Done.com Inc.

COMPLIANCE PROGRAM

David Faith

Compliance Officer

DONE OTC

Compliance Program Table of Contents

Table of Contents

1. Introduction

1.1 Purpose and Scope

The purpose of this Compliance Program ("Program") is to establish a comprehensive framework for Done.com Inc. Inc. (" Done.com Inc. ") to effectively manage and mitigate risks associated with money laundering (ML), terrorist financing (TF), sanctions evasion, and other illicit financial activities. As a Money Services Business (MSB) specializing in over-the-counter (OTC) solutions across multiple asset classes, with a particular focus on foreign exchange and digital currencies, Done.com Inc. recognizes the importance of strict adherence to applicable Canadian laws and regulations, notably the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, its associated Regulations, and all related FINTRAC guidelines.

This Compliance Program outlines policies, procedures, controls, and training designed to ensure Done.com Inc. 's operations remain fully compliant, transparent, and secure. The Program applies to all business activities undertaken by Done.com Inc. , including customer onboarding, transaction processing, monitoring, record-keeping, reporting obligations, and ongoing risk assessment practices. All employees, management, directors, consultants, contractors, and third-party service providers engaged by Done.com Inc. are within the scope of this Program and are required to adhere to its provisions at all times. The Program aims to foster a robust compliance culture, safeguard the financial system's integrity, and uphold Done.com Inc. 's reputation as a responsible and trustworthy financial services provider.

1.2 Regulatory Framework Overview

Done.com Inc. 's Compliance Program is structured around a comprehensive understanding of, and strict adherence to, the relevant Canadian legislative and regulatory framework. Specifically, Done.com Inc. is subject to, and will maintain compliance with, the following laws, regulations, and guidelines:

Primary Legislation:

- **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**
  - Establishes obligations for record-keeping, client identification, reporting of suspicious transactions, and registration requirements for Money Services Businesses (MSBs).
  - Defines responsibilities for monitoring transactions to detect and prevent money laundering and terrorist financing activities.
- **Criminal Code of Canada**
  - Defines criminal offenses related to money laundering, terrorist financing, and sanctions evasion.

- **United Nations Act, Special Economic Measures Act, and Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law)**

  - Establish sanctions-related obligations, including screening customers and transactions against sanctioned entities and jurisdictions.

Regulations and Associated Guidelines:

- **Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)**
  - Outlines specific operational requirements for MSBs including customer identification, record-keeping standards, transaction reporting thresholds, and registration processes.
- **FINTRAC Guidelines and Directives**
  - Provide detailed compliance expectations including risk assessment methodologies, suspicious transaction reporting procedures, customer due diligence (CDD), and enhanced due diligence (EDD) practices.

Oversight and Enforcement Agencies:

- **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**
  - Canada's financial intelligence unit responsible for monitoring compliance with the PCMLTFA and PCMLTFR, receiving transaction reports, and conducting compliance examinations.
- **Office of the Superintendent of Financial Institutions (OSFI)**
  - Provides guidance relevant to interactions with regulated financial institutions, particularly in correspondent banking relationships.
- **Royal Canadian Mounted Police (RCMP) and Local Law Enforcement**
  - Responsible for investigating violations related to money laundering and terrorist financing offenses.

International Standards:

- **Financial Action Task Force (FATF) Recommendations**
  - Establish international AML/CFT standards adopted by Canada and integrated into domestic legislation.
- **Basel Committee on Banking Supervision Guidelines**
  - Relevant guidance on risk management practices and frameworks applicable to OTC transactions.

Other Relevant Legislation:

- **Privacy Act and Personal Information Protection and Electronic Documents Act (PIPEDA)**
  - Governs the collection, use, and disclosure of personal information of clients, ensuring privacy and data security standards.

1.3 Definitions and Terminology

Regulatory and Legal Terms

PCMLTFA: Proceeds of Crime (Money Laundering) and Terrorist Financing Act: Canada's primary anti-money laundering and anti-terrorist financing law.

PCMLTFR: Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations: Detailed operational requirements under PCMLTFA.

FINTRAC: Financial Transactions and Reports Analysis Centre of Canada: Canada's financial intelligence unit that monitors MSB compliance.

OSFI: Office of the Superintendent of Financial Institutions: Federal regulator providing oversight in banking/correspondent relationships.
RCMP: Royal Canadian Mounted Police: Law enforcement body investigating ML/TF violations.
FATF: Financial Action Task Force: International AML/CFT standard-setter.
Basel Committee on Banking Supervision: Provides guidance on global risk management standards.
PIPEDA: Personal Information Protection and Electronic Documents Act: Governs privacy and data use in Canada.
United Nations Act / Special Economic Measures Act / Magnitsky Law: Canadian legislation enforcing sanctions.

Compliance Roles

Compliance Officer (CO): Senior officer responsible for implementing and managing the Compliance Program.
Compliance Analyst / Associate: Staff conducting day-to-day CDD/EDD, monitoring, and reporting.
Compliance Training Coordinator: Staff responsible for training and awareness programs.
Internal Audit and Review Staff: Independent reviewers of controls and monitoring.

Core AML/CTF Concepts

AML/ATF: Anti-Money Laundering / Anti-Terrorist Financing.
ML: Money Laundering.
TF: Terrorist Financing.
CDD: Customer Due Diligence: Standard process for verifying customer identity and risk.
EDD: Enhanced Due Diligence: Extra checks applied to high-risk clients/transactions.
KYC: Know Your Customer: The identification and verification process for clients.
PEP: Politically Exposed Person: Individuals in prominent public roles, including family/associates, subject to EDD.
Beneficial Ownership: Identification of natural persons who ultimately own/control 25%+ of a legal entity.
Third-Party Determination: Assessing whether a customer acts on behalf of another person or entity.
Non-Face-to-Face (NFTF) Verification: Remote/digital client verification methods (dual-process, credit file, photo ID with technology).

Transaction Reporting

STR (Suspicious Transaction Report): Filed when activity is suspected to be linked to ML/TF.

LCTR (Large Cash Transaction Report): Filed when CAD $10,000+ in physical cash is received.

EFT (Electronic Funds Transfer) Report: Filed when CAD $10,000+ is transferred cross-border via wire/SWIFT/other.
VCTR (Virtual Currency Transaction Report): Filed when CAD $10,000+ in cryptocurrency is sent/received.
Cross-Border Transactions: Transactions where value enters or leaves Canada; reportable via EFT or VCTR.
Risk Assessment
Risk Categories: Customer, Product/Service, Geographic, Delivery Channel.
Risk Ratings: Low / Medium / High Based on likelihood and impact.
Risk Assessment Matrix: Tool documenting identified risks and corresponding mitigation controls.
High-Risk Jurisdictions: Countries listed by FATF, subject to sanctions, or known for corruption.
High-Risk Transactions: Large, frequent, cross-border, crypto-to-fiat, structured, or anonymity-focused transactions.
Record-Keeping & Controls
Retention Period: Minimum of 5 years for KYC, reports, risk assessments, training, and monitoring records.
Confidentiality Requirements: STRs and reports must remain undisclosed to clients ("tipping-off" prohibited).
Audit Trails: Documentation of monitoring, access, and compliance review activities.

2. Compliance Policies and Procedures

2.1 Appointment of a Compliance Officer

Done.com Inc. shall appoint a Compliance Officer who holds primary responsibility for the implementation, oversight, and management of this Compliance Program. The Compliance Officer will have the requisite authority, resources, independence, and support from senior management to effectively carry out their compliance duties and responsibilities.

The Compliance Officer's responsibilities include, but are not limited to:

- Developing, implementing, maintaining, and periodically updating Done.com Inc.'s Compliance Program.

- Ensuring adherence to all relevant regulatory requirements including the PCMLTFA, associated regulations, and FINTRAC guidance.

- Conducting regular reviews and updates of compliance policies and procedures to reflect regulatory changes and emerging risks.
- Providing compliance training and awareness programs for employees and third parties engaged by Done.com Inc. .
- Conducting risk assessments, monitoring compliance with the established controls, and promptly addressing any identified deficiencies.
- Preparing and submitting required regulatory reports (e.g., Suspicious Transaction Reports, Large Cash Transaction Reports, etc.).
- Serving as the primary liaison between Done.com Inc.and regulatory agencies including FINTRAC.
- Reporting periodically to senior management and the Board of Directors on the effectiveness of the Compliance Program and on any compliance-related issues or developments.

Compliance Officer Information

Name: David Faith
Title/Position: Compliance Officer
Date of Appointment: July 25th 2025
Business Address: Suite 830-2425 Matheson Boulevard East Mississauga ON L4W 5K4
Phone Number: 647-617-4456
Email Address: david@doneotc.com

Date: August 1st 2025

2.2 Roles and Responsibilities of Compliance Staff

All compliance staff members at Done.com Inc. , under the direction and supervision of the appointed Compliance Officer, have clearly defined roles and responsibilities to ensure the effectiveness of the Compliance Program. These roles include but are not limited to:

Compliance Officer

- Oversees the Compliance Program, ensuring full adherence to regulatory requirements.
- Reports directly to senior management and the Board of Directors on compliance status, regulatory changes, and emerging risks.

- Manages regulatory reporting obligations and liaises with regulatory bodies including FINTRAC.

- Coordinates ongoing risk assessments and updates to the Compliance Program.
- Supervises and provides guidance to compliance analysts and other staff members.

Compliance Analysts/Compliance Associates

- Conduct customer due diligence (CDD) and enhanced due diligence (EDD) processes.
- Review customer transactions and activity to identify potential suspicious transactions or AML/CTF red flags.
- Prepare and submit required reports (e.g., Suspicious Transaction Reports (STR), Large Cash Transaction Reports (LCTR), Virtual Currency Transaction Reports (VCTR), etc.).
- Maintain compliance records and documentation according to regulatory and internal policy requirements.
- Assist the Compliance Officer in executing training programs and maintaining compliance awareness across the organization.

Compliance Training Coordinator

- Develops, schedules, and delivers AML/CTF training programs to all employees and relevant third parties.
- Maintains training records, ensuring staff have received and understood necessary compliance training.
- Tracks regulatory changes and updates training materials to reflect the latest standards and practices.

Internal Audit and Review Staff

- Conduct independent audits and reviews of compliance procedures, internal controls, and transaction monitoring processes.
- Identify compliance gaps, recommend improvements, and monitor the implementation of corrective actions.
- Prepare internal compliance audit reports for review by the Compliance Officer and senior management.

Management and Senior Staff

- Support and promote a strong compliance culture throughout the organization.
- Ensure adequate resources and authority are allocated to compliance functions.
- Participate in regular compliance reviews and training sessions.
- Respond promptly to compliance-related issues, recommendations, or concerns raised by the compliance staff.

All Employees and Third Parties

- Comply fully with Done.com Inc.'s Compliance Program, policies, and procedures.
- Attend and actively participate in compliance training sessions.
- Promptly report suspicious activities or concerns to compliance staff or the Compliance Officer.

- Maintain confidentiality of compliance-related information and client data.

2.3 Employee Background Checks and Suitability

To maintain the integrity and reliability of its compliance operations, Done.com Inc. requires that all employees—particularly those involved in compliance, operations, finance, customer onboarding, and transaction handling—undergo background screening and suitability assessments prior to employment and, where appropriate, at regular intervals thereafter.

The objective is to ensure that individuals in sensitive roles demonstrate the highest standards of ethical conduct, integrity, and financial responsibility, and are not susceptible to financial crime, conflicts of interest, or coercion.

Pre-Employment Screening Requirements:

- Identity Verification: Confirmation of legal name and government-issued identification.
- Criminal Background Check: Screening for criminal convictions, especially those related to financial crimes, fraud, terrorism, or regulatory offenses.
- Sanctions and Watchlist Screening: Cross-checking against national and international watchlists (e.g., OSFI, UN Sanctions, INTERPOL, etc.).
- Employment History Verification: Review of previous roles, responsibilities, and professional conduct.
- Education and Qualifications Check: Confirmation of stated educational achievements and professional certifications (as applicable).

Ongoing Suitability and Monitoring:

- Annual Declarations: Employees in key compliance and operational roles are required to declare any changes in personal circumstances (e.g., criminal charges, conflicts of interest, bankruptcy, etc.).
- Access Reviews: Periodic reviews of system access levels and privileges to ensure they remain aligned with employee roles.
- Random and Triggered Re-Screening: Re-screening of employees may occur based on role changes, compliance incidents, or at random to reinforce control effectiveness.

Confidentiality and Data Handling:

All background checks are conducted in compliance with applicable privacy laws and internal confidentiality policies. Done.com Inc. ensures that the collection, use, and storage of personal information during background checks align with the Personal Information Protection and Electronic Documents Act (PIPEDA) and other relevant legislation.

2.4 Approval, Updating, and Maintenance of Policies

Done.com Inc. is committed to maintaining a robust and up-to-date Compliance Program that reflects current regulatory requirements, industry best practices, and the specific risks associated with its business activities. To ensure this, all compliance policies and procedures are subject to formal approval, periodic review, and ongoing maintenance.

Policy Approval

- All compliance-related policies and procedures must be reviewed and approved by the **Compliance Officer** and submitted to **senior management** for final authorization.
- Material updates that affect operational practices, reporting obligations, or risk mitigation strategies must also be communicated to the **Board of Directors**, where applicable.

Review and Update Schedule

- Compliance policies shall be reviewed **at least annually**, or more frequently if:
  - There are changes to applicable laws or FINTRAC guidance;
  - The company expands into new products, services, jurisdictions, or delivery channels;
  - Internal audits, compliance reviews, or regulatory examinations identify deficiencies or gaps;
  - There are significant operational or structural changes within Done.com Inc.
- The Compliance Officer is responsible for tracking regulatory updates and initiating timely policy revisions to maintain alignment with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and other applicable frameworks.

Version Control and Documentation

- Each version of the Compliance Program and related policies must be:
  - Dated and assigned a revision number;
  - Retained in both hard copy and digital format for a minimum of **five years**;
  - Accessible to relevant employees, regulators, and auditors upon request.
- A **Policy Change Log** shall be maintained to document:
  - The nature of each change;
  - The reason for the update;
  - The date of implementation;
  - The individual(s) responsible for the revision and approval.

Communication and Training

- Once updated, all relevant employees and stakeholders must be notified of changes and, where applicable, receive updated training or guidance.
- New or revised policies will be distributed through official channels (e.g., secure company portal or internal communications), with mandatory acknowledgment of receipt and understanding for key personnel.

3. Risk Assessment

3.1 Methodology for Identifying ML/TF Risks

Done.com Inc. employs a structured, risk-based approach for identifying, assessing, and documenting money laundering (ML), terrorist financing (TF), and sanctions evasion risks inherent to its business operations. This methodology is designed to ensure effective and proactive risk management consistent with regulatory guidelines from FINTRAC and the PCMLTFA framework.

The following outlines Done.com Inc. 's comprehensive risk assessment methodology:

Step 1: Risk Identification

Done.com Inc. systematically identifies risks through analysis of various categories:

Customer Risk

- Types of customers (individuals, corporate entities, PEPs)
- Occupation or business activity of customers
- Customer geographic location or jurisdictional ties
- Expected transaction volume and frequency

Product and Service Risk

- OTC currency exchange activities
- Digital currency transactions
- High-value transactions or large cash activities
- Cross-border financial services

Geographic Risk

- Transactions involving jurisdictions identified as high-risk by FATF
- Countries subject to economic sanctions, embargoes, or terrorist activity
- Regions with weak AML/CFT regulatory enforcement

Delivery Channel Risk

- Face-to-face vs. non-face-to-face transactions
- Online or digital transaction channels
- Transactions involving third-party intermediaries or agents

Step 2: Risk Analysis and Assessment

Identified risks are analyzed and assigned ratings based on:

- **Likelihood** of the risk occurring
- **Impact or Severity** if the risk materializes

A clearly defined **risk rating scale** (e.g., low, medium, high) is applied to each identified risk factor. This allows Done.com Inc. to categorize and prioritize risks systematically.

Risk Rating	Definition	Required Action
Low	Risk unlikely; minimal potential impact	Standard due diligence
Medium	Moderate likelihood or potential impact	Enhanced monitoring and periodic review
High	Significant likelihood or severe impact	Enhanced due diligence, senior-level review

Step 3: Documentation of Risk Assessment

- Results from the risk identification and assessment are documented in a formal **Risk Assessment Matrix**.
- The documentation includes justification for assigned risk ratings, analysis of risk factors, and reference to the controls implemented to mitigate identified risks.

Step 4: Risk Mitigation and Controls

Based on the risk assessment outcomes, Done.com Inc. implements appropriate internal controls including:

- Enhanced Due Diligence (EDD) for high-risk customers
- Transaction monitoring tailored to risk ratings
- Special procedures or approvals for high-risk jurisdictions or activities
- Ongoing staff training focused on ML/TF risk awareness and detection

Step 5: Review and Ongoing Monitoring

- The ML/TF risk assessment methodology and results are reviewed at least **annually** or more frequently in response to regulatory changes, new products/services, emerging threats, or after significant business events.
- Continuous monitoring and periodic reassessment ensure the risk management process remains dynamic, effective, and responsive.

