain records of specified transaction details and client information for qualifying electronic transfers.

4.4 Sanctions Obligations

Sanctions are restrictive measures imposed to influence the behavior, policies, or actions of targeted individuals, entities, countries, or sectors. They typically involve three core elements: an economic or operational restriction, the clear identification of a target, and an intended outcome aimed at altering the target's conduct. Sanctions may limit or prohibit trade, financial transactions, asset access, diplomatic engagement, or cross-border movement. These measures can be implemented through targeted sanctions or broader, comprehensive programs, and are enforced by domestic and international regulatory authorities.

Compliance is mandatory and requires the implementation of controls including client and transaction screening, the blocking and reporting of assets, and the prohibition of facilitation or provision of services to sanctioned

parties. All potential sanctions matches are subject to internal investigation and must be escalated to the Compliance Officer for assessment and appropriate action in accordance with applicable legal obligations.

4.4.1 Canadian Sanctions

The Government of Canada imposes economic sanctions under federal statutes and acts related to trade measures and restrictions:

- The Criminal Code
- United Nations Act
- Justice for Victims of Corrupt Foreign Officials Act
- Special Economic Measures Act
- Freezing Assets of Corrupt Foreign Officials Act

Canadian sanction laws prohibit Money Service Businesses engaging with designated persons, jurisdictions, and specific sectors. Compliance with sanctions law is mandatory and requires screening, monitoring, and reporting to meet obligations. Obligations for all Canadian individuals and entities remain under subsection 83.1(1) Criminal Code (R.S.C., 1985, c. C-46).

Canadian sanctions laws impose strict liability on Fortaleza for both direct and indirect dealings with designated individuals, entities, or jurisdictions. These laws also require Fortaleza to comply with asset-freezing obligations, ensuring that sanctioned parties are prevented from accessing financial services, assets, or material support through any means. Fortaleza is committed to full compliance with all applicable Canadian sanction's legislation.

4.4.2 OFAC Sanctions

The United States government imposes economic and trade sanctions under federal legislation administered by the U.S. Department of the Treasury, through the Office of Foreign Assets Control (OFAC). Key legal authorities include:

- The International Emergency Economic Powers Act (IEEPA)
- The Trading with the Enemy Act (TWEA)
- The Foreign Narcotics Kingpin Designation Act
- The USA PATRIOT Act
- Executive Orders issued under national security authority

U.S. sanctions laws prohibit direct and indirect dealings with designated persons, entities, countries, and sectors identified by OFAC. These laws have extraterritorial reach and apply even to non-U.S. entities where a U.S. nexus exists, including transactions in U.S. dollars or those routed through U.S.-based systems.

4.4.3 Sanctions Evasion

Sanctions evasion refers to any deliberate or attempted act to circumvent applicable sanctions laws and regulatory restrictions. This includes structuring transactions, concealing the identity or beneficial ownership of sanctioned parties, using third-party intermediaries or affiliates to disguise the true counterparty, or routing activity through jurisdictions with limited sanctions enforcement to obscure origin or destination.

Evasion efforts may involve indirect dealings, facilitation by non-sanctioned entities, or attempts to use crypto-native tools such as mixers, privacy-enhancing technologies, or complex wallet structures to avoid detection.

Sanctions evasion undermines regulatory frameworks and exposes Fortaleza to significant legal, financial, and reputational risks.

Fortaleza maintains a zero-tolerance policy for sanctions evasion. Any suspected attempts must be immediately escalated to the Compliance Officer. If warranted, the matter will be reported to the appropriate regulatory or enforcement authorities in accordance with Fortaleza's legal obligations and reporting protocols.

4.5 Non Compliance

Compliance with applicable anti-money laundering, counter-terrorist financing, and sanctions legislation is mandatory. Regulators may assess the severity of a compliance failure based on the harm caused to financial intelligence gathering, transparency, and the integrity of the broader financial system.

Failure to comply with legal and regulatory obligations may result in significant civil, administrative, or criminal consequences for Fortaleza and, where applicable, its directors, officers, employees, or agents. Sanctions for non-compliance may include monetary penalties, suspension or revocation of MSB registration, public enforcement actions, asset seizures, or criminal prosecution. Offences may relate to failures in reporting, recordkeeping, client due diligence, or the submission of false or misleading information to regulators.

Fortaleza is committed to maintaining full compliance with all applicable legal obligations. Any deficiencies identified through internal reviews, third-party audits, or regulatory examinations will be promptly addressed through appropriate remedial actions. The company continuously evaluates its compliance framework to ensure that it remains effective, risk-based, and aligned with evolving regulatory expectations.

5.0 Fortaleza's Compliance Program

Fortaleza maintains a governance framework designed to support the effective implementation, oversight, and continuous enhancement of its AML/CTF Compliance Program. The program is structured to ensure alignment with applicable regulatory obligations, mitigate financial crime risks, and foster a company-wide culture of integrity, accountability, and regulatory awareness.

While the Compliance Department holds primary responsibility for administering the program, all Fortaleza employees share a role in supporting its success. This includes adhering to documented policies and procedures, cooperating with internal control measures, and promptly escalating any activity that appears unusual, suspicious, or inconsistent with expected client behavior or business operations.

5.1 Compliance Officer

The Compliance Officer is formally appointed by, and reports directly to Fortaleza's senior management and Board of Directors, ensuring sufficient authority and independence from operational and revenue-generating functions. The Compliance Officer plays a critical role in overseeing adherence to regulatory obligations, safeguarding the integrity of Fortaleza's financial operations, and supporting a culture of compliance across the organization.

Key responsibilities of the Compliance Officer include:

- Exercising independent oversight and decision-making authority, free from internal or external conflicts of interest.

- Maintaining unrestricted access to personnel, systems, data, and records necessary to fulfill compliance obligations.
- Escalating material compliance issues directly to senior leadership without delay or interference.
- Serving as the primary point of contact for regulators, auditors, and law enforcement agencies, and maintaining accurate compliance documentation.
- Developing, maintaining, and updating the AML/CTF Compliance Program to ensure ongoing alignment with applicable legal and regulatory requirements, guidance, and Fortaleza's business model.
- Ensuring that records are retained and retrievable in accordance with applicable legislative and internal requirements.
- Overseeing the effectiveness of transaction monitoring systems, including the investigation, escalation, and resolution of alerts.
- Managing sanctions screening processes to ensure that clients, counterparties, and transactions are appropriately reviewed and screened on an ongoing basis.
- Delegating certain compliance functions to qualified staff or third parties where operationally appropriate, while retaining ultimate accountability.

The Compliance Officer is expected to remain informed of changes in regulatory obligations, industry guidance, and emerging financial crime risks. The role requires continuous adaptation of the Compliance Program to maintain its effectiveness and relevance in a rapidly evolving regulatory and technological landscape.

The Compliance Officer must be subscribed to FINTRAC Mailing List at all times. This subscription ensures timely receipt of updates related to regulatory expectations, new or amended publications, guidance, Ministerial Directives, and changes to reporting mechanisms or requirements. Maintaining this direct line of communication with FINTRAC is essential for ensuring ongoing awareness and adherence to evolving compliance obligations.

5.2 Risk Assessment

Fortaleza maintains an Enterprise-Wide Risk Assessment (EWRA) framework to identify, assess, and manage the risks of money laundering, terrorist financing, sanctions evasion, and other forms of illicit financial activity across all business operations. The EWRA forms the foundation of Fortaleza's risk-based approach and directly informs the design, implementation, and continuous refinement of the company's AML/CTF compliance program.

The EWRA evaluates risk across the following core categories:

- Services and delivery channels
- Client base and behavioral profiles
- Geographic exposure
- Sanctions risk and politically sensitive regions
- Operational and staffing structures
- Applicable legal and regulatory environments

Each risk category is assessed from two perspectives:

- **Inherent Risk**: The level of risk present before applying any internal controls, based on the nature, scope, and complexity of each factor.
  Residual Risk: The level of risk that remains after mitigation through policies, procedures, technology, and governance controls.

Fortaleza employs a layered and adaptive risk mitigation strategy that includes client due diligence, transaction monitoring, sanctions and jurisdictional screening, employee training, and regular program reviews. This framework is designed to reduce elevated inherent risks to residual risk levels that align with Fortaleza's established risk appetite.

Fortaleza operates within a MODERATE residual risk tolerance. The company does not engage in activities or relationships that result in unmitigated high residual risk. Any business lines, client types, or geographic exposures that cannot be brought within this threshold are considered outside of Fortaleza's risk appetite and are therefore not pursued or maintained.

5.3 Staff AML Training

Fortaleza maintains a formal Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Training Program to ensure that all personnel understand their legal, regulatory, and operational responsibilities in identifying and preventing financial crime. The program is designed to comply with applicable obligations under Canadian and U.S. law, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), the Bank Secrecy Act (BSA), and guidance issued by FINTRAC, FinCEN, and other relevant authorities.

The training program is mandatory for all Fortaleza employees, directors, contractors, and other people authorized to act on behalf of the company. It applies to staff involved directly or indirectly in activities such as onboarding, transaction processing, client support, platform development, product oversight, compliance operations, or system administration. The training supports a culture of compliance, reinforces regulatory awareness, and equips personnel to identify and escalate suspicious activity effectively.

5.3.1 Training Objectives

The purpose of the training program is to:

- Promote understanding of AML/CTF and sanctions obligations applicable to Fortaleza under Canadian and U.S. law.
- Educate staff on the methods and typologies used in money laundering, terrorist financing, and sanctions evasion.
- Familiarize employees with Fortaleza's internal AML/CTF policies, procedures, and reporting protocols.
- Reinforce staff awareness of client due diligence (CDD), enhanced due diligence (EDD), transaction monitoring, and suspicious transaction reporting (STR/SAR).
- Encourage timely escalation of unusual behavior, red flags, or jurisdictional risk indicators.
- Emphasize confidentiality obligations, particularly with respect to suspicious activity reporting and tipping-off prohibitions.
- Strengthen individual accountability in maintaining the integrity of Fortaleza's compliance controls.

5.3.2 Delivery and Frequency

- **Onboarding Training**: All new applicable employees must complete foundational AML/CTF training within 30 days of accessing client information, financial systems, or operational environments.
- **Ongoing Training**: AML/CTF training is delivered on an annual basis and is mandatory for all applicable staff. Refresher modules are updated annually to reflect regulatory changes, new typologies, compliance findings, or evolving risk exposures.

- **Role-Based Training**: Targeted training modules are provided to employees in higher-risk or specialized roles, such as compliance, finance, and product development.
- **Remedial Training**: Additional sessions are conducted in response to identified deficiencies, changes in regulatory expectations, or material compliance incidents.
- **Leave and Reintegration**: Staff returning from extended leave are required to complete current AML/CTF training within 30 days of their return to duty.

5.3.3 Training Content

Training materials cover, but are not limited to:

- Fortaleza's regulatory obligations under the PCMLTFA and the BSA.
- Company AML/CTF and sanctions policies and internal procedures.
- Identification of money laundering, terrorist financing, and sanctions evasion red flags.
- Practical case studies and typologies relevant to Fortaleza's products and services.
- Recordkeeping, escalation procedures, and STR/SAR reporting protocols.
- Staff responsibilities regarding client confidentiality and non-disclosure.

5.3.4 Oversight and Recordkeeping

The Compliance Department is responsible for maintaining the training curriculum, monitoring training completion, and tracking curriculum updates. Records of training completion, materials, assessments (where applicable), and update logs are retained for a minimum of five years and made available upon regulatory request.

5.4 Two Year Effectiveness Review

Fortaleza conducts an independent effectiveness review of its AML/CTF Compliance Program at least every two years, or more frequently as warranted by changes in regulatory expectations, risk exposure, internal audit findings, or material changes to business operations. This review is a critical element of Fortaleza's compliance oversight framework and ensures that the program remains aligned with applicable regulatory requirements in both Canada and the United States.

The purpose of the effectiveness review is to independently assess the adequacy and operational effectiveness of Fortaleza's written compliance policies, internal controls, training, reporting practices, and enterprise-wide risk assessment (EWRA). The review is also intended to identify any instances of non-compliance, deficiencies in execution, or opportunities for enhancement in line with regulatory guidance and industry best practices.

The review must be conducted by a qualified compliance professional with expertise in Canadian AML/CTF regulations (including the PCMLTFA and FINTRAC guidelines) and a working understanding of U.S. requirements under the Bank Secrecy Act (BSA), FinCEN guidance, and sanctions compliance under OFAC.

5.4.1 Scope of Review

At a minimum, each independent effectiveness review must include the following components:

- Interviews with Compliance Staff to evaluate awareness, role clarity, and escalation processes.
- client Identification and Due Diligence Testing to assess whether onboarding and verification procedures are consistently applied and compliant.