3.2 Risk Assessment Frequency and Triggers

Done.com Inc. conducts its ML/TF Risk Assessment on a regular and structured basis to maintain the effectiveness and relevance of its Compliance Program. The frequency of formal assessments and the triggers for interim reviews are as follows:

Regular Risk Assessment Schedule:

- **Annual Review:**
  A comprehensive risk assessment is conducted at least once per calendar year. The annual review ensures that risk ratings, identified threats, and corresponding control measures remain accurate, effective, and reflective of Done.com Inc. 's current operations and regulatory requirements.

Interim or Trigger-Based Reviews:

Additional risk assessments or updates are performed in response to specific events or triggers, including but not limited to:

- **Regulatory Changes:**
  - New or amended legislation, regulations, or FINTRAC guidelines.
  - Updates to international AML/CFT standards (e.g., FATF recommendations).
- **Business Model or Operational Changes:**
  - Introduction of new products, services, or delivery channels.
  - Entry into new geographic markets or jurisdictions.
  - Major operational changes, such as mergers, acquisitions, or significant growth in business volume.
- **Identified Compliance Issues or Incidents:**
  - Discovery of significant compliance gaps, control failures, or ineffective procedures.
  - Significant increase in suspicious or unusual transaction activity.
- **External Events or Emerging Threats:**
  - Publicly reported financial crime trends or typologies relevant to OTC and digital currency markets.
  - FATF or other regulatory body risk assessments or reports identifying new vulnerabilities or threats.

Documentation and Record-Keeping:

- Each assessment, whether scheduled or triggered, is thoroughly documented, including:
  - Date and reason for the assessment.
  - Identified risks, analysis, and changes to risk ratings.
  - Recommended adjustments or additional controls.
- Records of these assessments are retained for a minimum of **five years** and are readily accessible for internal review and regulatory inspection.

3.3 Customer and Product Risk Categories

Done.com Inc. classifies customers and products into distinct risk categories to apply proportionate and effective controls. This categorization is crucial for tailoring appropriate due diligence measures, transaction monitoring processes, and risk mitigation strategies.

Customer Risk Categories

Low Risk:

- Established customers with transparent business operations.
- Customers with verifiable legitimate sources of funds.
- Customers domiciled in jurisdictions with strong AML/CFT regulations and enforcement.

Medium Risk:

- Non-resident customers from jurisdictions with moderate AML/CFT controls.
- Customers conducting frequent but predictable OTC transactions.
- Small and medium-sized businesses engaged in regulated industries with clear ownership structures.

High Risk:

- Politically Exposed Persons (PEPs), their associates, and family members.
- Non-resident customers from high-risk or FATF-identified jurisdictions.
- Corporate entities with complex or opaque ownership structures.
- Customers involved in cash-intensive businesses or industries vulnerable to financial crime.
- Customers conducting frequent, large-value, or otherwise unusual transactions.
- Customers linked to sectors commonly associated with elevated ML/TF risks (e.g., cryptocurrency exchanges, money remitters, precious metal dealers).

Product and Service Risk Categories

Low Risk:

- Standard currency exchange transactions with low monetary thresholds.
- Domestic transactions within Canada involving established banks or regulated financial institutions.

Medium Risk:

- Cross-border OTC currency exchange services involving jurisdictions with moderate regulatory controls.

- Routine digital currency transactions involving regulated virtual asset service providers (VASPs).

High Risk:

- High-value currency exchange transactions, particularly involving cash.
- Digital currency transactions involving decentralized exchanges, peer-to-peer trading, or unregulated VASPs.
- OTC transactions involving significant privacy or anonymity features.
- Transactions involving jurisdictions under sanctions, FATF high-risk jurisdictions, or countries with weak AML/CFT regimes.

Risk Category Controls

The assignment of customers and products into these risk categories guides the application of corresponding AML/CFT measures:

Risk Category	Customer Due Diligence Measures	Transaction Monitoring Requirements	Approval Requirements
Low	Standard CDD procedures	Standard transaction monitoring thresholds	Routine operational approval
Medium	Enhanced identity verification, periodic review	Enhanced monitoring, additional scrutiny	Compliance officer oversight
High	Enhanced Due Diligence (EDD), extensive source of funds checks	Real-time or frequent monitoring, enhanced scrutiny	Senior management approval

3.4 Geographic and Transaction Risk Assessment

Done.com Inc. assesses both geographic and transactional risk factors to identify exposure to jurisdictions, transaction types, and behaviors that may indicate heightened risk of money laundering, terrorist financing, or sanctions evasion. This assessment guides the application of enhanced controls where required.

A. Geographic Risk Assessment

Geographic risk is assessed based on a customer's country of residence, transaction destination, or source of funds/jurisdictional involvement. Done.com Inc. uses reliable sources such as FATF, OSFI, Global Sanctions Lists, Transparency International, and the Basel AML Index to evaluate jurisdictions.

Geographic Risk Categories:

Risk Level	Criteria	Example Controls Applied
Low	Countries with strong AML/CFT legislation, FATF membership, and low corruption levels	Standard CDD, standard monitoring
Medium	Jurisdictions with moderate AML/CFT enforcement or higher levels of informal cash use	Enhanced CDD, targeted monitoring
High	FATF-listed jurisdictions, countries under sanctions or embargoes, or known secrecy havens	EDD, senior management approval, sanctions screening

Examples of High-Risk Jurisdictions (subject to ongoing review):

- Iran, North Korea, Myanmar
- Countries under UN, OSFI, or Magnitsky-related sanctions
- Jurisdictions known for high levels of corruption, terrorism financing, or organized crime

B. Transaction Risk Assessment

Transaction risk is assessed based on factors such as transaction type, size, frequency, parties involved, and the nature of the asset class. OTC and digital currency transactions can present unique risks, especially when involving anonymity, cross-border elements, or high volumes.

Transaction Risk Indicators:

Risk Level	Indicators	Example Controls Applied
Low	Routine, face-to-face FX transactions under set thresholds	Standard monitoring
Medium	Digital asset transfers involving moderate values, repeatable customer patterns	Pattern recognition, enhanced review
High	Large-value or high-frequency trades, crypto-to-fiat transactions, transactions with no clear economic rationale, or use of mixers/tumblers	Real-time alerting, EDD, source of funds/wealth documentation

High-Risk Transaction Types:

- Crypto-to-cash or cash-to-crypto conversions over reporting thresholds
- Multiple small transactions structured to avoid reporting (smurfing)

- Transactions involving shell companies or complex layering
- Third-party transactions where the customer is not the beneficiary or sender

Integrated Risk Scoring Approach

Done.com Inc. combines geographic and transaction risk ratings to generate an **overall transaction risk score**, which determines:

- Whether the transaction is permitted
- The level of due diligence and review required
- Escalation or approval workflows

Sample Combined Risk Matrix:

Geographic Risk ↓ Transaction Risk →	**Low**	**Medium**	**High**
Low	Low	Medium	High
Medium	Medium	Medium	High
High	High	High	Prohibited/EDD Required

3.5 Documentation and Record-Keeping of Risk Assessments

Done.com Inc. maintains thorough documentation of all risk assessments to support the integrity, traceability, and effectiveness of its Compliance Program. These records provide an auditable trail of how ML/TF risks are identified, assessed, categorized, and mitigated, in accordance with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), its Regulations, and FINTRAC guidance.

Risk Assessment Documentation Requirements

The following elements must be documented in each risk assessment:

- **Date of Assessment**
  Date when the risk assessment was completed or last updated.
- **Purpose/Trigger**
  Explanation of whether the assessment is part of the scheduled annual review or a result of a triggering event (e.g., regulatory change, new product launch, internal audit finding).
- **Scope and Methodology**
  Description of the approach used, including risk categories assessed (customer, product/service, geography, delivery channel) and rating criteria (likelihood, impact).
- **Findings**
  Summary of identified risk levels across categories, including notable high-risk areas or emerging concerns.

- **Mitigation Measures**
  Controls and procedures implemented to address identified risks, including updates to transaction monitoring, customer due diligence, or training protocols.
- **Approvals and Sign-Offs**
  Evidence of review and sign-off by the Compliance Officer and, where applicable, senior management or the Board of Directors.
- **Supporting Materials**
  - Data sources and risk indicators used (e.g., FATF lists, sanctions databases, transaction logs)
  - Risk scoring matrices or summaries
  - Meeting minutes or audit comments (if applicable)

Retention Requirements

- All risk assessment records must be retained for a minimum of **five (5) years** from the date of creation or last update, in compliance with PCMLTFA requirements.
- Records may be maintained in **electronic or physical format**, provided they are:
  - Securely stored;
  - Easily retrievable for internal audits, compliance reviews, or regulatory examinations;
  - Protected from unauthorized access, tampering, or deletion.

Version Control and Change Logs

- Each version of the risk assessment must be labeled with:
  - A unique version number;
  - The date of revision;
  - A description of changes made;
  - The name(s) of the reviewer(s) and approver(s).
- A **Risk Assessment Change Log** must be maintained to track updates over time.

3.6 Risk Assessment Matrix

Risk Category	Risk Factor	Likelihood	Impact	Risk Rating	Mitigation Measures / Controls
Customer Risks	Politically Exposed Persons (PEPs)	High	High	High	Enhanced due diligence; senior management approval required.
Customer Risks	Non-resident customers	Medium	Medium	Medium	Enhanced customer due diligence; ongoing monitoring.
Customer Risks	Corporate entities with complex ownership structures	Medium	High	High	Beneficial ownership verification; detailed source of funds verification.
Customer Risks	Customers involved in cash-intensive businesses	High	High	High	Enhanced transaction monitoring; limits on cash transactions.
Customer Risks	Customers conducting frequent high-value transactions	High	High	High	Enhanced due diligence; periodic account review.
Product/Service Risks	OTC currency exchange services	Medium	Medium	Medium	Transaction monitoring thresholds; EDD for unusual patterns.
Product/Service Risks	Digital currency transactions	High	High	High	Blockchain monitoring; enhanced customer verification.
Product/Service Risks	Cross-border financial transactions	High	Medium	High	Sanctions screening; detailed transaction reporting.
Product/Service Risks	High-value transactions	High	High	High	Enhanced due diligence; mandatory source of funds verification.
Geographic Risks	Transactions involving FATF high-risk jurisdictions	High	High	High	Geographic risk scoring; enhanced monitoring and reporting.
Geographic Risks	Countries under international sanctions/embargoes	Medium	High	High	Sanctions list screening; strict compliance controls.
Geographic Risks	Regions known for high corruption or terrorist activity	Medium	High	High	Enhanced due diligence; additional management oversight.
Delivery Channel Risks	Non-face-to-face transactions (Online/Digital)	Medium	Medium	Medium	Multi-factor authentication; enhanced digital verification methods.
Delivery Channel Risks	Use of third-party intermediaries or agents	Medium	Medium	Medium	Strict vetting processes for third parties; periodic audits.
Delivery Channel Risks	Anonymous or pseudonymous transaction capabilities	High	High	High	Prohibition or strict limitation of anonymous transactions; identity verification required.

4. Customer Identification and Verification

4.1 Customer Due Diligence (CDD) Procedures

Done.com Inc. implements a structured Customer Due Diligence (CDD) process to verify the identity of customers, assess the legitimacy of their financial activities, and ensure compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, its associated Regulations, and FINTRAC guidance. These procedures are proportionate to the customer's risk level and the nature of the products or services being accessed.

A. When CDD Is Required

CDD must be conducted in the following circumstances:

- Prior to entering into a business relationship with a customer.
- Before executing a transaction equal to or exceeding CAD 10,000 (single or aggregated over 24 hours).
- When conducting virtual currency transactions equivalent to CAD 1,000 or more.
- When there are reasonable grounds to suspect the customer or transaction is related to ML/TF.
- When there is doubt about the veracity or adequacy of previously obtained customer information.

B. CDD Process Overview

1. **Identification and Verification**
    - **Individuals**:
        - Full legal name
        - Date of birth
        - Residential address
        - Government-issued photo ID (validated through physical, digital, or dual-process methods)
    - **Corporations and Legal Entities**:
        - Full legal name and registration number
        - Incorporation documents or registry extracts
        - Names of directors and authorized signatories
        - Identification of beneficial owners (individuals owning ≥25%)
2. **Purpose and Intended Nature of Relationship**
    - Collect information about:
        - The reason for opening the account or executing a transaction
        - The expected transaction volume, types, and frequency
        - The customer’s source of funds and, when applicable, source of wealth

3. **Ongoing Monitoring**
    - Monitor transactions to ensure they are consistent with the customer's profile.
    - Identify deviations from expected behavior and escalate unusual or suspicious activity for review.
    - Refresh CDD documentation periodically based on risk rating:
        - **Low Risk**: Every 2–3 years
        - **Medium Risk**: Every 1–2 years
        - **High Risk**: Annually or more frequently as needed

C. Record-Keeping Requirements

- Retain all CDD documentation (including ID copies and verification logs) for **at least five (5) years** after the end of the relationship or transaction.
- Ensure records are secure, accessible, and retrievable for FINTRAC or law enforcement upon request.

D. CDD Failures

- If a customer refuses or fails to provide required identification:
    - Do not open the account or proceed with the transaction.
    - Consider filing a Suspicious Transaction Report (STR) if appropriate.
    - Escalate to the Compliance Officer for further review and risk mitigation.

E. Technology and Automation

- Where applicable, Done.com Inc. uses secure digital onboarding tools (e.g., liveness detection, biometric verification, secure upload of ID documents) to streamline the CDD process without compromising compliance or security.

4.2 Enhanced Due Diligence (EDD) for High-Risk Customers

Enhanced Due Diligence (EDD) is a critical control applied by Done.com Inc. when dealing with customers or transactions that present elevated risk of money laundering, terrorist financing, or sanctions evasion. EDD involves deeper investigation, greater scrutiny, and heightened ongoing monitoring. The following outlines Done.com Inc. 's EDD procedures for three key high-risk categories:

A. Politically Exposed Persons (PEPs)

A **PEP** is an individual who holds or has held a prominent public position, such as:

- Heads of state or government
- Senior politicians or government officials

- Judges, military officials, ambassadors
- Family members and close associates of such individuals

EDD Procedures for PEPs:

- Identify whether the customer is a foreign or domestic PEP, or a close associate.
- Obtain senior management approval before establishing or continuing the business relationship.
- Obtain source of funds and **source of wealth** documentation.
- Perform ongoing enhanced monitoring of transactions for inconsistencies or red flags.
- Re-screen PEP status regularly (minimum annually or based on relationship risk).

B. High-Risk Jurisdictions

These are countries or territories:

- Listed by FATF as high-risk or non-cooperative
- Subject to sanctions or embargoes (e.g., under the **United Nations Act**, **Magnitsky Law**, etc.)
- Known for corruption, weak AML/CFT enforcement, or secrecy practices

EDD Procedures for High-Risk Jurisdictions:

- Flag all clients with nationality, residency, or transactional ties to such jurisdictions.
- Require documented justification for engaging in business with those clients.
- Collect detailed information on the purpose and expected nature of the relationship.
- Perform sanctions screening at onboarding and in real time during transactions.
- Apply stricter transaction limits and higher thresholds for automated alerts.

C. Correspondent Banking Relationships

(*Applicable if* Done.com Inc. *enters a relationship with another financial institution*)

A **correspondent banking relationship** involves the provision of services by one financial institution (the correspondent) to another (the respondent). These relationships carry heightened risk due to:

- Lack of direct access to the respondent's customers
- Use of nested or indirect accounts
- Cross-border activity

EDD Procedures for Correspondent Relationships:

- Perform detailed due diligence on the respondent institution:

  - Licensing and regulatory status
  - Ownership structure and control
  - Quality of their AML/CFT controls
  - Reputation and any history of regulatory violations
- Obtain senior management approval prior to onboarding.
- Document the nature and intended purpose of the relationship.
- Ensure written agreement that the respondent has implemented effective AML/CFT programs.
- Periodically review the relationship, including audit reports and transactional activity.

4.3 Non-Face-to-Face Verification Procedures

Done.com Inc. recognizes that non-face-to-face onboarding and transaction processing—particularly in digital environments—can present increased money laundering and terrorist financing risks. To address these risks, Done.com Inc. applies strict and well-documented **Non-Face-to-Face (NFTF) Verification Procedures** that comply with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)** and align with FINTRAC guidance.

A. When NFTF Verification Is Required

Non-face-to-face identity verification procedures are used when:

- Customers open accounts remotely via digital platforms or online portals.
- Transactions are initiated without in-person interaction.
- Business relationships are conducted entirely through virtual channels.

B. Approved NFTF Verification Methods

Done.com Inc. uses one or more of the following FINTRAC-approved verification methods to verify identity in a non-face-to-face context:

1. **Dual-Process Method**
   - Obtain information from two different, reliable, and independent sources.
   - One source must confirm the individual's **name and address**; the other must confirm the **name and date of birth**.
   - Acceptable sources include:
     - Utility bills
     - Government-issued records (e.g., CRA notices)
     - Credit bureau files
     - Bank or credit card statements from a Canadian financial institution
2. **Credit File Method**
   - Use a Canadian credit bureau to confirm identity.