- Transaction Monitoring and Reporting Testing to evaluate the accuracy, timeliness, and completeness of suspicious transaction reports (STRs), large virtual currency transaction reports, and, where applicable, U.S. suspicious activity reports (SARs).
- Review of AML/CTF Policies to verify alignment with current legal obligations, internal operational practices, and regulatory guidance.
- Assessment of the Enterprise-Wide Risk Assessment (EWRA) to confirm that it accurately reflects Fortaleza's risk profile and is used to inform control design.
- Testing of Recordkeeping and Sanctions Screening Controls to validate that records are retained and retrievable and that sanctions screening procedures are functioning effectively.

5.4.2 Reporting and Remediation

The Compliance Officer is responsible for reviewing the findings of the effectiveness review and presenting a formal report to senior management within 30 days of the review's completion. The report must include:

- A summary of all identified deficiencies or non-compliance issues.
- A documented remediation plan, including corrective actions and clearly defined implementation timelines.
- An evaluation of whether a Voluntary Self-Declaration of Non-Compliance (VSDONC) should be submitted to FINTRAC, based on the nature and severity of the findings.
- Recommendations for program enhancements to ensure continued alignment with regulatory expectations and best practices.

Fortaleza may conduct interim or targeted reviews in response to risk events, regulatory changes, or internal audit findings. The results of each review are retained in accordance with recordkeeping obligations and may be made available to FINTRAC, FinCEN, or other supervisory authorities upon request.

5.5 Written Compliance Program

Fortaleza maintains a formal, written Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Compliance Program that outlines the internal policies, procedures, and controls implemented to meet its obligations under applicable Canadian and U.S. laws and regulations. The program establishes the operational framework through which Fortaleza prevents, detects, and responds to money laundering, terrorist financing, sanctions evasion, and other forms of illicit financial activity across its services and operations.

The written compliance program is tailored to Fortaleza's business model, risk exposure, and regulatory footprint, and is designed to support a risk-based approach in all areas of operation. It incorporates essential components, including client due diligence, transaction monitoring, regulatory reporting, recordkeeping, staff training, and independent oversight.

The program is reviewed and updated on a regular basis to ensure continued effectiveness and alignment with evolving regulatory expectations, internal audit findings, and emerging financial crime typologies. All material updates to the written compliance program are reviewed and approved by the Compliance Officer and presented to senior management and the Board of Directors for formal approval and governance oversight. Documentation of all revisions, approvals, and implementation timelines is maintained in accordance with applicable recordkeeping requirements.

5.5.1 Client Due Diligence

Fortaleza is required to identify and verify the identity of all clients before being onboarded and approved for services through approved methods in accordance with applicable Canadian and U.S. AML/CTF regulations. The purpose of client due diligence (CDD) is to confirm the legitimacy of the client, assess client-specific risk, and support internal recordkeeping and monitoring obligations.

To meet these requirements, client-provided documentation must:

- Be authentic and unaltered, with the characteristics of an original, credible document
- Be valid and not rendered inaccurate due to name changes, expiry, or other inconsistencies
- Be issued by a federal, provincial, territorial, or state government authority
- Contain the full legal name of the individual or entity
- Include a unique identification number (e.g., ID number, business registration number)
- Be current and valid at the time of verification

Fortaleza is required to identify and verify the identity of all legal entities seeking to establish a business relationship or conduct transactions through its services. This includes confirming the existence of the entity, its legal structure, control persons, and beneficial owners, as part of Fortaleza's obligation to assess institutional risk and prevent the misuse of corporate vehicles for illicit purposes.

To meet these requirements, entity clients must provide documentation that:

- Confirms the legal name, registration number, and address of the entity
- Demonstrates the entity's legal formation and current standing (e.g., certificate of incorporation or equivalent)
- Identifies the nature of the business and primary line of activity
- Names all directors, authorized signing officers, and individuals with control over the account

Fortaleza must identify and verify the beneficial owners of the entity, defined as any natural person who directly or indirectly owns or controls 25% or more of the entity's equity or voting rights, or who otherwise exercises significant control over the entity's operations or decision-making.

For each beneficial owner, Fortaleza collects and verifies the following information:

- Full legal name
- Date of birth
- Residential address
- Ownership percentage
- Government-issued identification document

Where no individual meets the ownership threshold, Fortaleza applies a control-based approach by identifying and verifying the most senior managing official of the entity.

Entity and beneficial ownership information must be verified using reliable and independent documents, data, or information. All records are retained in accordance with applicable legal requirements and subject to ongoing monitoring.

Fortaleza frequently engages with clients through non-face-to-face channels. As such, it is required to implement enhanced controls and take reasonable measures to mitigate the elevated risks of impersonation, identity fraud, and anonymity associated with remote onboarding.

When verifying client identity without in-person interaction, Fortaleza must:

- Use multi-factor authentication techniques that combine document verification with biometric, knowledge-based, or digital behavior-based elements.
- Leverage reputable third-party verification providers with appropriate due diligence to validate document authenticity and match personal attributes.
- Confirm the existence of the client using secondary data sources, such as utility records, credit bureaus, or government databases.
- Implement real-time monitoring during the onboarding process to flag mismatches, delays, or suspicious navigation patterns.

All clients, beneficial owners, and authorized representatives must be screened against applicable sanctions lists, watchlists, and adverse media sources at onboarding and throughout the business relationship.

Fortaleza is required to maintain detailed records of all customers due diligence activities, including those performed during non-face-to-face onboarding. This includes documentation of the identity information collected, the methods used for verification, and any reasonable measures taken where standard verification procedures were not applicable.

For each client, Fortaleza must retain:

- The date on which identity was verified
- Copies of identification documents reviewed or summaries of the reference source consulted
- Records confirming the verification method used, including reliance on third-party providers where applicable
- A description of any reasonable measures applied to mitigate verification limitations or address remote onboarding risks
- Beneficial ownership declarations and supporting evidence for entity clients
- Information on the authority of individuals acting on behalf of an entity

Please note that Fortaleza does not onboard Shell Companies under any circumstances.

Certain entity structures such as non-profits, trusts and charities require enhanced due diligence and outlined later in this policy.

5.5.2 Screening

Fortaleza screens all applicants and clients using a third-party compliance solution integrated with global sanctions, politically exposed persons (PEP), and watchlist databases. Screening is performed on individuals, business entities, ultimate beneficial owners (UBOs), directors, and authorized signatories prior to account activation. All clients are enrolled in ongoing monitoring, which automatically scans for new listings or updates that may affect existing Business Relationships.

If a match is identified, the system generates an alert that is immediately escalated to the Chief Compliance Officer (CCO) for manual review and disposition. Screening outputs and actions taken are logged and retained in accordance with Fortaleza's recordkeeping obligations.

Fortaleza does not transact with sanctioned individuals or entities under any circumstances. Sanctions-related matches identified through onboarding or monitoring must be escalated, and where confirmed, reported via a Suspicious Transaction Report (STR) to FINTRAC. The Chief Compliance Officer may also initiate account restrictions or seizure measures as appropriate.

Fortaleza uses a third blockchain forensics tool to monitor virtual asset activity and detect exposures to sanctioned jurisdictions, entities, or wallets. Alerts triggered by such exposures are prioritized as severe and are subject to immediate compliance review, regardless of asset type, transaction volume, or flow characteristics. Direct or indirect exposure to designated sanctions targets is strictly prohibited.

Fortaleza does not onboard sanctioned persons or entities. PEPs and Heads of International Organizations (HIOs) may only be accepted on a case-by-case basis with documented approval from the Chief Compliance Officer and application of Enhanced Due Diligence measures.

5.5.3 Client Risk Rating and Classification

Fortaleza assesses the risk level of all applicants during onboarding and periodically re-evaluates existing clients to ensure ongoing alignment with its risk appetite and compliance obligations. Risk assessments are based on a range of factors including client profile, geographic exposure, business activity, and screening results. Clients are categorized into three classifications:

1. **Unacceptable Risk:** Applicants or clients who present an unacceptable level of risk are declined or offboarded. This determination is based on risk factors that are outside Fortaleza's stated risk appetite or violate the thresholds outlined in this policy. A classification of unacceptable risk may arise from a single high-severity factor or from the accumulation of multiple high-risk indicators.

   All unacceptable risk decisions must be reviewed by the Chief Compliance Officer, who will determine whether a Suspicious Transaction Report (STR) or Attempted Suspicious Transaction Report (ASTR) must be submitted to regulatory authorities.

2. **High Risk:** Applicants and Clients classified as high risk are subject to Enhanced Due Diligence (EDD), heightened transaction monitoring, and scheduled risk reviews. A high-risk classification may result from a single elevated factor or from the cumulative presence of multiple moderate risk indicators. High-risk clients must be reassessed at intervals defined by Fortaleza's compliance framework.

3. **Acceptable Risk:** The majority of Fortaleza clients are expected to fall within the acceptable risk category. This classification includes clients whose profiles align with Fortaleza's standard risk tolerance and for whom risk mitigation measures such as screening, monitoring, and customer due diligence (CDD) are proportionate and effective. Clients in this category are monitored routinely in accordance with Fortaleza's compliance program.

5.5.4 Client Risk Rating Table Guide

Risk Rating	Determinations	Actions
Unacceptable	● Banned industry or jurisdiction associations. ● Sanctions or watchlist associations. ● Fraudulent or altered documents. ● Multiple high-risk factors are determined to be unacceptable by the Chief Compliance Officer. ● UBOs are unverifiable. ● Verification and Fortaleza AML Policy requirements not met.	Applicants denied services, clients offboarded and assessed by Chief Compliance Officer to determine reporting eligibility.
Acceptable	● Low Risk industry or jurisdiction. ● No Sanctions or PEP exposures ● No adverse media exposure related to financial or criminal offenses. ● Verification and Fortaleza AML Policy requirements complete.	Fortaleza services may commence/continue. Transaction monitoring remains at standardized levels. 36-month client maintenance review schedule.
High	● High Risk industry or jurisdiction associations as defined by Fortaleza's policies. ● Complex organization structures including charities or trusts. ● Lack of transparency or insufficient information about the source and owners of funds. ● Associations to PEPs	EDD measures required. Fortaleza services may commence/continue. Transaction monitoring remains at standardized levels. 18-month client maintenance review schedule.

A systematic risk scoring model must be used by Fortaleza to evaluate and classify all applicant and client risk factors as low, medium, or high. This scoring model supports a consistent, objective, and repeatable application of Fortaleza's customer risk assessment framework across all business relationships and services. It is designed to inform the overall customer risk rating and guide the level of due diligence, monitoring, and review applied to each client.

At a minimum, the risk assessment must evaluate and assign scores based on the following categories at minimum:

- Client type, legal form and nature of principal business
- Geographic exposure and jurisdictional risk
- Product or service usage
- Ownership and control structure (for entities)
- Sanctions, Politically Exposed Person (PEP), or Head of International Organization (HIO) screening results
- Adverse media findings

The scoring model must be fully documented within Fortaleza's Customer Risk Assessment Procedures and include defined thresholds, escalation protocols, and reassessment timelines. Changes to the scoring methodology must be approved by the Chief Compliance Officer and reflected in the corresponding procedures. All customer risk ratings and supporting assessments must be recorded, retained, and available for review by auditors or regulatory authorities as required.

6.0 Enhanced Due Diligence

An Enhanced Due Diligence assessment aims to confirm the legitimacy and further verify an individual, business entity, or source of funds. Fortaleza's Compliance team may apply enhanced due diligence efforts at any stage of a client relationship and for a number of reasons including but not limited to:

- Associations with banned or high-risk industries or clients base for business entities.
- Associations with banned or high-risk jurisdictions.
- Transaction patterns or volumes that are outside of established client profiles.
- Data inconsistencies or missing information.
- Additional due diligence required to mitigate various red flags identified by Fortaleza compliance.

6.1 Enhanced Measures

Enhanced measures are applied to higher-risk clients or situations where additional verification is necessary to address specific risk indicators. These measures must be documented, proportionate to the identified risk, and integrated into Fortaleza's due diligence process to ensure a more comprehensive understanding of all Business Relationships.

6.1.1 Elevated Verification

Enhanced verification of individuals or business entities involves collecting supplementary information or documentation to substantiate the legitimacy and nature of the client. This may include, but is not limited to:

- A secondary government-issued photo identification
- A valid business license or certificate of good standing
- A corporate organizational chart or ownership structure
- A business plan describing intended operations and sources of revenue
- A copy of the entity's AML/CTF policy where relevant

6.1.2 Source of Funds and Wealth

To establish the legitimacy of a client's financial resources, Fortaleza may request supporting documentation demonstrating the origin of funds and the source of wealth. Acceptable documentation includes:

- Three most recent months of complete, unredacted personal or corporate bank statements
- Audited financial statements or tax filings
- Documentation evidencing proceeds from business operations, asset sales, or inheritance

6.1.3 Open-Source Intelligence (OSINT)

Fortaleza may use publicly available tools and databases to validate client-submitted information or identify risk factors. This includes:

- Verifying legal entity registration with corporate registries or regulatory licensing bodies
- Conducting general internet and media searches for adverse news
- Searching for related social media profiles or reviews using red flag keywords such as "fraud," "scam," "criminal," or "theft"

- Using mapping and satellite tools to assess business premises or declared addresses for authenticity

All findings and documentation collected as part of enhanced measures must be recorded and stored in the client's compliance file. These measures are mandatory for high-risk clients and may also be initiated at the discretion of the Chief Compliance Officer in response to emerging risks or red flags.