   - The credit file must be at least **three years old**, and match the person's name, date of birth, and address.
   - This method must be performed by Done.com Inc. , not the customer.
3. **Government-Issued Photo ID Method (with technology)**
   - Obtain a scan or image of a **valid government-issued photo ID** (e.g., passport, driver's license).
   - Use a **secure and reliable technology** to:
     - Verify authenticity (e.g., holograms, MRZ codes)
     - Match the customer's face to the ID using facial recognition or live video verification
   - Ensure the process is auditable, recorded, and secure.

C. Supplementary Controls for NFTF Verification

To further reduce risk when verifying identity remotely, Done.com Inc. applies the following controls:

- **Liveness Detection**: Use biometric tools to confirm the customer is physically present (not using a photo or recording).
- **IP Geolocation & Device Fingerprinting**: Monitor for IP address anomalies and device signatures inconsistent with the claimed location.
- **Sanctions & PEP Screening**: Screen all customers during onboarding using global watchlists and PEP databases.
- **Transaction Pattern Profiling**: Implement stricter limits and flagging thresholds during early-stage account use.
- **Two-Factor Authentication (2FA)**: Enforce MFA (e.g., SMS/Authenticator app) for account access and transactional approvals.

D. Documentation and Record-Keeping

- All identity verification attempts and supporting evidence must be securely documented and stored for **a minimum of five (5) years**.
- Screenshots, timestamps, technology logs, and verification results must be available for audit and FINTRAC review.

E. Failure to Verify Identity

- If Done.com Inc. cannot verify a customer's identity through approved NFTF methods:
  - The account will not be opened, or the transaction will not proceed.
  - The case will be escalated to the Compliance Officer.
  - A **Suspicious Transaction Report (STR)** may be filed if there are reasonable grounds.

4.4 Beneficial Ownership Identification

To maintain transparency and mitigate risks associated with money laundering, terrorist financing, and hidden ownership structures, Done.com Inc. performs strict due diligence to identify and verify the **beneficial ownership** of all business clients. These procedures are in accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and **Regulations**, and reflect current FINTRAC guidance.

A. Definition of Beneficial Ownership

Beneficial owners are the natural persons who ultimately:

- **Own or control 25% or more** of a corporation or other entity, directly or indirectly; or
- **Control the entity through other means** (e.g., voting rights, decision-making power); or
- **Exercise de facto control** if no one meets the above criteria.

For trusts and similar arrangements:

- The settlor, trustees, and known beneficiaries are treated as beneficial owners.

B. Information to Be Collected

Done.com Inc. collects the following from each beneficial owner of a business client:

- Full legal name
- Date of birth
- Address and nationality
- Type and percentage of ownership or control
- Nature of control (ownership, voting rights, influence through agreements)

Additionally, Done.com Inc. documents the **ownership structure** of the entity using organizational charts or written declarations.

C. Verification of Beneficial Ownership

Verification of beneficial ownership is risk-based and must be completed **before or shortly after** establishing a business relationship:

- **Low/Medium Risk Clients**:
  - Accept written attestations from directors, executives, or legal counsel.
  - Use publicly available records (e.g., corporate registries).
  - Obtain legal incorporation documents or shareholder agreements.
- **High-Risk Clients**:

- Independently verify ownership through third-party databases or legal documents.
- Require notarized declarations or audited financial statements.
- Escalate for Compliance Officer or senior management approval.

D. Record-Keeping and Updates

- Maintain a **register of beneficial owners** for each business client.
- Update beneficial ownership information:
  - At least **annually** for high-risk clients.
  - Immediately upon notification or discovery of changes.
- All records must be **retained for at least 5 years** after the end of the business relationship.

E. Inability to Identify Beneficial Owners

If Done.com Inc. cannot obtain or verify beneficial ownership:

- The business relationship will not be established.
- Existing relationships may be restricted or terminated.
- A **Suspicious Transaction Report (STR)** will be filed if warranted.
- The matter is escalated to the Compliance Officer for risk mitigation actions.

4.5 Third-Party Determination and Documentation

Done.com Inc. is required under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)** to determine whether a person or entity is conducting a financial transaction or business relationship **on behalf of a third party**. This requirement is essential for detecting and preventing the misuse of Done.com Inc. 's services for concealing the identity of the true party behind a transaction.

A. When Third-Party Determination is Required

Third-party determination must be made when:

- A person or entity opens an account, executes a transaction, or initiates a business relationship.
- There are **reasonable grounds to suspect** that the customer is acting on behalf of another party, regardless of whether a formal declaration has been made.

B. Questions to Ask the Customer

As part of the onboarding and transaction process, Done.com Inc. will ask the customer:

1. **"Are you conducting this transaction or opening this account on behalf of another individual or entity?"**
2. If yes, then Done.com Inc. must obtain:
    - The third party's full legal **name**;
    - Their **address**;
    - Their **date of birth** (if an individual);
    - The **relationship** between the customer and the third party;
    - The **nature of the third party's business or occupation**.

C. Documentation Requirements

If the customer confirms third-party involvement:

- Document the **identity and role** of the third party in Done.com Inc. 's records.
- Use a standardized **Third-Party Declaration Form**.
- Record the **method of verification** (if applicable).
- Retain copies of supporting documentation (e.g., corporate agreements, instructions, declarations).

All information must be:

- Stored **electronically and/or physically** in a secure system;
- Retained for a **minimum of five (5) years** from the date of the transaction or end of the relationship;
- Made readily available for internal audit or regulatory inspection upon request.

D. Reasonable Grounds to Suspect Third-Party Activity

Done.com Inc. trains staff to recognize indicators of third-party activity, such as:

- The customer lacks knowledge of transaction details.
- Instructions appear to be relayed from someone else.
- The customer refuses to disclose the origin of funds.
- Patterns suggest layering or structured transactions.

If suspicion arises, even without confirmation, the transaction may be:

- Escalated to the **Compliance Officer**;
- Flagged for further review;
- Subject to a **Suspicious Transaction Report (STR)** if warranted.

E. Ongoing Monitoring and Review

- Third-party information is reviewed and refreshed as part of Done.com Inc. 's **ongoing monitoring** program.
- Material changes in the customer's behavior or relationship structure will trigger **reassessment**.

5. Transaction Monitoring and Reporting

5.1 Procedures for Ongoing Monitoring of Transactions

Done.com Inc. maintains a robust and risk-based system for **ongoing monitoring** of customer transactions to detect, assess, and report suspicious activities that may indicate money laundering (ML), terrorist financing (TF), sanctions evasion, or other financial crimes. Ongoing monitoring is essential for ensuring that customer activity aligns with the information obtained during onboarding and throughout the business relationship.

A. Objectives of Ongoing Monitoring

- Detect transactions inconsistent with the customer's known profile.
- Identify changes in behavior, risk level, or beneficial ownership.
- Assess patterns or anomalies that may warrant escalation or reporting.
- Ensure timely updates to customer due diligence (CDD) and risk ratings.

B. Monitoring Approach

Done.com Inc. applies a **risk-based approach**, meaning the **frequency, depth, and method of monitoring** depend on the risk level of the customer and product:

Risk Level	Monitoring Frequency	Controls Applied
Low	Periodic reviews (annually)	Basic transaction pattern checks; automated rule-based alerts
Medium	Ongoing	Threshold alerts; pattern recognition; manual spot checks
High	Continuous	Real-time alerts; enhanced analytics; Compliance review queue

C. Key Elements of Monitoring Procedures

1. **Transaction Profiling**
    - Establish a baseline for each customer's expected activity (volume, frequency, type, asset class).

- Profiles are based on data collected during onboarding and updated regularly.

2. **Automated Monitoring Tools**
   - Monitor transaction activity for red flags such as:
     - Structuring (smurfing)
     - Sudden large volume trades
     - Rapid movement between fiat and digital assets
     - Use of high-risk jurisdictions or addresses
   - Alerts are generated based on pre-set thresholds and behavior models.
3. **Manual Review and Investigation**
   - Compliance team investigates triggered alerts or inconsistencies.
   - Transaction logs, communications, and identity data are reviewed.
   - Justifications or supporting documents may be requested from the customer.
4. **Risk Rating Adjustments**
   - Customer risk ratings are adjusted if new information or activity indicates elevated ML/TF risk.
   - Increased risk may trigger Enhanced Due Diligence (EDD), reporting obligations, or offboarding.
5. **Link Analysis & Sanctions Screening**
   - Screen all transactions and counterparty data against:
     - Sanctions lists (e.g., OSFI, UN, US OFAC)
     - PEP and adverse media databases
     - Blockchain risk scoring providers (for digital assets)

D. Escalation and Reporting

- If a transaction or series of transactions is deemed suspicious:
  - The Compliance Officer is notified immediately.
  - A Suspicious Transaction Report (STR) is filed with **FINTRAC** as required by law.
  - Customer account activity may be paused pending review.

E. Documentation and Retention

- All alerts, investigations, and monitoring decisions are fully documented.
- Records of monitoring activities, flagged transactions, and communications must be kept for **at least five (5) years**.
- These records must be accessible for audits and regulatory reviews.

5.2 Identification and Handling of Unusual Transactions

Done.com Inc. maintains rigorous procedures for identifying, assessing, and responding to **unusual transactions**—those that deviate from a customer's known activity or raise red flags for money laundering, terrorist financing, or other illicit purposes. These procedures are integral to the company's overall AML/ATF framework and comply with the requirements of the **Proceeds**

of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated regulations.

A. Definition of an Unusual Transaction

An **unusual transaction** is one that:

- Appears inconsistent with a customer's known profile or stated purpose;
- Involves activity significantly above or below typical transaction volumes;
- Includes unexpected use of high-risk jurisdictions, counterparties, or assets;
- Involves complex or unnecessarily layered structures;
- Cannot be readily explained or justified by the customer.

Unusual transactions are not automatically suspicious but must be **reviewed and documented** to determine if further action is required.

B. Common Indicators of Unusual Transactions

Examples of triggers for review include:

Transaction Type	Potential Red Flags
Crypto-to-Fiat Conversions	Frequent conversions with no apparent source of wealth
Large OTC Trades	Sudden large-value trades inconsistent with prior activity
Cross-Border Transfers	Use of sanctioned or high-risk jurisdictions
Multiple Transactions	Structuring or smurfing behavior below reporting thresholds
Third-Party Activity	Use of intermediaries or non-transparent counterparties
Anonymous Wallets or Mixers	Funds routed through privacy-enhancing technologies

C. Detection Process

1. **Automated Alerts**
    - Triggered by rule-based thresholds, pattern deviations, or blockchain risk analytics.
    - Include real-time alerts for high-risk transaction types or jurisdictions.
2. **Manual Review**
    - Alerts are reviewed by the Compliance team for context and documentation.
    - Analysts assess whether the transaction is explainable and aligned with the customer's risk profile.

3. **Customer Contact (If Needed)**
    - Customers may be asked to provide clarification, contracts, or source of funds documents.
    - All communications are recorded as part of the case file.

D. Escalation and Action

If a transaction is determined to be:

- **Justified**: No further action; the rationale is documented.
- **Unusual but not suspicious**: Enhanced monitoring may be applied.
- **Suspicious**: An **STR (Suspicious Transaction Report)** is prepared and submitted to FINTRAC promptly.

Transactions subject to escalation may also trigger:

- A review of the customer's risk rating
- Temporary transaction holds
- Reporting to law enforcement (in cases of immediate threat or criminal activity)

E. Record-Keeping

- All unusual transactions and related investigations must be documented and retained for **at least 5 years**.
- Documentation must include:
    - Description of the transaction
    - Reason for flagging
    - Details of the investigation and outcome
    - Any communication with the client
    - Actions taken (e.g., STR filed, account restrictions applied)

5.3 Suspicious Transaction Reporting (STRs)

Done.com Inc. is legally obligated to detect and report **suspicious transactions** that may be related to money laundering (ML), terrorist financing (TF), or other criminal activity. This obligation is outlined in Section 7 of the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and enforced by **FINTRAC**. The process of identifying, documenting, and reporting such transactions is critical to the integrity of Done.com Inc. 's compliance program.

A. What Is a Suspicious Transaction?

A **suspicious transaction** is any transaction—completed or attempted—that:

- Gives reasonable grounds to suspect it is related to the commission or attempted commission of a money laundering or terrorist activity financing offence;
- Appears inconsistent with the customer's known profile or typical activity;
- Involves unusually complex or opaque structures with no apparent economic purpose;
- Cannot be reasonably explained or justified by the customer.

Note: A transaction can be suspicious even if it does not involve large amounts or is not completed.

B. Reporting Obligations

- Suspicious transactions must be reported to **FINTRAC** using the **Suspicious Transaction Report (STR)** format as soon as practicable after the suspicion arises.
- STRs must be submitted even if:
    - The transaction is not completed;
    - The customer refuses to proceed;
    - No specific offence is identified.

C. STR Identification and Escalation Workflow

1. **Detection**
    - Triggered through automated alert systems or manual monitoring.
    - Any employee who identifies suspicious behavior must escalate to the **Compliance Officer** immediately.
2. **Initial Review**
    - The Compliance Officer assesses the transaction against the customer’s KYC file, historical behavior, and applicable risk indicators.
3. **Investigation**
    - Additional documentation or justification may be requested from the customer.
    - Link analysis, sanctions screening, and transaction history reviews are performed.
4. **Decision**
    - If suspicion remains, the Compliance Officer drafts and submits the STR to FINTRAC using the secure online portal.
5. **Post-Submission**
    - The transaction and account are flagged for enhanced monitoring.
    - Internal records are updated with the STR reference number and summary.

D. Contents of an STR

A properly completed STR must include:

- Customer details (full name, DOB, address, occupation)

- Transaction details (type, amount, time, parties involved)
- Nature and rationale of the suspicion
- Supporting documents or data used in the investigation

E. Confidentiality Requirements

- Customers must **not** be informed that a suspicious transaction report is being filed.
- The existence or content of an STR is strictly confidential and may only be discussed with:
    - FINTRAC;
    - Law enforcement (if legally compelled);
    - Relevant internal compliance personnel.

F. Record-Keeping

- A copy of each STR submitted, including any supporting documentation and internal correspondence, must be:
    - Retained securely for **five (5) years**;
    - Protected against unauthorized access or disclosure;
    - Made available upon request to FINTRAC or law enforcement.

5.4 Large Cash Transaction Reporting (LCTRs)

As a registered Money Services Business (MSB), Done.com Inc. is legally obligated under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** to report **Large Cash Transactions (LCTRs)** to **FINTRAC**. This requirement supports transparency and helps identify potential money laundering activity involving physical cash.

A. What Is a Large Cash Transaction?

A **Large Cash Transaction** involves the receipt of **CAD $10,000 or more in cash**, either in:

- A single transaction; or
- Two or more transactions that occur **within 24 consecutive hours** and together total CAD $10,000 or more, **if the transactions are by or on behalf of the same person or entity**.

Note: Only **physical currency** (i.e., notes and coins) is considered a "cash" transaction for LCTR purposes—cheques, wire transfers, or crypto assets do **not** qualify.

B. Reporting Requirements

- A **Large Cash Transaction Report (LCTR)** must be submitted to **FINTRAC within 15 calendar days** of the transaction date.

- If a suspicious element is also detected, a **Suspicious Transaction Report (STR)** must be submitted separately and **must not be delayed** by the LCTR.

C. LCTR Submission Process

1. **Trigger Detection**
   - System or staff detects that a cash transaction has reached or exceeded CAD $10,000.
   - Aggregation rules apply to cash received from the same customer within a 24-hour period.
2. **Information Collection**
   The following must be recorded:
   - Full legal name and address of the individual/entity
   - Occupation or nature of business
   - Date of birth (for individuals)
   - Transaction amount, currency, and purpose
   - Method of cash delivery (e.g., in-person, drop-off)
   - Name and details of person conducting the transaction (if different from the account holder)
   - Identification document(s) used (type, number, issuing jurisdiction)
3. **Verification**
   - Identity of the person must be verified through an approved FINTRAC method (photo ID, dual-process, credit file, etc.).
4. **Submission**
   - The Compliance Officer or designated compliance delegate submits the LCTR via the FINTRAC secure web form.

D. Record-Keeping Requirements

Done.com Inc. must retain records of all LCTRs, including:

- A copy of the report submitted
- Supporting documentation and identification records
- Internal review notes, if any
- Submission date and confirmation

All records must be:

- **Retained for at least five (5) years** from the transaction date
- **Securely stored and accessible** only to authorized personnel

E. Exemptions and Limitations

LCTR reporting **does not apply** when:

- The funds are **not cash** (e.g., crypto, cheque, EFT)
- The cash is **not received directly by** Done.com Inc.
- The transaction is conducted **between financial institutions**

Done.com Inc. does **not** accept cash payments except in designated OTC locations with secure handling protocols. All such instances are monitored and logged by compliance staff.

5.5 Electronic Funds Transfer (EFT) Reporting

Done.com Inc. complies with mandatory Electronic Funds Transfer (EFT) reporting requirements under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and associated **Regulations**. These obligations are designed to increase transparency of cross-border movements of funds and help detect and deter money laundering, terrorist financing, and sanctions evasion.

A. What Is an EFT?

An **Electronic Funds Transfer (EFT)** includes any transmission of instructions for a financial transaction via electronic means (e.g., SWIFT, wire transfer, blockchain protocol) that:

- Is initiated **at the request of a client**;
- Involves the **transfer of CAD $10,000 or more** (or equivalent in foreign currency);
- Is **sent to or received from a person or entity outside of Canada**, including both incoming and outgoing transfers.

EFTs do not include:

- Internal transfers between accounts held by the same person/entity at Done.com Inc. ;
- Transfers that do not cross a border;
- Payments made using a credit or debit card for purchasing goods/services.

B. When an EFT Report Must Be Filed

Done.com Inc. must report to FINTRAC **within 5 working days** of:

- Sending out an international EFT of CAD $10,000 or more;
- Receiving an international EFT of CAD $10,000 or more;
- Aggregating two or more smaller EFTs within a **24-hour period** that together total CAD $10,000 or more, from or to the same person/entity.

C. Required Information for EFT Reports

When reporting an EFT, the following must be documented and submitted to FINTRAC:

- Name and address of the **originator** (for outgoing EFTs) or **beneficiary** (for incoming EFTs)
- The **person/entity requesting or receiving** the transfer
- The **name and address of the recipient financial institution**
- The **amount and currency** of the transaction
- The **date and purpose** of the transaction
- Method of delivery (e.g., bank transfer, blockchain)
- Identifying information such as client ID, wallet address, or financial account number

D. Reporting Workflow

1. **Detection**
   - Systems automatically flag or queue international transactions ≥ CAD $10,000.
2. **Verification**
   - Compliance staff reviews customer and transaction details.
   - Identity is confirmed and documentation verified.
3. **Submission**
   - The EFT report is submitted to FINTRAC via the secure web portal within **5 business days** of the transaction.
4. **Post-Submission**
   - Transactions are reviewed for patterns that may require additional compliance action (e.g., STR).

E. Record-Keeping

Done.com Inc. must retain the following for all reportable EFTs:

- A copy of the EFT report submitted to FINTRAC
- All supporting documentation (e.g., KYC, source of funds, payment confirmations)
- Internal communications or rationale used during investigation

These records must be:

- **Kept for a minimum of 5 years**
- **Stored securely**, with access restricted to compliance-authorized personnel
- **Available for audit** by FINTRAC or law enforcement upon request

F. Risk Controls and Monitoring

- Automated threshold detection is applied to all wallet-based or bank-based transfers.
- Blockchain analytics tools are used for crypto transfers to monitor counterparties, risk scores, and jurisdictional exposure.
- Customers conducting frequent or large cross-border EFTs are subject to **enhanced due diligence (EDD)** and closer monitoring.

5.6 Virtual Currency Transaction Reporting (VCTRs)

As a registered Money Services Business (MSB) dealing in digital assets, Done.com Inc. is required to comply with **Virtual Currency Transaction Reporting (VCTR)** requirements under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and associated **Regulations**. These obligations aim to improve transparency, traceability, and oversight in the virtual currency space, particularly for significant-value transactions.

A. What Is a Virtual Currency Transaction Report (VCTR)?

A **VCTR** is required when Done.com Inc. **receives** or **sends** a virtual currency transaction of **CAD $10,000 or more** in a single transaction, or in two or more transactions that occur within **24 hours** and total CAD $10,000 or more **from or to the same person or entity**.

Virtual currency includes:

- Bitcoin (BTC)
- Ethereum (ETH)
- Stablecoins (e.g., USDC, USDT)
- Other blockchain-based cryptocurrencies or tokens

B. When to File a VCTR

A VCTR must be submitted to FINTRAC **within 5 business days** of:

- Receiving virtual currency equivalent to CAD $10,000 or more;
- Sending virtual currency equivalent to CAD $10,000 or more;
- Aggregating transactions over 24 hours from/to the same party that meet or exceed CAD $10,000.

VCTRs apply **whether the counterparty is inside or outside Canada** and **whether the customer is an individual or entity**.

C. Required Information for VCTR

Done.com Inc. must collect and report the following information:

1. Customer Information:

- Full name
- Address
- Date of birth (if individual)
- Occupation or business type

- Client reference number (e.g., internal ID)

2. Transaction Information:

- Date and time
- Type of virtual currency (e.g., BTC, ETH)
- Amount in both virtual currency and CAD equivalent
- Blockchain wallet addresses involved
- Transaction hash (TxID)
- Purpose and context (e.g., trade, OTC settlement, payout)

3. Counterparty Information (if available):

- Name and address of sender/receiver
- Wallet ownership and relationship to client
- Jurisdiction of wallet provider (e.g., exchange, DeFi protocol)

D. VCTR Submission Process

1. **Transaction Detection:**
   - Automated flagging of incoming/outgoing virtual currency ≥ CAD $10,000.
   - 24-hour rolling aggregation for split transactions.
2. **Compliance Review:**
   - Verify customer identity and KYC file.
   - Conduct blockchain analysis for wallet risk (e.g., mixers, sanctioned entities).
3. **VCTR Submission:**
   - Submit report to FINTRAC using the secure online platform within 5 business days.
   - Maintain log of transaction hash and internal case ID.

E. Record-Keeping Requirements

Done.com Inc. must retain all VCTR-related records, including:

- The submitted report and confirmation receipt
- Supporting evidence (e.g., blockchain screenshots, wallet risk analysis)
- Internal review notes and KYC details

These must be:

- **Retained for 5 years**
- **Securely stored** with controlled access
- **Available for FINTRAC or law enforcement inspection**

F. Risk-Based Controls for Virtual Currency

To support VCTR compliance and broader AML efforts, Done.com Inc. applies the following controls:

- **Blockchain analytics tools** to assess counterparty wallets and transaction patterns
- **Address risk scoring** to detect links to darknet markets, sanctioned entities, or mixers
- **Enhanced due diligence (EDD)** for high-volume or high-risk digital asset customers
- **Transaction pattern monitoring** for structuring or layering

5.7 Cross-Border Transaction Reporting

Done.com Inc. complies with cross-border transaction reporting obligations as outlined under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and its Regulations. Cross-border reporting is an essential part of Done.com Inc. 's compliance framework, particularly given the nature of its over-the-counter (OTC) services across fiat and digital currencies, which frequently involve **international counterparties**.

A. Cross-Border Reporting Obligations

Under Canadian regulations, cross-border transaction reporting is fulfilled through:

- **Electronic Funds Transfer Reports (EFTs)** – when funds (CAD $10,000 or more) are transferred internationally.
- **Virtual Currency Transaction Reports (VCTRs)** – when digital assets (equivalent to CAD $10,000 or more) are sent to or received from outside Canada.

There is **no separate "cross-border" report**, but international movement of value must be captured through **EFT** or **VCTR** as applicable.

B. Scope of Cross-Border Transactions

Done.com Inc. considers a transaction cross-border if:

- Funds or digital assets **leave or enter Canada**, regardless of the client's location.
- The counterparty is located **outside Canada**, or the wallet/bank destination is internationally hosted.
- The originator or beneficiary financial institution is **foreign-based**.

This applies to:

- Wire transfers

- Blockchain transactions
- Payments to/from foreign counterparties or exchanges

C. Identification and Classification

Each cross-border transaction is assessed based on:

- **Type of asset** (fiat vs. virtual currency)
- **Jurisdiction of sender/receiver**
- **Routing method** (e.g., SWIFT, SEPA, blockchain)
- **Transaction value and frequency**
- **Associated customer risk profile**

Any transaction over the **CAD $10,000 threshold** will trigger:

- **EFT Report** if fiat;
- **VCTR** if digital currency;
- **STR** if suspicious indicators are present.

D. Monitoring and Reporting Process

1. **Automated Detection**
    - Transaction monitoring systems flag:
        - Transfers to/from non-Canadian IBANs or SWIFT codes
        - Wallet addresses geolocated to high-risk jurisdictions
        - IP address metadata during platform use
2. **Compliance Review**
    - Conduct origin/destination verification
    - Assess for potential structuring, layering, or sanctions risk
3. **Reporting**
    - Submit required EFT or VCTR to FINTRAC **within 5 business days**
    - If suspicion exists, file an accompanying **Suspicious Transaction Report (STR)**

E. Supporting Risk Controls

Done.com Inc. enhances cross-border transaction controls via:

- **Geo-fencing and wallet address risk-scoring**
- Screening all counterparties and intermediaries against:
    - **Sanctions lists** (OFAC, UN, OSFI)
    - **FATF grey/blacklisted countries**
    - **Adverse media** and PEP lists
- Requiring **enhanced due diligence (EDD)** for clients transacting with high-risk jurisdictions

F. Record-Keeping

All cross-border transactions subject to reporting are fully documented, including:

- Transaction details and amount
- Jurisdictions involved
- Client identification and verification records
- Submission confirmation from FINTRAC

Records are **retained for a minimum of 5 years**, in accordance with regulatory obligations.

6. Record-Keeping and Documentation

6.1 Record Retention Policy

Done.com Inc. maintains a comprehensive **Record Retention Policy** to ensure that all client, transaction, and compliance-related records are stored securely, retrievable upon request, and retained in accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and applicable FINTRAC regulations.

This policy applies to both **physical and electronic records** and is designed to support transparency, regulatory compliance, internal audits, and investigations.

A. Retention Periods

The minimum record retention period for all reportable and non-reportable activity is **five (5) years**, calculated from the **date the record is created**, or from the **end of the business relationship**, whichever is later.

Record Type	Minimum Retention Period
Know Your Client (KYC) documents	5 years from last transaction or relationship end
Transaction records (fiat & crypto)	5 years from transaction date
Suspicious Transaction Reports (STRs)	5 years from date submitted
Large Cash Transaction Reports (LCTRs)	5 years from date submitted
Electronic Funds Transfer Reports (EFTs)	5 years from date submitted
Virtual Currency Transaction Reports (VCTRs)	5 years from date submitted
Risk assessments and mitigation records	5 years from date created or updated
Training records	5 years from training completion
Internal compliance audits & reviews	5 years from audit date
Third-party determination forms	5 years from transaction date or relationship end

B. Record Types and Format

Records may include but are not limited to:

- Customer identification and verification files
- Source of funds declarations
- Wallet addresses and blockchain transaction data
- Signed agreements and declarations
- Internal compliance reviews and approvals
- Communications with clients related to onboarding or flagged activity
- Case files related to STRs or investigations

Records may be stored in:

- Encrypted digital databases
- Secure cloud storage systems with audit trails
- Restricted-access internal servers
- Paper files stored in a locked, monitored environment (if applicable)

C. Security and Access Controls

To ensure integrity, confidentiality, and availability:

- Access to records is **restricted** to authorized personnel (Compliance, Legal, Audits).
- All records are **encrypted at rest and in transit** when stored electronically.
- Systems implement **multi-factor authentication (MFA)** and role-based permissions.
- Regular backups are performed, and offsite copies are maintained where appropriate.

D. Disposal and Destruction

After the five-year retention period (or longer if required by a legal hold), Done.com Inc. will:

- Permanently delete electronic records using secure data destruction tools.
- Shred or destroy paper records using cross-cut shredders or certified destruction services.
- Document the destruction process, including method, date, and responsible personnel.

No record will be destroyed if:

- It is subject to an active investigation, legal hold, or audit;
- Retention is required under tax, regulatory, or other laws.

E. Auditing and Quality Assurance

- Randomized audits of record storage systems are conducted **annually** to verify compliance.
- Any discrepancies, missing records, or access violations are reported to the **Compliance Officer** and addressed immediately.
- Compliance logs are reviewed and signed off by senior compliance staff or external reviewers, where applicable.

6.2 Types of Records to be Kept

To meet the compliance requirements under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and guidance issued by **FINTRAC**, Done.com Inc. maintains detailed records for all aspects of its operations, particularly those relating to **client identification**, **transactions**, **monitoring**, and **reporting**. These records ensure transparency, auditability, and support for investigations if necessary.

Below is a breakdown of the categories and specific types of records that must be retained.

A. Client Identification Records

These include documents and data collected during the onboarding and verification process:

- Full name, date of birth, address, occupation/business type
- Identification documents (e.g., driver's license, passport)
- Dual-process verification documentation (e.g., utility bill + credit file)
- Politically Exposed Person (PEP) declarations
- Source of funds and purpose of business relationship
- Beneficial ownership information (for entities)
- Third-party determination forms

B. Transaction Records

Records of financial transactions conducted by or on behalf of clients:

- OTC trade confirmations (including asset, volume, price, date/time)
- Incoming and outgoing wire transfers
- Virtual currency transfers (including wallet addresses and TxIDs)
- Trade execution records and communication logs
- Transaction authorizations and customer instructions
- Internal transaction notes or exception justifications

C. Reporting Records

Copies and supporting documentation for all regulatory filings submitted to FINTRAC:

- Suspicious Transaction Reports (STRs)
- Large Cash Transaction Reports (LCTRs)
- Electronic Funds Transfer Reports (EFTs)
- Virtual Currency Transaction Reports (VCTRs)
- Correspondence or receipts confirming report submission
- Internal notes and justifications related to each report

D. Monitoring and Risk Assessment Records

These include logs and assessments used to monitor client activity and determine risk levels:

- Ongoing transaction monitoring logs
- Risk assessment matrices and scoring models
- Blockchain analytics and wallet risk reports
- Internal case reviews and escalation memos
- Customer risk ratings and justification for risk level
- Geographic, product, and delivery channel risk profiles

E. Compliance Program and Internal Controls

Records documenting the design and operation of the compliance program:

- AML/ATF compliance policy and version history
- Updates to policies and procedures
- Roles and responsibilities matrix
- Internal compliance audits and testing outcomes
- Board or management compliance approvals
- Documentation of corrective actions taken after deficiencies

F. Training Records

Evidence of AML/ATF training for staff:

- Attendance records
- Training materials and presentation decks
- Test results or acknowledgments
- Training schedules and staff sign-offs
- Records of specialized or refresher training (e.g., STR handling)

G. Communications and Correspondence

Internal and external communications relevant to compliance and risk management:

- Correspondence with FINTRAC, legal counsel, or regulators
- Client communications regarding KYC or flagged transactions
- Escalation memos and compliance approvals
- Responses to requests for additional information from authorities

6.3 Access to Records

Done.com Inc. enforces strict access controls over all compliance, client, and transaction-related records to safeguard the **confidentiality**, **integrity**, and **availability** of sensitive information. The organization adheres to the principles of **least privilege** and **need-to-know**, ensuring that only authorized personnel may access records required for their specific duties.

This access policy supports compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, FINTRAC guidelines, and internal data security protocols.

A. Authorized Personnel

Access to records is limited to the following roles, subject to specific conditions:

Role	Access Scope
Chief Compliance Officer (CCO)	Full access to all compliance records, reports, KYC files, and audit trails
Compliance Analysts	Access to KYC, transaction records, STRs, risk assessments, and monitoring logs
Senior Management	View-only access to policy documents, audit reports, and high-level summaries
IT/Systems Admin	Access to encrypted backups and system logs only, for maintenance and security (no access to content)
Auditors/Consultants	Temporary, supervised access for the duration of specific reviews or regulatory audits
Regulators (e.g., FINTRAC)	Access granted upon formal request or during inspections, in accordance with legal requirements

B. Authentication and Access Control Measures

- All users must authenticate using **multi-factor authentication (MFA)** and secure credentials.
- Access to records is granted via **role-based access controls (RBAC)** defined in internal policy.
- Access permissions are reviewed **quarterly** and revoked immediately upon employee departure or role change.

C. System and Physical Security

- Electronic records are stored in encrypted databases with access logging and daily backups.
- Physical records (if applicable) are kept in a **secure, access-controlled cabinet** in the compliance office.
- All access—whether physical or digital—is logged and subject to periodic audit.

D. Record Access for Regulatory or Legal Requests

When required by law or regulatory inspection:

- Done.com Inc. will provide full access to relevant records to **FINTRAC**, law enforcement, or other authorized agencies.
- All disclosures will be **documented**, including:
  - Nature of the request
  - Legal basis (e.g., subpoena, compliance inspection)
  - Date of access
  - Identity of the receiving authority

Under no circumstances will customers be informed of such disclosures where prohibited by law (e.g., in the case of STRs or ongoing investigations).

E. Access Audits and Violations

- All access to records is **monitored and logged** via secure audit trails.
- Unusual access patterns, unauthorized attempts, or breaches are immediately escalated to the **Compliance Officer** and **IT Security**.
- Violations are investigated promptly and may result in disciplinary action or legal reporting.

6.4 Protection and Confidentiality of Records

Done.com Inc. is committed to protecting the confidentiality, integrity, and availability of all records containing customer, transaction, and compliance information. The company has

implemented robust administrative, technical, and physical safeguards in accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, **Personal Information Protection and Electronic Documents Act (PIPEDA)**, and best practices for secure data management.