7.0 Reporting Requirements

Compliance with reporting obligations is mandatory. Fortaleza must report qualifying transactions to FINTRAC and other agencies as required. Each report has specific conditions for which types of transactions must be reported and a specific timeline within which a report must be submitted to FINTRAC.

FINTRAC reports are submitted electronically through the FINTRAC Web Reporting System (FWR) or FINTRAC Reporting Ingest API.

Volume-based reports subject to FINTRAC's 24-hour rule are confined to a static 24-hour period that matches any calendar day from 0:00 to 23:59. Multiple transactions from a single conductor, beneficiary or third party outside of this timeframe will not be considered for volume-based reporting under FINTRAC's 24-hour rule.

7.1 Canadian Reporting Requirements

Report Type	Conditions	Timeline
Electronic Funds Transfer Report (EFTR)	Upon initiating or finally receiving international electronic funds transfers totaling $10,000 CAD or more in a single transaction or multiple transactions within a 24-hour period, where the reporting entity is the initiator, the final recipient, or both.	5 working days
Large Cash Transaction Report (LCTR)	Upon receipt of Cash (paper or coin money) from a single customer in an amount greater than or equivalent to $10,000 CAD in a single transaction or multiple transactions within a 24 hour period.	15 calendar days
Large Virtual Currency Transactions Report (LVCTR)	Upon receipt of virtual currency from a single customer in an amount greater than or equivalent to $10,000 CAD in a single transaction or multiple transactions within a static 24 hour period.	5 working days
Suspicious Transaction Report (STR)	In the event that there are reasonable grounds to suspect or reasonable grounds to believe suspicion related to money laundering, terrorist financing or sanctions evasion has occurred for completed transactions.	As soon as practicable, no longer than 30 days
Attempted Suspicious Transaction Report (ASTR)	In the event that there are reasonable grounds to suspect or reasonable grounds to believe suspicion related to money laundering, terrorist financing or sanctions evasion without a transaction being conducted.	As soon as practicable, no longer than 30 days
Listed Person or Entity Property Reports (LPEPRs)	In the event the company identifies funds or property that is affiliated with a listed sanctioned or terrorist person or entity a report must be filed immediately with FINTRAC and additionally with CSIS and RCMP.	Immediately

7.1.1 Electronic Funds Transfer Reports (EFTRs)

As a Money Service Businesses, Fortaleza must submit EFTRs under three specified conditions.

1. Initiation: When Fortaleza initiates an international electronic funds transfer of $10,000 CAD or more in a single transaction at the request of a person or entity.
2. Final Recipient: When Fortaleza finally receives an international electronic funds transfer of $10,000 or more in a single transaction.
3. Initiation and Final Recipient: When Fortaleza initiates an international electronic funds transfer of $10,000 or more in a single transaction, that is requested by a person or entity, if Fortaleza also finally receives or will finally receive the same electronic funds transfer for a beneficiary and when Fortaleza finally receives an international electronic funds transfer of $10,000 or more in a single transaction, if Fortaleza also initiated the same electronic funds transfer at the request of a person or entity.

7.1.2 Large Cash Transaction Reports (LCTRs)

Large Cash Transaction Reports are not applicable to Fortaleza services and will not be filed as Fortaleza does not accept Cash - Coin or paper money issued by a Central Bank.

7.1.3 Large Virtual Currency Transaction Reports (LVCTRs)

As a Money Service Business Dealing in Virtual Currency, Fortaleza will need to file LVCTRs if transactions meet the reportable conditions.

Fortaleza must use the Canadian dollar exchange rate established at the time of the virtual currency transaction to determine whether the reporting threshold is met. Due to the fluctuating value of virtual currencies, this rate will vary based on a per trade basis.

7.1.4 Suspicious Transactions & Attempted Suspicious Transactions

Fortaleza is required to report any transaction or attempted transaction where there are reasonable grounds to suspect that the activity is related to the commission or attempted commission of a money laundering, terrorist financing, or sanctions evasion offence.

All staff are responsible for identifying and escalating red flags to the Compliance Team without delay. Upon escalation, the Compliance Officer or delegate will assess available information, document investigative steps, and determine whether the threshold of reasonable grounds to suspect has been met.

STRs and ASTRs must be filed promptly once a reasonable suspicion is formed. Reports must be clear, concise, and include all relevant facts, contextual information, and risk indicators that support the basis for suspicion.

Reporting obligations apply regardless of transaction value and include both completed and attempted activity. STRs and ASTRs must be filed promptly once a reasonable suspicion is formed. Reports must be clear, concise, and include all relevant facts, contextual information, and risk indicators that support the basis for suspicion.

All STR and ASTR investigations, decisions, and report filings are documented and retained in accordance with Fortaleza's recordkeeping obligations.

Fortaleza prohibits tipping off and enforces strict confidentiality procedures around suspicious transaction reporting. Internal communications, customer notifications, and account actions must be handled in accordance with defined compliance protocols to avoid interference with law enforcement or regulatory processes.

7.1.5 Listed Person or Entity Property Reports (LPEPRs)

Listed Person or Entity Property Reports are submitted offline and exclusively through fax or paper mail with Paper Report Forms available for download from the FINTRAC website. Reports must be submitted to the Canadian Security Intelligence Service (CSIS) by fax at 613-369-2303 and the Royal Canadian Mounted Police (RCMP) by fax at 613-825-7030. Additionally, an STR must be filled with FINTRAC through conventional methods.

Fortaleza must conduct regular screening in line with business relationship ongoing measures against applicable Canadian lists, including but not limited to:

- Public Safety Canada Listed Terrorist Entities
- Public Safety Canada Current Listed Entities
- United Nations Security Council Consolidated List | Security Council
- Consolidated Canadian Autonomous Sanctions List

In the event of a positive match to any of the listed sanctions or terrorist designations, or if Fortaleza has reasonable grounds to believe that a customer owns or controls property on behalf of a listed person, or is associated with a terrorist group as defined under section 83.01 of the Criminal Code, an internal escalation to the Chief Compliance Officer must be initiated without delay and a coordinated review must be conducted in consultation with General Counsel and Senior Management. Reports must be submitted to FINTRAC, the RCMP, and CSIS as required, and assets must be frozen in accordance with applicable legislation.

A comprehensive internal investigation must be conducted and documented to determine the nature and scope of the exposure, assess contributing factors, identify control gaps, and implement corrective actions. Findings must be used to inform compliance training, enhance internal controls, and strengthen the overall effectiveness of Fortaleza's compliance program.

7.2 US Based Reporting Obligations

Fortaleza complies with all applicable reporting obligations under the Bank Secrecy Act (BSA), the regulations of the Financial Crimes Enforcement Network (FinCEN), and the Office of Foreign Assets Control (OFAC). Internal procedures are maintained to support the identification, escalation, and timely submission of regulatory reports for U.S.-based customers.

7.2.1 Suspicious Activity Reports (SARs)

Fortaleza files Suspicious Activity Reports (SARs) with FinCEN when it knows, suspects, or has reason to suspect that a transaction or pattern of transactions:

- Involves funds derived from illegal activity
- Is designed to evade BSA requirements (e.g., structuring)
- Lacks a legitimate or lawful business purpose
- May involve the use of Fortaleza to facilitate money laundering, terrorist financing, or other criminal activity

SARs must be filed within 30 calendar days from the date of initial detection. If no subject is identifiable, the filing deadline may be extended to 60 days. Continuing SARs are submitted every 90 days following the most recent filing if the activity persists.

All SAR-related decisions are made by the Chief Compliance Officer, who ensures documentation is retained for at least five years. Disclosure of SAR filings to unauthorized parties is strictly prohibited and may result in legal and disciplinary consequences.

7.2.2 Currency Transaction Reports (CTRs)

Fortaleza is required to file a Currency Transaction Report (CTR) with FinCEN for any transaction or series of related transactions that exceed $10,000.00 in cash (U.S. or foreign) within a single business day, conducted by or on behalf of the same person. CTR requirements include:

- Aggregating same-day cash transactions
- Verifying the identity of the transacting individual
- Filing a CTR within 15 calendar days
- Retaining all CTR records and documentation for five years

Fortaleza does not currently accept or dispense physical currency. Therefore, CTR filings are not expected under the current business model.

7.2.3 OFAC Blocking and Reporting

Fortaleza complies with OFAC regulations regarding blocked and rejected transactions. Transactions involving designated individuals, entities, or jurisdictions must be escalated for immediate action.

If a blocking requirement applies:

- Assets are frozen and not returned to the client
- A Blocked Property Report is filed with OFAC within 10 business days
- Annual reporting is completed by September 30 for all blocked assets
- The incident is reviewed for a potential SAR filing

If a transaction must be rejected (e.g., involving a comprehensively sanctioned country), Fortaleza will:

- Reject the transaction
- Notify OFAC within 10 business days
- Document the rationale and retain all records

OFAC screening is conducted through automated tools at onboarding and during monitoring. Alerts are reviewed for confirmation and necessary escalation. The Chief Compliance Officer oversees all filings and ensures compliance with retention and reporting standards.

8.0 Identifying Suspicious Activity & Investigations

Identifying suspicious transactions begins with screening and identifying any transactions that appear unusual based on risk flags and detection measures, assessing the facts and context surrounding these transactions and linking any indicators of money laundering, terrorist financing or sanctions evasion to an evaluation.

Examples of red flags for suspicion for Fortaleza services include but are not limited to:

- Fraud or risk alert triggers through Fortaleza's automated transaction review software
- Transaction volumes and frequency outside of the established client profile
- Funds originate from, or are sent to, an exchange that is not registered in the client's jurisdiction; or are in areas that have Virtual Currency regulations
- Client opens multiple accounts
- Clients that frequently change their credentials, including email addresses, IP addresses, or financial information
- Structuring transactions in small amounts and under the record-keeping or reporting thresholds
- Virtual currency transfers immediately after purchase to multiple virtual asset service providers

Grounds for suspicion must be outlined in a Fortaleza investigation report detailing how the facts, context, and indicators resulted in the conclusion:

- "Fact" refers to an objective detail or event such as the red flag or trigger that led to the investigation, a fact cannot be an opinion.
- "Context" provides clarity on the circumstances surrounding a transaction, including details regarding the client profile, client financial background and the investigation steps taken to determine suspicion. Transactions alone may not seem suspicious, however, context can outline the conditions that support suspicious activity.

Established Client profiles, including assigned risk ratings, must be assessed and leveraged during the investigation to identify indicators specific to the Client. Fortaleza's Chief Compliance Officer must review and approve all suspicious activity investigations prior to filing a Suspicious Report to ensure the reasonable grounds to suspect threshold has been met and adequate facts, context and indicators are included in the investigation.

8.1 Investigation Framework

Fortaleza's standardized investigation process includes the following measures:

1. **Forensic Activity within third party blockchain analysis software:** Analysis of client wallet and virtual currency transactional data considering asset, velocity, volume and exposure.
2. **Sanctions Screening and Review:** Screening business entities, directors, UBOs, authorized signatories, and known associates against sanctions lists and comprehensive review of related compliance requirements.
3. **OSINT Investigation**: Open-source intelligence (OSINT) gathering to gather relevant information including examination of social media profiles and associated websites for additional context.
4. **Elevated Verification:** Obtaining further information from the client to support verification through a Request for Information (RFI) process adhering to the terms outlined in this policy and with the approval of Fortaleza's Chief Compliance Officer or designate. Requests must be reasonable and avoid any instances of "tipping off".

8.2 Investigation Outcomes

Following the review and analysis of unusual or potentially suspicious activity, Fortaleza must document the outcome of each investigation under one of the following categories. Each outcome must be supported by clear rationale and corresponding evidence, recorded in the compliance case management system:

1. **No Further Action:** The red flags identified are reasonably explained or resolved through investigation. No indicators of money laundering, terrorist financing, sanctions evasion, or other financial crime remain present. The activity is determined to be consistent with the client's expected profile, and no regulatory reporting or additional escalation is required.
2. **Flagged for Further Monitoring and Due Diligence:** Although activity may not meet the threshold for a Suspicious Report, certain indicators warrant increased scrutiny. The client is subject to enhanced monitoring procedures and re-evaluated through a new client risk assessment. Additional documentation may be required to maintain the relationship, and future activity will be closely tracked for escalation.
3. **Client Offboarded (Demarketed):** Where the investigation identifies an unacceptable level of risk or repeated patterns of concern, Fortaleza may determine that the client relationship is no longer within the company's risk appetite. Offboarding may also be triggered by the discovery of regulatory breaches, submission of fraudulent documents, or continued high-risk behavior. The Chief Compliance Officer must review and approve all decisions to terminate client relationships.
4. **Suspicious Report Filed:** Where reasonable grounds exist to suspect that the activity may involve the proceeds of crime, terrorism financing, sanctions evasion, or other illicit behavior, Fortaleza will submit a Suspicious Report to the appropriate regulatory body (e.g., FINTRAC or FinCEN). The filing must be completed within the required reporting timeline and supported by all available documentation.