A. Objectives of Protection

- Ensure that all records are **protected from unauthorized access, alteration, loss, or destruction**.
- Maintain the **confidentiality of sensitive information**, particularly client identity, financial activity, and regulatory reports.
- Prevent **data leaks, internal misuse, and external breaches**.
- Ensure **timely retrieval** of records for internal, regulatory, or legal purposes.

B. Physical Security Measures

- Physical records, if any, are stored in **locked, access-controlled filing cabinets** in secured office areas.
- Access to the compliance and record storage areas is restricted to **authorized personnel only**.
- Visitor access is logged and monitored during audits or third-party reviews.
- Redundant copies of critical records are stored offsite or digitally for disaster recovery purposes.

C. Digital Security Measures

- Records are stored in **encrypted databases** and secure cloud environments with:
  - **AES-256 encryption at rest**
  - **TLS encryption in transit**
- Access to digital records is controlled through:
  - **Role-based access controls (RBAC)**
  - **Multi-factor authentication (MFA)**
  - **Strict user session timeouts**
- All access to records is logged and auditable.

D. Internal Confidentiality Protocols

- Employees and contractors are required to sign **Confidentiality Agreements** as part of onboarding.
- All staff receive regular training on data privacy, security, and proper record handling.
- Compliance-related reports (e.g., STRs) are marked as **confidential** and shared only on a **need-to-know basis**.

E. Protection of Sensitive Reports

- **Suspicious Transaction Reports (STRs)**, **VCTRs**, **LCTRs**, and **EFT reports** are stored separately and flagged as "restricted".
- Clients are **not to be informed** about the filing of STRs or the contents of any regulatory reports.
- Only the **Compliance Officer and designated deputies** may handle, submit, or access these reports.

F. Data Breach Prevention and Response

- Regular vulnerability assessments and penetration testing are conducted to identify and mitigate risks.
- Anti-malware and endpoint protection are installed across all staff workstations.
- In the event of a breach, Done.com Inc. follows a formal **Incident Response Plan**, which includes:
    - Immediate containment
    - Internal investigation and mitigation
    - Notification to regulators (if required by law)
    - Remediation and system hardening

G. Data Sharing and External Access

- Records are not shared externally unless:
    - Required by law (e.g., FINTRAC audits, law enforcement subpoenas)
    - Authorized by the Compliance Officer and with appropriate legal documentation
- All data shared externally is transmitted securely via encrypted channels or file transfer portals.

6.5 Electronic Records and Data Management

Done.com Inc. manages all compliance, client, and transaction-related data primarily through **secure electronic systems**, ensuring efficient storage, protection, and retrieval. The company's electronic records and data management practices are designed to meet or exceed the regulatory requirements set out in the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, **FINTRAC guidance**, and applicable Canadian data protection laws.

A. Scope of Electronic Recordkeeping

The following categories of information are managed electronically:

- Customer due diligence (CDD) and know-your-client (KYC) documentation
- Risk assessments, onboarding notes, and enhanced due diligence (EDD) files
- Transaction logs, trade records, and crypto transfer details

- Regulatory reports (STRs, LCTRs, VCTRs, EFTs) and submission confirmations
- Audit logs, policy documents, and internal compliance reviews
- Training attendance and materials
- Communications relevant to compliance investigations

B. Systems and Storage Infrastructure

All electronic records are stored in a **secure, access-controlled digital infrastructure**, which includes:

- **Encrypted cloud-based storage** platforms hosted in Canada or other FINTRAC-compliant jurisdictions
- **Internal encrypted databases** for structured data (e.g., client profiles, transaction logs)
- **Document management systems (DMS)** for storing PDF, CSV, XLSX, and multimedia files
- **Blockchain analytics tools** that log risk scores, wallet metadata, and activity timelines

C. Data Integrity and Retention Controls

To ensure data is complete, unaltered, and available:

- All records are subject to **automated backups** on a **daily basis**
- **Checksums and hash verification** are applied to ensure file integrity
- Records are retained in accordance with the **5-year minimum retention period**
- Time-stamped logs are maintained for record creation, access, modification, and deletion
- Versioning is enabled for key compliance documents and policies

D. Access and User Management

Access to electronic records is governed by:

- **Role-Based Access Controls (RBAC)**: Each employee can only view or edit records based on their job function.
- **Multi-Factor Authentication (MFA)**: All access requires secondary verification.
- **Session Logging**: All user access and actions are recorded for audit purposes.

Periodic reviews are conducted to ensure access rights remain appropriate and unused accounts are deactivated.

E. Data Backup and Disaster Recovery

To prevent data loss or downtime:

- Backups are stored in **physically separated regions** to prevent correlated failure

- Weekly snapshots are retained for disaster recovery
- A documented **Disaster Recovery Plan (DRP)** includes steps for rapid restoration of records in case of:
    - System outage
    - Cybersecurity event
    - Physical infrastructure failure

F. Compliance with Legal and Regulatory Standards

Done.com Inc. ensures its electronic recordkeeping processes comply with:

- **PCMLTFA** and FINTRAC Recordkeeping Regulations
- **PIPEDA** (Personal Information Protection and Electronic Documents Act)
- Best practices for **cybersecurity**, **privacy**, and **data minimization**

G. Review and Maintenance

- The electronic records system is reviewed **annually** by the Compliance and IT teams
- Any system changes, migrations, or upgrades undergo **security and compliance reviews**
- Third-party vendors involved in data storage or backup services are subject to **due diligence** and contractual safeguards

7. Training and Awareness Program

7.1 Training Requirements and Frequency

Done.com Inc. recognizes that the strength of its Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) compliance program depends on a well-informed and vigilant workforce. To that end, the company mandates regular and role-appropriate training for all relevant personnel to ensure understanding of regulatory obligations, internal procedures, and emerging risks.

To maintain high standards of AML knowledge and industry credibility, Done.com Inc. uses the globally recognized training and certification platform **ACAMS** (www.acams.org) as its primary provider for formal compliance education.

A. Who Must Receive Training

The following categories of personnel must complete AML/ATF training:

Role	Training Requirement
Chief Compliance Officer (CCO)	Advanced AML certification (e.g., CAMS) + annual refresher training
Compliance Staff	Initial onboarding AML/ATF course + annual recertification via ACAMS
Senior Management	AML awareness and risk oversight modules (every 2 years minimum)
Operations/Trading Staff	Onboarding AML/ATF training + transaction monitoring awareness
Customer Support Staff	KYC, fraud red flags, and client onboarding risk training
IT & Technical Teams	Data protection, cybersecurity in financial services (every 2 years)

B. Frequency of Training

Training Type	Frequency	Delivery Method
Onboarding AML Training	Within 30 days of hire	ACAMS e-learning or internal session
Annual AML Refresher	Once per calendar year	ACAMS certified course or internal updates
Role-Specific Updates	As needed based on regulatory or procedural changes	Targeted email briefings or live sessions
Management Oversight Training	Every 2 years	ACAMS or industry seminars
Incident-Driven Training	Immediately following any compliance breach or audit finding	Internal session with compliance officer

C. Topics Covered in Training

Training covers all core elements of AML/ATF obligations, including:

- Overview of the PCMLTFA and FINTRAC expectations
- How to identify and escalate suspicious activity
- Customer due diligence (CDD), enhanced due diligence (EDD), and PEPs
- Virtual asset risks and blockchain forensics fundamentals
- Record-keeping and reporting obligations (STRs, LCTRs, EFTs, VCTRs)

- Transaction monitoring and red flags
- Privacy, confidentiality, and data protection
- Emerging typologies in digital currency markets

D. Certification and Tracking

- Staff who complete ACAMS courses will receive **formal certification**, which is retained in their HR file and compliance record.
- The Compliance Officer maintains a **training log** that includes:
  - Course names and dates
  - Completion status and scores (where applicable)
  - Certification validity and renewal due dates
- Training compliance is audited annually and any staff with overdue training may be suspended from client-facing duties until recertification is complete.

7.2 Content of Training Sessions

Done.com Inc. 's AML/ATF training sessions are designed to equip employees and senior management with a deep understanding of regulatory obligations, internal procedures, and practical skills to detect and mitigate risks related to money laundering, terrorist financing, and financial crime.

Training content is tailored to employee roles and draws from guidance issued by **FINTRAC**, the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, and global best practices provided by **ACAMS (Association of Certified Anti-Money Laundering Specialists)**.

A. Core Topics Covered in All Training Sessions

All employees required to complete AML/ATF training will receive instruction on the following foundational subjects:

1. **Introduction to AML/ATF**
   - Purpose and importance of Canada's AML/ATF regime
   - Role of FINTRAC and the PCMLTFA
2. **Key Offences**
   - Definitions of money laundering and terrorist financing
   - Real-world examples and case studies
   - Common methods used in digital currency and OTC markets
3. **Regulatory Reporting Obligations**
   - When and how to file:
     - Suspicious Transaction Reports (STRs)
     - Large Cash Transaction Reports (LCTRs)
     - Electronic Funds Transfer Reports (EFTs)

    - Virtual Currency Transaction Reports (VCTRs)
4. **Customer Due Diligence (CDD)**
    - Standard KYC requirements
    - Identifying and documenting beneficial ownership
    - Third-party determination
    - Record-keeping requirements
5. **Enhanced Due Diligence (EDD)**
    - Politically Exposed Persons (PEPs)
    - High-risk jurisdictions and correspondent banking relationships
    - EDD triggers and documentation standards
6. **Transaction Monitoring**
    - Identifying unusual or suspicious activity
    - Recognizing red flags in fiat and crypto markets
    - Reporting and escalation process
7. **Data Protection and Confidentiality**
    - Privacy and security obligations under PIPEDA
    - Internal safeguards for sensitive records
    - Handling and protecting regulatory filings (e.g., STR confidentiality)

B. Role-Specific Content

Role	Additional Topics
Compliance Officers	Risk assessment frameworks, internal audits, regulator communications, sanctions screening, oversight responsibilities
Trading/Operations Staff	Trade surveillance, wallet address risk scoring, source of funds documentation, handling OTC settlements
Customer Service Staff	Client onboarding, dual-process verification, handling KYC document collection, identifying red flags
IT/Data Security Teams	Secure data storage practices, record retention policies, access controls, incident response
Senior Management	AML governance, accountability under PCMLTFA, oversight responsibilities, approving the compliance program

C. Delivery Method and Format

- **ACAMS Learning Management System (LMS):** for foundational and certification-level content
- **Internal Workshops & Webinars:** hosted by the Chief Compliance Officer, especially when procedures or laws change
- **Case Study Discussions:** based on industry scenarios involving digital assets and OTC trading

- **Quizzes & Assessments:** to evaluate understanding and reinforce retention

D. Training Materials Provided

- ACAMS official course materials and video modules
- Internal compliance handbook and reporting guides
- Red flag indicators and escalation flowcharts
- Reference documents (e.g., FINTRAC guidance, PCMLTFA excerpts)

7.3 Training Records and Documentation

Done.com Inc. maintains detailed training records and documentation to demonstrate compliance with Canadian AML/ATF regulatory requirements and to support internal accountability for all training efforts. These records are essential to meet **FINTRAC expectations**, fulfill obligations under the **PCMLTFA**, and provide audit-ready evidence during inspections or third-party reviews.

A. Purpose of Maintaining Training Records

- Ensure all employees have completed required AML/ATF training within specified timeframes
- Track certification and recertification cycles (especially for high-risk and client-facing roles)
- Monitor gaps in compliance knowledge and assign remedial or targeted training
- Provide supporting documentation for FINTRAC audits or enforcement inquiries
- Maintain accountability and documentation trail for internal audit and governance purposes

B. Types of Training Records Maintained

The Compliance Officer ensures the following records are created and retained for **a minimum of five (5) years** from the date of training:

Record Type	Contents
Training Attendance Logs	Date, session title, participant names, signatures or digital confirmations
Certificates of Completion	Issued by ACAMS or internal compliance team, with issue and expiry dates
Training Materials	Slides, manuals, case studies, internal guidance documents
Assessment Results	Quiz scores, exam pass/fail results, corrective action (if applicable)
Training Schedules	Historical records of past sessions and planned future sessions
Refresher Training Records	Documentation of recurring training and recertification by employee

Role-Based Training Maps	Record of what content each role is required to complete
Training Compliance Logs	Overview dashboard of staff training status maintained by the Compliance Officer

C. Storage and Accessibility

- All training records are stored **electronically** in a secure, access-controlled system, with appropriate backups and audit logging.
- Physical records (e.g., signed attendance sheets) are scanned and digitized when possible, or stored in a locked compliance filing cabinet.
- Records are accessible only by authorized personnel in the Compliance and Human Resources departments.
- Digital access is controlled via **Role-Based Access Control (RBAC)** and **Multi-Factor Authentication (MFA)**.

D. Review and Updates

- Training logs are reviewed **quarterly** by the Compliance Officer to ensure no staff are overdue for required training.
- The compliance program's training component is **audited annually**, and logs are updated to reflect findings.
- If new regulatory guidance or internal procedures are introduced, new training records are generated accordingly.

E. Regulator Access and Confidentiality

- Upon request by **FINTRAC or other authorized regulatory bodies**, training records are made available promptly.
- All training records are handled with the same level of confidentiality and integrity as client and transaction records.
- No sensitive customer data is ever stored in training records, ensuring privacy compliance with **PIPEDA**.

7.4 Testing and Certification of Employee Knowledge

To ensure the effectiveness of its AML/ATF training program, Done.com Inc. incorporates formal **testing and certification** measures to validate employee comprehension and readiness. These measures are aligned with **FINTRAC guidance**, the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, and global best practices from **ACAMS**.

The purpose of this testing and certification process is to confirm that employees:

- Understand their roles and responsibilities under the compliance program
- Can identify red flags and escalate suspicious activity appropriately
- Are equipped to follow proper onboarding, monitoring, and reporting procedures
- Maintain a current and practical understanding of regulatory requirements

A. Certification Requirements

Role	Certification Requirement
Chief Compliance Officer	Completion of the CAMS (Certified Anti-Money Laundering Specialist) certification or equivalent
Compliance Analysts	ACAMS foundational certification + internal role-specific assessments
Trading and Operations Staff	Internal knowledge test + training completion confirmation
Customer Support Staff	Internal AML/KYC test focused on onboarding and red flags
Senior Management	Certification of AML governance understanding and policy oversight
New Hires (All roles)	Must pass onboarding AML/ATF test within 30 days of employment

B. Testing Components

Employee knowledge is tested using a combination of:

- **Multiple-choice quizzes** on core AML topics (thresholds, reporting types, definitions)
- **Scenario-based case studies** (e.g., handling a high-risk client or a suspicious crypto transaction)
- **Short written assessments** for roles requiring decision-making (e.g., compliance staff)
- **Verbal debriefs or interviews** for senior management or specialized roles

C. Frequency of Testing

Test Type	Frequency
Initial onboarding test	Within 30 days of employment
Annual knowledge check	Once per year for all regulated staff
Refresher test	Upon procedural or regulatory changes
Incident-based reassessment	After audit findings or compliance breach

D. Passing Standards and Remediation

- A minimum **passing score of 80%** is required for most tests.
- Employees who do not pass on the first attempt must:
  - Review assigned refresher material
  - Retake the assessment within 7 business days
- Persistent non-compliance may result in **temporary suspension of duties** or escalation to HR and management.

E. Certification Records

- All test results and certifications (e.g., CAMS, ACAMS Essentials) are stored in the employee's compliance file.
- Expiry and renewal reminders are tracked by the Compliance Officer.
- A training and certification dashboard is maintained for audit and reporting purposes.

F. Independent Verification (Where Applicable)

- The CAMS certification (via ACAMS) provides third-party validation of compliance expertise.
- Senior compliance personnel may be subject to additional verification via continuing professional education (CPE) requirements.

8. Compliance Monitoring and Review

8.1 Internal Audit and Review Procedures

Done.com Inc. conducts regular internal audits and reviews of its Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) Compliance Program to ensure the effectiveness, adequacy, and ongoing alignment with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, **FINTRAC guidelines**, and evolving risk exposures.

These procedures serve to detect gaps, verify policy implementation, and ensure staff and systems remain compliant with all applicable obligations.

A. Objectives of Internal Audit and Review

- **Verify the effectiveness** of the compliance program and risk mitigation measures
- **Assess adherence** to written policies and procedures across departments
- **Test internal controls** for recordkeeping, reporting, and transaction monitoring
- **Ensure regulatory filings** (e.g., STRs, LCTRs, VCTRs, EFTs) are accurate, timely, and complete
- **Identify areas for improvement** and implement corrective actions

- Provide audit-ready documentation for **regulatory inspections** (e.g., by FINTRAC)

B. Audit Scope and Methodology

Internal audits and reviews cover the following core areas:

Area	Audit Focus
Customer Due Diligence	Proper KYC procedures, verification, beneficial ownership, EDD
Transaction Monitoring	Accuracy of flagged alerts, escalation practices, completeness of logs
Regulatory Reporting	Accuracy and timeliness of STRs, VCTRs, LCTRs, EFTs
Training and Awareness	Staff training logs, certification, knowledge testing outcomes
Recordkeeping and Retention	Completeness, accuracy, accessibility, and encryption of records
Policy and Procedure Compliance	Whether staff follow documented processes
IT and Access Controls	Integrity of access logs, RBAC enforcement, secure system setup
Governance and Oversight	Compliance officer's role, board review, and senior management engagement

Audits include:

- **File testing** (sampling of customer files and transactions)
- **Process walkthroughs**
- **Staff interviews**
- **Data analysis** (especially for transaction logs and wallet analytics)

C. Frequency and Scheduling

Review Type	Frequency
Comprehensive AML Audit	Annually (minimum)
Thematic Review (e.g., STRs or CDD)	Quarterly or based on risk triggers
Targeted Spot Checks	Ad hoc based on incidents
Post-Regulatory Audit Remediation	Within 30 days of FINTRAC finding

The **Chief Compliance Officer (CCO)** is responsible for coordinating the schedule and execution of these audits and may engage **external consultants** as needed for independent reviews.