9.0 Business Relationship Monitoring

Fortaleza conducts ongoing monitoring of client transactions to identify and report any suspicious activity and evaluate Business Relationships. Fortaleza's IT systems have pre-programmed notifications and triggers that notify Fortaleza Compliance of unusual activity related to fiat transactions. Reviews of high volume/high velocity transfers are conducted bi-weekly by Fortaleza compliance to support client monitoring and reporting initiatives.

In addition to automated and event-driven reviews, Fortaleza schedules periodic reassessments of client activity based on the client's risk rating. Higher-risk clients are subject to more frequent and detailed monitoring, including comprehensive reviews of transactional behavior, geographic exposure, and changes in ownership or business activity.

The primary focus and scope of Fortaleza's compliance monitoring is determined by the risks identified in its Enterprise-Wide Risk Assessment, AML policies, and established procedures. Fortaleza reviews for activities and transactions that deviate from what is expected with established client profiles.

Virtual Currency transactions undergo assessment through API with the third party blockchain forensics tool where pre-programed risk parameters are established to prompt alerts for manual review by Fortaleza Compliance on a weekly basis. Forensic analysis traces the origin of funds on the blockchain, followed by risk rule matching based on Fortaleza's risk appetite. These risks rules focus on Severe and High-Risk alerts such as sanctions, terrorist financing, child abuse material, and other illicit activity associations. Such incidents prompt a thorough review and may lead to an investigation and filing of Suspicious Reports where applicable.

9.1 Virtual Currency KYT Review Framework

Fortaleza applies a structured Know-Your-Transaction (KYT) review framework to assess virtual currency activity for indicators of financial crime, sanctions exposure, and overall risk. The framework is triggered by automated alerts generated by Fortaleza's blockchain analytics tools and requires manual review of certain high-severity and complex cases.

Manual reviews are triggered when automated transaction monitoring systems generate alerts due to exposure concerns or unusual behavior. The review process involves a comprehensive evaluation of the following factors to assess the legitimacy and risk associated with the transaction:

Assessment criteria must Include:

1. **Exposure Percentage:** The proportion of the transaction volume linked to wallets or counterparties with identified risk, including sanctioned entities, darknet marketplaces, mixing services, or other illicit typologies.
2. **Volume:** The total notional value of the virtual asset involved in the transaction, assessed alongside the proportion of that value associated with identified risk exposures. This includes measuring how much of the total volume interacts with wallets or services linked to financial crime typologies or sanctioned entities/wallets. Higher risk is attributed where a significant portion of the transaction value is exposed, even if the overall transaction size is moderate.
3. **Asset Type:** Assessment of the virtual currency involved, considering characteristics such as transaction speed, privacy features, market liquidity, and common use in obfuscation typologies.
4. **Hop Analysis:** Hop analysis evaluates how closely a transaction is connected to known risk exposures on the blockchain. This includes direct exposure, where the transaction immediately involves a wallet associated with illicit activity or a sanctioned party, and indirect exposure, where the transaction passes through a chain of intermediary wallets. The number of intermediary wallets, the nature of those intermediaries, and their relationship to known risk sources all contribute to assessing the level of exposure and the potential for illicit linkage.
5. **Exposure Direction:** Transaction direction provides essential context in determining the nature and potential intent of a transaction. Outbound transactions may signal an effort to conceal value, transfer illicit assets, or avoid regulatory scrutiny. Inbound transactions can suggest the client is receiving tainted funds or acting as an intermediary. Directional analysis helps identify suspicious behavior patterns and assess whether a transaction aligns with the expected risk profile of the client.

These reviews must evaluate the transaction context, the source and destination of funds, the nature of the involved wallets or counterparties, and whether the activity is consistent with the client's known profile and risk classification. Reviewers must consider client documentation, historical risk ratings, and blockchain intelligence results.

All manual reviews must be documented clearly. This includes the final decision, whether the alert is dismissed, escalated for further investigation, or results in a regulatory report, along with a clear explanation of the reasons behind that decision. Fortaleza's internal procedures must define the criteria for conducting manual reviews to ensure consistency, regulatory alignment, and a defensible audit trail.

10.0 Record Keeping

To facilitate information requests, and to be aligned with compliance best practices, records must be maintained in an organized and accessible format and be retained for a minimum of 5 years after the date the record was created. Access to records on Fortaleza servers is granted on an as-needed basis and is accessible only through two factor authentication.

In the event of a FINTRAC request for information, the request must be fulfilled within 30 calendar days.

Documents for Fortaleza to meet record keeping requirements with the information supported in this policy include:

- Copies of every report submitted to FINTRAC.
- Records relating to commercial transactions over $10,000.00 USD or equivalent conducted by Fortaleza.
- Records related to Government Issued Photo ID verification.
- Business relationship records outlining services and client profiles and risk ratings used to anticipate transactions and activity used to support suspicion identification.
- Records related to the compliance program, onboarding and monitoring policies, procedures, and methodology.
- Entity verification and Beneficial Ownership records.
- Records of any verifications, transactions
- Sanctions and PEP screening records.
- Record requirements related to measures implemented by Ministerial Directives.
- Copies of Independent reviews, FINTRAC Exams, and Law Enforcement Requests.

11.0 Voluntary Self-Declaration of Non-Compliance (VSDONC)

FINTRAC promotes a regulatory approach that is based on the promotion of compliance and not to penalize reporting entities with fines and penalties. Unreported transactions may hold value for FINTRAC and law enforcement, and must be reported even when missed, late, or uncovered during a scheduled or independent effectiveness review.

Submitting a VSDONC, an entity officially acknowledges compliance obligation short-comings and lists implemented measures to regain compliance. FINTRAC will work with a reporting entity to guide and correct instances of non-compliance without proposing administrative penalties, if:

1. The voluntarily declared non-compliance issues are not a repeated instance of a previous, voluntarily disclosed issue.
2. The VSDONC submission is not after a reporting entity has been notified of a FINTRAC Examination.