D. Documentation and Reporting

Every audit and review results in a formal **Audit Report** that includes:

- Summary of areas reviewed
- Findings and observations
- Severity ratings (low, medium, high)
- Recommendations for remediation
- Responsible parties and deadlines

These reports are reviewed by **Senior Management** and, where appropriate, the **Board of Directors**.

E. Remediation and Follow-up

- A **Corrective Action Plan (CAP)** is developed for each material finding.
- Follow-up reviews are conducted to confirm that issues are resolved.
- Any unresolved or repeat deficiencies may result in disciplinary actions or escalated reporting.

F. Confidentiality and Independence

- All audit information is treated as **confidential** and stored securely.
- To ensure objectivity, reviews are ideally conducted by personnel **not directly involved** in the day-to-day operations being audited.
- When feasible, **external independent audits** will be performed every **2–3 years** to validate internal controls and benchmark program performance.

8.2 Independent Testing and Assessment

To ensure objectivity and validate the overall effectiveness of its Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) Compliance Program, Done.com Inc. conducts regular **independent testing and assessments** by qualified third parties. These external reviews are crucial for identifying blind spots, benchmarking practices against industry standards, and fulfilling the requirements of the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and **FINTRAC's Guidance on Compliance Program Effectiveness**.

A. Purpose of Independent Testing

- Provide an **objective evaluation** of the compliance program
- Assess the **adequacy and effectiveness** of internal controls, policies, and procedures
- Evaluate the company's **risk-based approach** to customer and transaction oversight
- Test the **accuracy and timeliness** of regulatory reports (STRs, LCTRs, EFTs, VCTRs)

- Confirm compliance with **recordkeeping** and **training requirements**
- Support **senior management accountability** and continuous improvement

B. Who Conducts the Testing

Independent assessments must be conducted by individuals or firms who are:

- **External to the daily operations** of Done.com Inc. 's compliance program
- **Qualified and experienced** in Canadian AML/ATF laws, virtual currency regulations, and FINTRAC expectations
- May include:
  - Independent compliance consultants
  - Legal or audit firms with AML/ATF expertise
  - CAMS-certified professionals not affiliated with Done.com Inc.

In cases where external review is not feasible (e.g., due to cost or operational sensitivity), the assessment may be conducted internally by staff **not directly involved** in day-to-day compliance duties, provided they meet objectivity and knowledge criteria.

C. Scope of Independent Testing

Each independent test will cover, at minimum:

Area	Evaluation Focus
Compliance Governance	Structure, role of Compliance Officer, escalation lines
CDD/EDD & KYC	Client file testing, beneficial ownership, PEP screening
Transaction Monitoring	Alert generation, response documentation, escalation process
STRs & Regulatory Reports	Filing accuracy, timeliness, completeness
Risk Assessments	Risk model, methodology, and documentation
Recordkeeping	File retention, access logs, data protection controls
Staff Training	Certifications, attendance logs, testing outcomes
IT & System Controls	Access controls, security of compliance systems
Change Management	Updates to policies, audit trails, training for new procedures

D. Frequency of Testing

Type of Business Activity	Testing Frequency
Standard MSB operations	Every 2 years minimum
High-risk (e.g., virtual currencies, OTC FX)	Annually (recommended)
Material change in business model	Within 90 days of change

E. Reporting and Remediation

Each independent assessment will result in a formal **Independent Assessment Report**, which must include:

- Summary of scope and methodology
- Detailed findings and gaps identified
- Compliance with applicable regulations
- Severity grading of issues (e.g., minor, moderate, major)
- Recommended corrective actions and deadlines

Remediation plans must be developed for all significant findings and tracked by the **Chief Compliance Officer (CCO)**. Progress is reported to **senior management** and incorporated into the next internal audit cycle.

F. Documentation and Regulator Access

- All independent assessment reports and associated documentation are securely stored and retained for **at least 5 years**
- These reports are made available to **FINTRAC or other regulators** upon request
- Disclosure of such reviews to the Board or senior executives is documented to demonstrate governance awareness and accountability

8.3 Reporting of Compliance Issues and Violations

Done.com Inc. promotes a culture of transparency, accountability, and zero tolerance for non-compliance with Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) obligations. All employees, contractors, and business units are required to promptly report any actual, potential, or suspected violations of the company's compliance policies or applicable laws and regulations, including those under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and guidance issued by **FINTRAC**.

A. Purpose and Importance of Reporting

- Detect and remediate policy breaches or suspicious behavior early
- Prevent regulatory violations and associated penalties
- Maintain the integrity and effectiveness of the AML/ATF program
- Empower employees to act responsibly and ethically
- Provide a mechanism for continuous improvement

B. What Must Be Reported

Employees are required to report, without delay, any of the following:

- Suspected **money laundering** or **terrorist financing** activity
- Breaches of **CDD, EDD, or onboarding** procedures
- Failure to file or inaccurate submission of **regulatory reports** (e.g., STRs, LCTRs, EFTs, VCTRs)
- Unusual or suspicious transactions not escalated or investigated properly
- Access to compliance systems by **unauthorized personnel**
- **Alteration or destruction** of records or audit trails
- **Non-compliance** with policies or regulatory guidance by staff or vendors
- Attempts to **coerce, influence, or retaliate** against employees who raise concerns

C. Internal Reporting Channels

Done.com Inc. provides multiple confidential and protected methods for reporting compliance concerns:

Channel	Details
Direct to Compliance Officer	Via secure email or in-person reporting
Internal Reporting Form	Located on internal portal or provided during onboarding
Anonymous Reporting Option	Via secure submission tool or encrypted email alias
Escalation to Management	In cases involving CCO or systemic breaches

All reports are treated as **strictly confidential**, and no adverse action will be taken against any employee making a report in **good faith**, even if the report is later found to be unsubstantiated.

D. Investigation Process

- The **Chief Compliance Officer (CCO)** or designated investigator will log and assess each report
- A preliminary review will determine whether a formal investigation is warranted
- Investigations will involve gathering documentation, interviewing relevant parties, and assessing regulatory impact
- Findings are documented, and appropriate remedial or disciplinary actions are proposed

E. Corrective Actions and Follow-Up

Depending on the outcome of the investigation, actions may include:

- **Remedial training** for involved personnel
- **Policy updates** or procedural clarifications
- **Internal control enhancements**
- **Voluntary disclosure** to FINTRAC (if appropriate)
- **Employee discipline**, up to and including termination

Follow-up reviews are conducted to verify the effectiveness of corrective measures.

F. Whistleblower Protections

- Done.com Inc. prohibits any **retaliation, harassment, or reprisal** against employees who report compliance concerns in good faith
- Whistleblowers may remain **anonymous** and are encouraged to report without fear of reprisal
- Any attempt to interfere with the reporting or investigation process is treated as a serious compliance violation

G. Reporting to Regulators

If an issue or violation constitutes a reportable breach under Canadian law or FINTRAC guidelines, the Compliance Officer will:

- Prepare and submit appropriate reports or disclosures
- Cooperate fully with regulatory inquiries or audits
- Document the disclosure process and communication trail

8.4 Corrective Action and Remediation Plans

Done.com Inc. maintains a formal process for implementing corrective actions and remediation plans when compliance issues, violations, audit findings, or regulatory concerns are identified. This ensures timely resolution, reduces risk exposure, and demonstrates to regulators like **FINTRAC** that the company is responsive, accountable, and committed to continuous improvement of its **AML/ATF Compliance Program**, in accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**.

A. Purpose of Corrective Actions

- Address gaps, weaknesses, or failures in AML/ATF controls
- Prevent recurrence of compliance issues
- Restore program integrity and regulatory compliance
- Satisfy audit or regulatory findings and recommendations
- Improve operational effectiveness and risk posture

B. When Corrective Actions Are Required

Corrective actions must be initiated when:

- Internal audits identify control deficiencies or non-compliance
- Independent reviews reveal policy or process failures

- Regulatory bodies (e.g., FINTRAC) issue findings, penalties, or recommendations
- Employees report or uncover violations of AML/ATF policies
- System changes or business expansions expose new risks
- Root cause analysis of suspicious activity or reporting errors identifies systemic gaps

C. Development of a Corrective Action Plan (CAP)

A formal **Corrective Action Plan (CAP)** must be developed by the **Chief Compliance Officer (CCO)** or delegated personnel. The plan must include:

Component	Description
Issue Description	Summary of the problem or non-compliance identified
Root Cause Analysis	Explanation of how/why the issue occurred
Risk Impact	Evaluation of risk level (low, moderate, high)
Corrective Actions	Detailed steps to remediate the issue
Responsible Parties	Names/roles of persons accountable for resolution
Timeline for Remediation	Clear deadlines and milestones
Monitoring Mechanism	How progress will be tracked and verified
Documentation	How actions will be recorded and retained

D. Approval and Oversight

- CAPs must be **approved by Senior Management** and, where applicable, presented to the Board of Directors or Audit Committee.
- The **Compliance Officer** is responsible for ongoing monitoring of implementation and communicating updates.
- If an external party (e.g., auditor or regulator) required the CAP, updates may be provided at their request.

E. Follow-Up and Verification

- Upon completion of all action items, a **final review** is conducted to ensure that:
  - The root cause was fully addressed
  - New or updated controls are in place and functioning
  - Staff have received any necessary re-training
  - Supporting documentation is available
- Results of the follow-up review are documented and added to the compliance audit trail.

F. Escalation and Non-Compliance

If action items are not completed within the required timeframe or issues persist:

- The matter is escalated to **senior management** or the **Board**
- Additional controls may be imposed (e.g., increased monitoring, restricted access)
- Repeated failures may trigger disciplinary action or **voluntary disclosure** to FINTRAC

G. Documentation and Retention

- All CAPs, supporting materials, and closure reports are securely stored and retained for **at least 5 years**
- These records are made available to regulators upon request

9. Reporting Obligations to FINTRAC

9.1 Registration Requirements and Procedures

As a Money Services Business (MSB) operating in Canada, Done.com Inc. is subject to the registration requirements outlined in the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and the associated **Money Services Business Regulations**. Registration with the **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** is mandatory prior to commencing operations and must remain current and accurate at all times.

A. Who Must Register

Done.com Inc. is classified as a **federal MSB** because it offers the following services:

- **Foreign exchange dealing**
- **Dealing in virtual currencies (VC)** including the buying, selling, and transfer of digital assets
- **Over-the-counter (OTC) transactions** across multiple asset classes, including crypto and fiat

These services fall under FINTRAC's definitions of regulated MSB activities.

B. Registration Requirements

To register as an MSB, Done.com Inc. must:

1. **Complete and submit the FINTRAC MSB Registration Form**, available through FINTRAC's online registration portal
2. Provide accurate information about:
    - Legal name and operating/trade names (e.g., Done.com Inc.)
    - Business structure (e.g., corporation)
    - Head office and operational addresses

    - Services provided
    - Owners and controlling minds
    - Banking relationships
    - Compliance Officer contact information
3. Appoint a designated **Compliance Officer** responsible for maintaining the compliance program
4. Submit ownership information for **beneficial owners** and key individuals
5. Acknowledge and agree to adhere to obligations under the **PCMLTFA** and **FINTRAC regulations**

C. Ongoing Obligations After Registration

Once registered, Done.com Inc. must:

Requirement	Frequency
Renew Registration	Every 2 years (biennial renewal through FINTRAC)
Update Registration Details	Within 30 days of any change (e.g., services, address, directors, beneficial ownership)
Notify FINTRAC of Ceasing Activities	Within 30 days if Done.com Inc. stops offering MSB services

Failure to meet these requirements can result in administrative monetary penalties (AMPs), deregistration, or enforcement actions.

D. Recordkeeping and Internal Documentation

- Copies of registration certificates, renewal confirmations, and communications with FINTRAC are stored securely in the **Compliance Program Repository**.
- The **Compliance Officer** ensures the registration status is monitored and renewed on time.
- Updates to FINTRAC registration are reflected in internal compliance documents, including the **Compliance Program Manual**, **Risk Assessment**, and **Organizational Charts**.

E. Penalties for Non-Compliance

Operating as an MSB without registration or with outdated information can lead to:

- Monetary penalties from FINTRAC
- Public naming and shaming
- Suspension or termination of banking relationships
- Criminal liability for directors and officers

9.2 Compliance Program Effectiveness Reports

Done.com Inc. is committed to maintaining a robust and evolving Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) Compliance Program. As required under **Section 71 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)** and outlined in **FINTRAC Guideline 4**, Done.com Inc. must regularly evaluate the **effectiveness of its compliance program** and document the results in formal **Compliance Program Effectiveness Reports**.

A. Purpose of the Effectiveness Report

The objective of the Compliance Program Effectiveness Report is to:

- Evaluate the overall health and functionality of the AML/ATF compliance framework
- Confirm the alignment of policies and procedures with regulatory expectations
- Identify any deficiencies or gaps and recommend corrective actions
- Support accountability and oversight by senior management and regulators
- Demonstrate proactive compliance management during audits or examinations

B. Key Components of the Report

Each report includes a comprehensive review of the five key elements of Done.com Inc. 's compliance program:

Program Element	Effectiveness Criteria
Compliance Officer Oversight	Independence, authority, and qualifications of the designated officer
Written Policies and Procedures	Currency, scope, accessibility, and operational relevance
Risk Assessment	Methodology, coverage of products/customers/geographies, integration with business changes
Ongoing Training Program	Coverage, documentation, frequency, and testing outcomes
Ongoing Monitoring and Reporting	STRs, LCTRs, EFTs, VCTRs, transaction alerts, and escalation workflows

C. Frequency of Report Preparation

Type of Assessment	**Frequency**
Full Compliance Effectiveness Review	At least once every two years (biennially)
Interim or Targeted Reviews	As needed after significant events (e.g., audit findings, business expansion, regulatory updates)

D. Responsibilities and Process

- The **Chief Compliance Officer (CCO)** is responsible for coordinating and producing the Effectiveness Report.
- Independent input may be obtained from:
  - Internal audit teams (if applicable)
  - Third-party compliance consultants
  - Senior managers from high-risk business units
- The report must be:
  - **Approved by Senior Management**
  - **Retained for a minimum of 5 years**
  - **Provided to FINTRAC upon request**

E. Remediation and Follow-Up

Any deficiencies or areas of improvement identified must be addressed through a formal **Corrective Action Plan (CAP)**. This plan must include:

- Assigned responsibilities
- Deadlines for remediation
- Monitoring mechanisms
- Follow-up reviews to confirm implementation

The results of corrective actions are included in the next reporting cycle to establish a continuous improvement feedback loop.

F. Recordkeeping and Accessibility

- Reports are stored securely in the **Compliance Documentation Repository**.
- Access is limited to the CCO, senior management, and authorized regulatory representatives.
- All versions of previous reports are archived for audit traceability and historical benchmarking.

9.3 Reporting Timelines and Methods

Done.com Inc. complies with all reporting obligations under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and associated regulations, particularly those set out by **FINTRAC**. This includes the accurate and timely submission of various types of reports related to suspicious activity, large cash transactions, electronic funds transfers, and virtual currency transactions.

To maintain compliance, Done.com Inc. has defined standardized **reporting timelines and submission methods** for each report type, ensuring data integrity, regulatory alignment, and internal accountability.

A. Regulatory Reporting Types and Timelines

Report Type	Trigger/Event	Deadline for Submission	Reporting Method
Suspicious Transaction Report (STR)	Reasonable grounds to suspect ML/TF	As soon as practicable (ideally within 30 days or sooner)	FINTRAC SecureUpload or Web Reporting
Large Cash Transaction Report (LCTR)	Receipt of CAD $10,000+ in cash in a single or multiple transactions within 24 hours	Within 15 calendar days of transaction	FINTRAC Web Reporting Portal
Electronic Funds Transfer Report (EFTR)	Outbound/inbound international wire transfers of CAD $10,000+	Within 5 business days of transaction	FINTRAC SecureUpload or Web Reporting
Virtual Currency Transaction Report (VCTR)	Virtual currency transactions CAD $10,000+ in a 24-hour period	Within 5 business days of transaction	FINTRAC Web Reporting Portal
Registration Updates (MSB Information)	Change in ownership, services, address, etc.	Within 30 calendar days of change	FINTRAC MSB Portal
Biennial MSB Registration Renewal	Ongoing MSB status	Every 2 years (before expiry date)	FINTRAC MSB Portal
Compliance Effectiveness Report (Internal)	Internal assessment of AML program	Every 2 years (or sooner if needed)	Internal documentation; made available to FINTRAC upon request

B. Internal Escalation Timelines

To support timely regulatory reporting, Done.com Inc. has established internal escalation deadlines:

Action	Escalation Deadline
Employee identifies suspicious activity	Immediately → escalate to Compliance within 24 hours
Compliance Officer begins STR review	Within 48 hours of escalation
Internal approval of STR before submission	Within 3 business days of draft

These internal buffers ensure reports are submitted **well within FINTRAC's regulatory deadlines** and allow for proper vetting and documentation.

C. Submission Methods and Tools

Done.com Inc. uses the following secure reporting channels:

- **FINTRAC Web Reporting System (FWR)**: Primary interface for STRs, LCTRs, VCTRs, and EFTRs
- **FINTRAC SecureUpload**: Used for batch submission or encrypted document uploads
- **MSB Registration Portal**: For registration and business information updates
- **Internal Compliance Management System**: Used to track reporting timelines, audit logs, report references, and document versioning

Access to these platforms is restricted to trained and authorized personnel, and multi-factor authentication is enforced where applicable.

D. Recordkeeping and Version Control

- A copy of each submitted report is saved in a secure directory, with metadata including:
  - Submission date
  - Staff responsible
  - Report ID/reference number
  - Supporting documents (e.g., screenshots, client files, investigation notes)
- Reports are retained for **at least 5 years** in accordance with PCMLTFA requirements

10. Protection of Information and Privacy

10.1 Privacy Policy and Compliance

Done.com Inc. is committed to protecting the personal information of its clients, employees, and stakeholders in accordance with applicable privacy laws, including the **Personal Information Protection and Electronic Documents Act (PIPEDA)** and other relevant provincial legislation. The organization's privacy policy is aligned with its obligations under the **Proceeds of Crime**

(Money Laundering) and Terrorist Financing Act (PCMLTFA) and **FINTRAC regulations**, ensuring that compliance efforts respect individual rights while fulfilling legal reporting and recordkeeping requirements.

A. Purpose of the Privacy Policy

- Protect the **confidentiality, integrity, and availability** of personal and financial information
- Outline how Done.com Inc. collects, uses, retains, and discloses personal information
- Ensure transparency with clients and compliance with federal privacy legislation
- Support lawful access, investigation, and reporting under AML/ATF laws

B. Scope of Information Collected

Done.com Inc. collects and retains personal information for the purposes of client onboarding, ongoing due diligence, transaction monitoring, and regulatory compliance. Information collected includes:

- Full legal name, date of birth, and government-issued ID
- Address, phone number, and email
- Occupation and source of funds/income
- Bank account or wallet details
- Beneficial ownership and control information
- IP addresses and device fingerprints (for non-face-to-face clients)
- Transaction history and risk profile

This information is collected in accordance with **Know Your Client (KYC)** and **Customer Due Diligence (CDD)** requirements.

C. Legal Basis for Collection and Use

Personal information is collected:

- With the **consent** of the individual (where required)
- To fulfill statutory obligations under the **PCMLTFA**
- For the **detection and deterrence of money laundering and terrorist activity financing**
- To meet requirements of financial partners, correspondent institutions, or regulators

D. Use and Disclosure of Information

Personal information is used solely for the purposes for which it was collected, including:

- Identity verification and client risk profiling

- Internal compliance audits and investigations
- Filing mandatory reports (e.g., STRs, VCTRs, LCTRs, EFTs) with FINTRAC
- Cooperation with law enforcement where legally compelled

Done.com Inc. does **not sell, rent, or share** personal information for marketing or commercial purposes.

E. Safeguards and Data Protection

- All data is stored on **secure, encrypted servers** with restricted access
- Role-based access controls (RBAC) are enforced for compliance and support staff
- Network traffic is protected by firewalls, intrusion detection, and endpoint security tools
- Access logs are monitored and reviewed for unauthorized activity
- Any personal data transmitted electronically is **encrypted in transit and at rest**

F. Client Rights and Access

Clients have the right to:

- Request access to their personal information held by Done.com Inc.
- Request correction of inaccurate or outdated information
- Withdraw consent for processing (where applicable), subject to AML laws
- File complaints with the Privacy Officer or applicable privacy authority

Exceptions apply where withholding information is required under AML legislation or for regulatory reporting.

G. Accountability and Oversight

- The **Chief Compliance Officer (CCO)** also acts as the **Privacy Officer**
- Regular privacy training is delivered to staff to reinforce confidentiality obligations
- Privacy controls are reviewed annually as part of the internal audit process

H. Retention and Disposal

Personal information is retained for **at least five years** following the last transaction or business relationship termination, as required by PCMLTFA. Upon expiry of the retention period, data is securely destroyed using cryptographic erasure or physical destruction (in the case of paper records).

10.2 Confidentiality of Information

Done.com Inc. treats the confidentiality of customer and business information as a fundamental pillar of its operations. As a regulated Money Services Business (MSB) operating under the

Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), the company is required to maintain strict confidentiality protocols when handling customer information, internal investigations, compliance reports, and regulatory filings.

A. Commitment to Confidentiality

Done.com Inc. is committed to:

- Protecting **client, transaction, and internal compliance data** from unauthorized disclosure or misuse
- Ensuring access to sensitive data is limited to **authorized personnel only**
- Maintaining confidentiality in all communications with regulators such as **FINTRAC**, banks, and law enforcement
- Complying with applicable **privacy, financial, and AML laws** governing confidential information

B. Categories of Confidential Information

Confidential information includes, but is not limited to:

Category	Examples
Customer Information	Name, date of birth, ID documents, bank accounts, virtual currency wallets, contact details
Transaction Details	Fiat and crypto transactions, OTC trade history, amounts, beneficiaries
Compliance Materials	Suspicious transaction reports (STRs), risk assessments, internal alerts, training records
Internal Documentation	Audit reports, corrective action plans, employee access logs
Vendor & Partner Info	Third-party service agreements, correspondent relationships

C. Access Controls and Restrictions

- Access to confidential information is granted strictly on a **need-to-know basis**
- Role-based access is implemented within all systems and databases
- Multi-factor authentication (MFA) is enforced for systems containing sensitive data
- Access logs are monitored regularly for unauthorized attempts or anomalies

D. Handling of Suspicious Transaction Reports (STRs)

- Information related to STRs is **highly confidential**
- Employees are prohibited from disclosing:
  - That an STR was filed
  - The content of the STR
  - The existence of any related investigation
- Breach of STR confidentiality may result in **criminal liability under PCMLTFA Section 65**

E. Employee Confidentiality Obligations

- All employees sign a **confidentiality agreement** as part of onboarding
- Confidentiality obligations extend beyond termination of employment
- Employees receive training on:
  - Handling of sensitive customer and compliance data
  - Legal obligations under AML/ATF laws and privacy regulations
  - Reporting suspected breaches of confidentiality

F. Third-Party and Vendor Confidentiality

- Vendors, contractors, or partners who receive access to sensitive information must:
  - Sign **confidentiality clauses** or non-disclosure agreements (NDAs)
  - Be vetted for information security controls and privacy compliance
- All external disclosures must be governed by **contractual agreements** and compliance oversight

G. Breach Response and Escalation

In the event of a suspected or confirmed breach of confidentiality:

1. The matter must be immediately reported to the **Chief Compliance Officer (CCO)**
2. An investigation is initiated to determine scope, cause, and impact
3. Affected parties and regulatory authorities are notified as required
4. Remediation actions (e.g., access revocation, retraining, disciplinary measures) are implemented
5. All incidents are logged and reviewed in annual compliance audits

H. Oversight and Enforcement

- The **CCO** is responsible for enforcing confidentiality protocols and conducting periodic reviews
- Confidentiality procedures are tested as part of **internal audits** and **independent compliance reviews**

- Any breach of confidentiality by staff is grounds for **disciplinary action**, up to and including termination

10.3 Data Security Measures and Cybersecurity Practices

Done.com Inc. maintains a rigorous and evolving set of data security measures and cybersecurity practices designed to protect customer information, transaction data, and compliance records from unauthorized access, manipulation, or loss. These controls are aligned with industry best practices, FINTRAC guidance, and the regulatory requirements under the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and **Personal Information Protection and Electronic Documents Act (PIPEDA)**.

A. Security Governance and Accountability

- The **Chief Compliance Officer (CCO)** is responsible for ensuring data security compliance within the AML/ATF framework.
- A dedicated **IT Security Lead** oversees the implementation of technical security infrastructure and cyber response procedures.
- Policies are reviewed and updated **at least annually** or following a significant system or risk change.

B. Core Cybersecurity Objectives

Done.com Inc. 's cybersecurity program is built around the following key pillars:

1. **Confidentiality** – Ensuring sensitive data is only accessible to authorized users
2. **Integrity** – Protecting data from tampering or unauthorized modification
3. **Availability** – Maintaining timely access to systems and data for legitimate operations

C. Technical Security Measures

Measure	Description
Encryption	All sensitive data is encrypted at rest and in transit (AES-256 / TLS 1.3)
Access Control	Role-based access (RBAC) and least privilege enforcement across systems
Multi-Factor Authentication	Required for all administrative accounts and compliance tools
Endpoint Protection	Anti-malware and EDR (Endpoint Detection & Response) on all employee devices
Firewall & IDS/IPS	Network perimeter secured with firewalls and intrusion detection systems

Database Hardening	Production databases are hardened and monitored for suspicious queries
Regular Patching	Operating systems and applications are patched in accordance with a set schedule
Cloud Security	Data hosted in secure, ISO 27001-compliant cloud environments (e.g., AWS, GCP)

D. Operational Security Practices

- **Data Loss Prevention (DLP):** Restrictions on USB usage, email forwarding, and external file sharing
- **Device Management:** All devices enrolled in Mobile Device Management (MDM) with remote wipe capabilities
- **Password Policy:** Complex password enforcement, auto-expiry, and lockout after failed attempts
- **Backups:** Regular encrypted backups with geographic redundancy
- **Logging and Monitoring:** Centralized log aggregation, SIEM tools, and 24/7 anomaly detection

E. Cybersecurity Awareness and Training

- All employees must complete **annual cybersecurity training**, including phishing simulations and secure data handling modules
- Specialized training is provided to **compliance staff** on secure STR handling and secure communications with FINTRAC
- Employees are encouraged to report suspicious emails or system activity through designated security channels

F. Incident Response and Recovery

- Done.com Inc. maintains a **Cybersecurity Incident Response Plan (CIRP)** that outlines procedures for:
  - Containment and eradication of threats
  - Notification to regulators or affected parties (if required by law)
  - Post-incident review and documentation
- A cybersecurity tabletop exercise is conducted **at least annually**

G. Third-Party Risk Management

- Vendors with access to Done.com Inc. systems or data must undergo **security due diligence**
- Data-sharing agreements include **confidentiality, encryption, and breach notification** clauses

- Access to third-party applications is reviewed quarterly and revoked if inactive or unnecessary

H. Compliance with Cybersecurity Standards

Done.com Inc. benchmarks its cybersecurity program against leading frameworks, including:

- **NIST Cybersecurity Framework (CSF)**
- **ISO/IEC 27001**
- **Center for Internet Security (CIS) Controls**

11. AML/CTF Governance and Oversight

11.1 Governance Structure and Oversight

Done.com Inc. has established a clear and accountable governance framework to oversee its Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) compliance program in accordance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and guidance from **FINTRAC**. This structure ensures that compliance is embedded into the company's leadership, risk management processes, and day-to-day operations.

A. Governance Objectives

The primary goals of Done.com Inc. 's governance structure are to:

- Ensure board-level visibility and oversight of AML/ATF compliance
- Allocate clear roles, responsibilities, and accountability across departments
- Support an ethical, compliant, and risk-conscious culture
- Maintain regulatory alignment through independent oversight and continuous improvement

B. Compliance Reporting Hierarchy

Role	Responsibility
Board of Directors (or Founders Group)	Ultimate accountability for the compliance program; approves key policies and risk appetite
Executive Management	Oversees compliance strategy and resource allocation; ensures business units cooperate with AML obligations
Chief Compliance Officer (CCO)	Directly responsible for the design, implementation, and effectiveness of the AML/ATF program

Compliance Team	Supports execution of customer due diligence, reporting, risk assessments, and internal audits
Business Unit Managers	Ensure compliance procedures are followed in operations (e.g., onboarding, trading, OTC desk)
All Staff	Required to comply with AML/ATF policies, complete training, and report suspicious activity

C. Chief Compliance Officer (CCO)

The CCO plays a central role in Done.com Inc. 's compliance governance framework:

- Reports directly to **Executive Management or the Board**
- Has **independent authority** to make compliance decisions without undue influence
- Leads the development and execution of:
  - AML/ATF policies and procedures
  - Risk assessment updates
  - Regulatory reporting (STRs, LCTRs, VCTRs, etc.)
  - Internal training programs
  - Internal audit and remediation follow-ups
- Participates in **strategic discussions** that may impact risk (e.g., product launches, new jurisdictions)

D. Board and Executive Oversight Activities

- Receive and review **quarterly compliance reports** summarizing:
  - Regulatory reporting activity
  - New or emerging risks
  - Internal audit findings and remediation progress
  - STR filing trends and enforcement developments
- Approve:
  - The **AML/ATF Compliance Program**
  - **Annual training plans**
  - **Risk assessment updates**
  - **Compliance budget and resourcing**
- Are briefed immediately in case of:
  - Regulatory inquiries, examinations, or penalties
  - Serious breaches or systemic compliance failures

E. Escalation and Communication Channels

Done.com Inc. maintains clear internal escalation channels to report:

- Suspicious activity or violations of compliance policies

- Emerging risks or potential system weaknesses
- Confidential disclosures or whistleblower concerns

Staff may escalate matters to their supervisor, the Compliance Team, or the CCO. Anonymous reporting is also available through designated secure channels.

F. Governance Documentation and Auditability

- The governance structure is formally documented in the **Compliance Program Manual**
- Changes to roles, reporting lines, or oversight responsibilities must be **board-approved**
- Governance documents are subject to **annual review**
- Records of compliance governance activities (e.g., board approvals, policy reviews, risk updates) are retained for **at least 5 years**

11.2 Board of Directors / Management Oversight

At Done.com Inc. , the Board of Directors (or equivalent governing body, such as the Founders Group in early-stage corporate structure) and executive management play an essential and proactive role in overseeing the company's Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) compliance framework. This oversight ensures that compliance is not only a legal obligation, but a strategic priority embedded in the company's risk culture, operations, and governance.

A. Governance Accountability

The Board and Executive Management are ultimately responsible for ensuring that Done.com Inc. :

- Has an effective, well-resourced, and independently managed AML/ATF compliance program
- Maintains a risk-aware organizational culture aligned with legal and ethical obligations
- Complies with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and related FINTRAC regulations

They are held accountable for ensuring that compliance risks are identified, understood, and properly mitigated throughout the business.

B. Key Oversight Responsibilities

The Board and Management commit to the following:

Responsibility	Details
Program Approval	Approving the written AML/ATF Compliance Program and any material updates
Compliance Officer Oversight	Appointing a qualified Compliance Officer and ensuring independence and authority
Risk Appetite & Strategy	Defining and reviewing AML/ATF risk tolerance and ensuring integration into business planning
Program Resourcing	Allocating sufficient budget, tools, and staff to support compliance functions
Monitoring Program Effectiveness	Reviewing periodic reports and audit results provided by the Compliance Officer
Regulatory Engagement	Being informed of significant compliance developments, regulatory inquiries, or penalties
Training and Awareness	Participating in senior management training and reinforcing compliance culture
Remediation and Enforcement	Supporting timely corrective action for any identified deficiencies or violations

C. Compliance Reporting to Management and the Board

The Chief Compliance Officer (CCO) reports to Executive Management and/or the Board on a **quarterly** basis (or more frequently if required). Reports include:

- Number and type of suspicious transaction reports (STRs), large cash transactions, VCTRs, and EFTs
- Updates on emerging risks and risk assessments
- Findings from internal or independent audits and status of remediation plans
- Summary of training, testing, and regulatory updates
- Any compliance incidents, breaches, or escalations

All board-reviewed materials are documented and archived for **at least five years** in accordance with PCMLTFA retention requirements.

D. Decision-Making and Approvals

The Board and/or Executive Management must formally approve the following elements:

- Appointment of the Compliance Officer
- Annual Compliance Program Review and Risk Assessment
- Major policy updates or remediation strategies

- Budget allocations for compliance functions and technology
- Engagements with external compliance consultants or legal counsel

These approvals are recorded in meeting minutes and compliance audit logs.