Voluntary self-declarations of non-compliance must be sent to: VSDONC.ADVNC@fintrac-canafe.gc.ca and include:

- Fortaleza's MSB details and contact details for submitting the report.
- The number of reports impacted, type, and the time period during which the issues occurred, as well as the reasons why the reports were not submitted, were late, or incorrect.
- The period during which the instances of non-compliance unrelated to reporting occurred and the reason for occurrence.
- A detailed plan to resolve the issues and submit all outstanding reports, including measures and timelines for corrective action.

Personal information regarding instances of non-compliance must be protected and not included in VSDONC reports or submission email. If private information is pertinent to the investigation, FINTRAC will provide secure information sources.

12.0 Whistle-Blower Function

Fortaleza is dedicated to preventing and addressing malpractice, including fraud and corruption. By fostering a culture of transparency and early reporting, Fortaleza aims to reduce risks and address issues promptly. Fortaleza maintains a strict policy against illegal or unethical behavior, including fraud, regulatory violations, and

breaches of company policies. All employees and stakeholders are encouraged to raise concerns openly, with procedures and protections in place to ensure whistleblowers are not subject to retaliation.

When raising a concern under the Fortaleza Whistleblower policy, Fortaleza ensures that Whistleblowers will not face any form of retaliation, victimization, or harm as a result of their actions. The Public Interest Disclosure Act (PIDA) may offer legal protection to Whistleblowers where concerns are raised in line with this Act.

- The Public Interest Disclosure (Whistleblower Protection) Act (PIDA)
- Freedom of Information and Protection of Privacy Act (FOIP)

All legitimate concerns will be taken seriously and addressed according to this procedure, whether submitted anonymously or with an identified individual. Fortaleza is committed to handling all issues with confidentiality and will maintain discretion wherever possible. If a situation arises where confidentiality cannot be preserved, Fortaleza will inform the Whistleblower at the earliest opportunity.

Concerns should always be reported internally, unless not feasible due to the involvement of individuals involved in whistleblowing reporting channels. Concerns may be submitted anonymously. Concerns about fraud, malpractice, or corruption can be reported to Fortaleza's Chief Compliance Officer (CCO), Chief Executive Officer (CEO) or Board of Directors.

Fortaleza treats all concerns seriously, addressing them independently, promptly, and confidentially while protecting identities. Reports are documented and assessed. Investigations may involve internal inquiries, consulting key stakeholders, auditing documents and engaging with the whistleblower for additional information, if possible.

Reports must include:

- Date(s) of the incident(s)
- Identity of individuals and witnesses
- Description of actions or omissions
- Discovery details
- Steps taken during the incident
- Supporting materials

13.0 Country Acceptance Policy

Fortaleza maintains a clear jurisdictional policy to ensure legal compliance and align with regulatory expectations across Canadian, U.S., and FATF frameworks. This policy governs both client onboarding and ongoing monitoring throughout the business relationship.

For the purposes of this policy, "Location" is defined broadly to capture any jurisdiction associated with a client's risk profile, including but not limited to office premises, residence, ownership structures, bank account jurisdictions, document issuance, address, and supply or service feeds.

13.1 Banned Countries

Fortaleza does not onboard or continue to service any client with direct or indirect ties to jurisdictions subject to active Canadian or U.S. sanctions, including those listed by Global Affairs Canada and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Canadian Ministerial Directives.

Fortaleza prohibits onboarding or continuing business relationships with clients who have direct ties to jurisdictions under sanctions. These clients are declined immediately or must be off boarded for the following jurisdictions:

- Afghanistan
- Belarus
- Central African Republic
- China
- Cuba
- Democratic Republic of the Congo
- Guatemala
- Haiti
- Iran
- Iraq
- Lebanon
- Libya
- Moldova
- Myanmar
- Nicaragua
- North Korea
- Russia
- Rwanda
- Somalia
- South Sudan
- Sri Lanka
- Sudan
- Syria
- Ukraine regions occupied by Russian forces
- Venezuela
- Yemen
- Zimbabwe

No exceptions are permitted for individuals or entities with direct residence, operational, or ownership presence in these jurisdictions.

However, where a UBO or key stakeholder holds verifiable, long-standing foreign residency outside of a banned jurisdiction, and comprehensive enhanced due diligence confirms no ongoing nexus to the sanctioned territory, exceptions may be considered on a strictly case-by-case basis. This process requires documented evidence of residency, a detailed risk analysis, and internal escalation prior to onboarding with written approval from Fortaleza's Chief Compliance Officer.

13.2 Restricted Countries

Fortaleza applies heightened scrutiny to clients with ties to Restricted Jurisdictions, which include countries or territories identified by the Financial Action Task Force (FATF) as having strategic AML/CFT deficiencies or elevated jurisdictional risk, but that are not subject under Canadian or U.S. sanctions laws.

Clients domiciled in, operating from, or with significant exposure to these jurisdictions may be onboarded only after successful completion of Enhanced Due Diligence (EDD).

Restricted Jurisdictions include:

- Algeria
- Angola
- Bolivia
- Bulgaria
- Cameroon
- Cote d'Ivoire
- Kenya
- Lao People's Democratic Republic
- Monaco
- Namibia
- Nepal
- Vietnam
- Virgin Islands UK

14.0 Industry Acceptance Policy

Fortaleza does not provide services to certain industries that pose heightened risks of money laundering, terrorist financing, chargebacks, regulatory conflict, or reputational damage.

Clients operating in the following sectors are automatically declined under all circumstances:

- Adult content
- Cannabis dispensaries and related CBD products
- Firearms or firearm accessories
- Multi-level marketing schemes
- Replica or Counterfeit Goods
- Exotic Animal trade

Note that even clients offering multiple product lines may be declined if any involve prohibited activity.

15.0 Policy Review Schedule

Fortaleza's Compliance Policy is reviewed at least once every 12 months to ensure continued alignment with regulatory obligations, risk exposure, business activities, and operational realities. Interim reviews may also be triggered by:

- Changes in applicable laws or regulatory guidance issued by FINTRAC or other Canadian authorities;
- Findings from effectiveness reviews, internal audits, or compliance testing;
- Material changes to Fortaleza's products, services, or geographic exposure; or
- Emerging typologies or developments in the financial crime landscape.

The Chief Compliance Officer is responsible for coordinating the review process, approving policy updates, and ensuring any required amendments are communicated to relevant personnel. Documentation of each review, including the date, scope, and nature of changes made, is maintained as part of Fortaleza's compliance records.

Next Scheduled Update: November 15th, 2026.