E. Board-Level Risk Culture and Ethics

The leadership at Done.com Inc. promotes a top-down tone of integrity and compliance by:

- Encouraging open communication and escalation of compliance concerns
- Supporting whistleblower protections and confidentiality
- Embedding AML/ATF risk considerations into strategic business decisions
- Ensuring that compliance is treated as a core business function, not an afterthought

11.3 Periodic Reporting to Senior Management

To maintain transparency, accountability, and proactive oversight of its Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) compliance program, Done.com Inc. ensures that periodic and event-driven reports are submitted by the **Chief Compliance Officer (CCO)** to **Senior Management and the Board of Directors (or Founders Group)**.

This structured reporting process helps management stay informed of key compliance metrics, risks, and regulatory obligations, while enabling timely decision-making and effective resource allocation.

A. Reporting Frequency

Report Type	Frequency
General Compliance Status Report	Quarterly
Suspicious Activity Summary	Quarterly (or ad hoc if critical)
Risk Assessment Review	Annually or upon major updates
Audit and Remediation Updates	Quarterly or post-audit
Regulatory Reporting Summary	Quarterly
Training Completion Report	Semi-annually
Significant Compliance Incidents	Immediate (within 24–72 hours)

B. Content of Compliance Reports

Each report includes key data, analysis, and trends relevant to AML/ATF compliance, such as:

- Summary of **STRs, LCTRs, VCTRs, and EFTs** filed with FINTRAC
- Overview of **unusual transaction patterns** or emerging threats
- Status of **risk assessment updates** and mitigation measures

- Internal or third-party **audit findings**, including pending and completed corrective actions
- **Compliance training participation and test results** by department
- Changes in **regulatory landscape** (e.g., FINTRAC updates, enforcement actions, typology alerts)
- Compliance breaches, incidents, or **escalated internal matters**

C. Audience and Delivery

Reports are submitted by the CCO to:

- **Chief Executive Officer (CEO)** or Managing Partner
- **Board of Directors / Founders**
- **Relevant Department Heads** (e.g., Trading Desk, Finance, Operations)

Reports may be delivered in:

- PDF format with appendices
- Presentation format for review during senior leadership meetings
- Verbal briefings with Q&A sessions when needed

D. Escalation of High-Risk Findings

If significant compliance issues are identified - such as:

- Failure to file a mandatory report
- Breach of confidentiality (e.g., STR exposure)
- Data security incident or suspicious employee activity
- New or heightened exposure to **sanctioned entities or high-risk jurisdictions**

Then the CCO is required to escalate immediately (within 24–72 hours depending on severity) to Executive Management, and initiate corrective measures in accordance with Section 8.4 (Corrective Action and Remediation).

E. Documentation and Retention

- All periodic reports are retained for **at least five years**
- Reports are archived in a secure Compliance Documentation Repository
- Access is restricted to authorized personnel and auditors/regulators upon request
- A version control system is in place to track changes and updates over time

12. Regulatory Communication and Cooperation

12.1 Communication with FINTRAC and Regulatory Authorities

Done.com Inc. is committed to maintaining proactive, transparent, and timely communication with the **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)** and other applicable regulatory authorities. This communication is essential to ensuring compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)** and supporting Canada's efforts to detect and deter money laundering and terrorist activity financing.

A. Designated Point of Contact

- The **Chief Compliance Officer (CCO)** is the designated liaison for all regulatory communications with FINTRAC and other authorities.
- The CCO ensures that all inquiries, requests, and notices from regulators are responded to accurately and in a timely manner.
- Contact information for FINTRAC and the CCO is documented in the Compliance Program and updated as needed.

B. Situations Requiring Communication with FINTRAC

Done.com Inc. communicates with FINTRAC in the following scenarios:

Communication Type	Trigger/Event
Suspicious Transaction Reports (STRs)	Reasonable grounds to suspect ML/TF activities
Large Cash Transaction Reports (LCTRs)	Receipt of CAD $10,000+ in cash within 24 hours
Electronic Funds Transfer Reports (EFTRs)	International wire transfers of CAD $10,000+
Virtual Currency Transaction Reports (VCTRs)	Virtual currency transactions totalling CAD $10,000+ within 24 hours
Registration and Renewal	New MSB registration or biennial renewal process
Change in Business Activities or Ownership	Significant changes to services, partners, corporate structure, or key personnel
Regulatory Requests or Examinations	Requests for documentation, interviews, or system access
Voluntary Disclosure or Incident Reporting	Self-reporting of errors, control failures, or policy breaches

C. Methods of Communication

Done.com Inc. uses the following secure channels to communicate with FINTRAC:

- **FINTRAC Web Reporting System (FWR)** – For submitting STRs, LCTRs, EFTRs, and VCTRs
- **MSB Portal** – For managing business registration, updates, and renewals
- **Secure Email or Phone** – For responding to inquiries or coordinating on compliance reviews
- **Written Correspondence** – For formal notices, submissions, and recordkeeping purposes

All communication records are securely retained for a minimum of **five years**.

D. Response Timelines

Type of Request	Response Deadline
Information request from FINTRAC	Within the timeline specified in request (typically 15 days)
Examination request for documentation	Immediate coordination; within 1–5 business days unless otherwise specified
Error or reporting correction	As soon as discovered, within 30 days
Voluntary disclosure	Promptly upon identification of non-compliance

E. Internal Escalation and Documentation

- Any correspondence from FINTRAC or other regulators is escalated to Executive Management within **24 hours**
- The CCO documents the nature of the inquiry, response actions taken, and any outcomes or follow-up items
- Communication logs are reviewed during **internal audits** and are made available to FINTRAC or legal counsel upon request

F. Communication with Other Authorities

In addition to FINTRAC, Done.com Inc. may be required to communicate with:

- **Law enforcement agencies** (e.g., RCMP, municipal police)
- **Canada Revenue Agency (CRA)** – in relation to tax compliance or audits
- **Office of the Superintendent of Financial Institutions (OSFI)** – if applicable
- **Provincial or territorial regulators** (if licensed in multiple jurisdictions)

The CCO ensures all such communications follow internal protocols, preserve confidentiality, and comply with applicable laws.

12.2 Cooperation with Law Enforcement Investigations

Done.com Inc. is committed to cooperating fully and lawfully with **law enforcement agencies** conducting investigations related to money laundering, terrorist financing, fraud, or other financial crimes. This cooperation is conducted in strict compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**, other applicable Canadian laws, and Done.com Inc. 's internal policies for confidentiality and regulatory reporting.

A. Legal Framework for Cooperation

Under Sections **63 to 65** of the PCMLTFA, reporting entities such as Done.com Inc. may be required to disclose certain information to law enforcement or other government bodies when:

- Served with a **production order**, **search warrant**, or **court order**
- Asked to provide additional information related to a previously submitted **Suspicious Transaction Report (STR)**
- Required to assist in investigations concerning transactions, customers, or patterns suggestive of money laundering or terrorist financing

B. Primary Law Enforcement Partners

Done.com Inc. may receive requests from the following agencies:

- **Royal Canadian Mounted Police (RCMP)**
- **Canada Border Services Agency (CBSA)**
- **Canada Revenue Agency (CRA) – Criminal Investigations Program**
- **Municipal or provincial police departments**
- **Other international enforcement bodies** (via legal mutual assistance treaties and proper legal channels)

C. Compliance Officer Role in Investigations

The **Chief Compliance Officer (CCO)** is the sole designated point of contact for law enforcement inquiries. The CCO is responsible for:

- Verifying the **legitimacy and scope** of any request before releasing information
- Ensuring the request is accompanied by **valid legal documentation** (e.g., warrant or court order)
- Coordinating internal efforts to retrieve relevant information
- Responding within the **legally prescribed timeline**
- Maintaining a **record of all disclosures, interactions, and supporting documentation**

No employee other than the CCO (or formally delegated Compliance Officer) may communicate with law enforcement about AML/ATF matters.

D. Confidentiality and Non-Tipping-Off

In accordance with Section 65 of the PCMLTFA:

- Employees are **strictly prohibited** from informing any client or external party that they are under investigation, or that information has been shared with law enforcement or FINTRAC.
- All responses to law enforcement are handled **confidentially** and **securely logged** in the compliance archive.

E. Process for Responding to Requests

1. **Receipt of Request:** The CCO receives and logs the inquiry or order.
2. **Verification:** The legal validity of the request is reviewed with internal or external legal counsel, if necessary.
3. **Data Collection:** Relevant documents, transaction records, customer profiles, and communication logs are retrieved.
4. **Disclosure:** Information is disclosed through **secure channels** only (e.g., encrypted email, secure portal).
5. **Confirmation:** A formal confirmation of delivery and receipt is obtained, if applicable.
6. **Internal Record-Keeping:** A file is created and stored in the compliance system, including:
    - Request details and contact information
    - Documents provided
    - Timeline of response
    - Legal basis for disclosure

F. Timeliness and Escalation

- Urgent requests are prioritized and responded to **within 24–72 hours**, depending on the nature and risk of the case.
- Any request that may have legal implications or exceed normal scope is escalated to **Executive Management and legal counsel** immediately.

G. Training and Preparedness

- All staff receive training on how to handle inquiries from law enforcement and are instructed to **redirect all such matters to the CCO**.
- Annual tabletop exercises may include mock law enforcement requests to ensure readiness and response consistency.

12.3 Procedures for Regulatory Examinations and Audits

Done.com Inc. is fully committed to maintaining readiness for **regulatory examinations, compliance reviews, and audits** conducted by **FINTRAC** or any other competent authority. These procedures ensure that all required records, systems, and personnel are prepared to support efficient, transparent, and accurate regulatory assessments.

A. Objectives of Examinations and Audits

Regulatory audits are conducted to:

- Assess compliance with the **Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)**
- Review the effectiveness of the AML/ATF Compliance Program
- Evaluate recordkeeping, reporting, and risk management practices
- Identify any weaknesses, gaps, or violations requiring corrective action

B. Primary Oversight Authority

The main authority responsible for AML/ATF compliance oversight is:

Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)
https://www.fintrac-canafe.gc.ca

Additional oversight may also come from:

- The Canada Revenue Agency (CRA)
- Provincial regulators (if applicable)
- Law enforcement (in coordination with FINTRAC or via legal orders)

C. Pre-Audit Preparation

When notified of an upcoming examination:

1. **Compliance Officer Notification:** The CCO is responsible for coordinating the response and serving as the primary point of contact.
2. **Internal Kickoff Meeting:** A preparation meeting is held with executive management and relevant staff.
3. **Document Review & Compilation:** All required documentation is collected, organized, and reviewed for completeness, including:
    - AML/ATF policies and procedures
    - Risk assessments
    - Training logs and materials
    - STRs, LCTRs, EFTRs, VCTRs
    - Client identification and due diligence files

- Records of internal audits, corrective actions, and board reports

4. **System Access:** Temporary, secure access may be granted to systems or files required by the regulator.

D. Examination Activities

During an examination or audit, regulators may:

Activity	Description
Interviews	With the CCO, compliance staff, senior management, or front-line employees
Document Review	Verification of customer files, transaction records, reports filed to FINTRAC
System Walkthroughs	Demonstrations of case management, onboarding, risk scoring, and alerts
Sampling and Testing	Randomly selected files for verification of compliance with PCMLTFA
Assessment of Risk Management	Review of risk framework, thresholds, and categorization methodology
Evaluation of Training	Evidence of training frequency, coverage, and effectiveness

E. During the Audit

- The **CCO** or delegate must be present during all interactions with examiners.
- All questions are answered **truthfully, respectfully, and transparently**.
- If information is unavailable or uncertain, the Compliance Team must **follow up in writing** as soon as reasonably possible.
- A secure meeting room or virtual environment is made available for the regulators.

F. Post-Examination Responsibilities

Following the examination:

1. **Receipt of Draft Findings:** The regulator may issue a **preliminary report** with findings and recommendations.
2. **Management Response:** The CCO drafts a written response, including clarification or challenge of findings where appropriate.
3. **Action Plan Development:** If deficiencies are identified, a **Corrective Action Plan** is created (per Section 8.4).
4. **Final Report Review:** The final outcome of the examination is documented and shared with the **Board or Founders**.

5. **Audit File Maintenance:** All correspondence, notes, and reports from the audit are retained securely for **minimum 5 years**.

G. Internal Communication

- The CCO delivers a **summary report** of audit results and required improvements to:
  - Executive Management
  - The Board of Directors (or Founders)
  - Any directly impacted departments or staff
- If the audit identifies **systemic issues**, internal retraining and process adjustments are initiated.

H. Continuous Readiness

To ensure readiness for unannounced audits or regulatory reviews:

- All records and reports are maintained **continuously and systematically**
- Internal audits are conducted at least **annually**
- Staff are trained to understand what to expect and how to respond during an examination

13. Fraud Prevention

13.1 Purpose & Scope

Purpose: Prevent, detect, and respond to first-party and third-party fraud that may overlap with ML/TF, sanctions evasion, or market abuse.

Scope: All DoneOTC products/channels — OTC crypto↔fiat, precious metals, FX, bank wires/e-transfers; corporate & individual clients; remote and face-to-face.

Regulatory alignment: Fraud indicators feed AML monitoring (unusual/suspicious transactions), KYC/KYB (identity assurance), VCTR/EFTR/LCTR/STR reporting, recordkeeping, and Travel Rule controls for virtual assets.

13.2 Definitions & Taxonomy

ATO (Account Takeover): Unauthorized access/control of a client account.

Social Engineering: Phishing, vishing, smishing, or other manipulation of clients/staff.

Synthetic Identity: Fabricated identity using real/false PII.

Money Mule: Person/entity moving funds for others (knowingly or not).

BEC (Business Email Compromise): Email fraud altering payment instructions.

Investment/Romance Scam: Inducing victims to fund fraudulent schemes (often crypto).

Refund/Chargeback Abuse: Illegitimate reversal of legitimate transactions.

First-Party vs Third-Party Fraud: Perpetrated by account owner vs external actor.

Crypto Typologies: Mixer/tumbler use, peel chains, darknet exposure, high-risk exchange clustering, sanctions proximity, chain hopping.

13.3 Governance & RACI

Role	Responsibilities	R	A	C	I
Board/CEO	Sets risk appetite; approves program/policies; receives KPI/KRI reports		A		I
CAMLO / Compliance Officer	Integrates fraud with AML/ATF; approves alerts → STR; regulator liaison		A	C	I
Fraud Lead / Analyst	Designs rules; investigates cases; recovery; evidence preservation	R		C	I
Engineering/Data	Builds controls, device signals, dashboards, model governance	R		C	I
Front-Office / Trading Ops	Callbacks, beneficiary validation; applies hold periods	R			I
Finance/Treasury	Settlement oversight; maker-checker for payouts	R		C	I
Legal	LEO requests; evidence handling; client notifications	R		C	I

13.4 Fraud Risk Assessment (FRA)

Separate FRA from ML/TF RA but cross-refer inputs/outputs.

Scales: Likelihood (1–5) × Impact (1–5) → Inherent risk; subtract control effectiveness (1–5) → Residual risk.

Data inputs: Product/channel maps, historical loss/chargebacks, alerts, ATO/mule cases, device/IP intel, blockchain analytics, law-enforcement typologies, ACFE/FATF advisories.

Cadence: Quarterly mini-FRA; annual full FRA.

Triggers for reassessment: New product/jurisdiction, material rule/model change, incident > CAD $25k, regulator notice, LEO inquiry.

13.5 Preventative & Detective Controls Across the Lifecycle

A. Onboarding (KYC/KYB)

- Identity assurance: Government ID (front/back), liveness/video check, selfie-to-ID match, document anti-tamper (EXIF, hologram, barcode validation).
- Device/IP/velocity: Device fingerprint, IP geolocation, VPN/hosting detection, signup velocity, impossible travel.
- KYB integrity: Registry pull, beneficial ownership verification, anti-tamper checks on corporate docs, watch for shell/redomicile patterns.
- Sanctions/PEP/adverse media screening; synthetic ID heuristics (thin file, inconsistent DOB, mismatched selfie/liveness).

B. Payments/Settlement

- Name matching & beneficiary validation (payee-name match, IBAN/ABA checksum).
- Dual-channel confirmation callbacks for first-time or high-value beneficiaries.
- Micro-deposits where applicable before first large payout.
- Velocity/amount limits (PLACEHOLDER): CAD $10k first 24h; $50k first 7 days; tier up post-review.
- Hold periods (risk-based) for new payees/funding sources; manual review for deviations.

C. Crypto-Specific

- Wallet risk scoring (cluster attribution, sanctions proximity, darknet/mixer exposure %, peel chains); deny-list and allow-list flows.
- Travel Rule readiness: collect/validate originator/beneficiary info when in scope; secure messaging with VASPs.
- Chain-hopping/mixer detection; monitor recently created or first-touch addresses; scrutinize cross-exchange hops.

D. Session/Device Security

- MFA (TOTP/passkey), device binding, session timeouts.
- ATO indicators: SIM-swap signals, credential-stuffing spikes, password resets + new device.
- Impossible travel and sudden device fingerprint change → step-up auth + lock.

E. Staff/Process

- Dual controls and maker-checker for payouts & address changes.
- Callback verification for high-risk instructions (verified numbers only).
- Segregation of duties (trader vs approver vs releaser).
- Four-eyes review for overrides/whitelisting.

13.6 Monitoring & Alerting

Signals - Rules: name mismatch; new device + high value; >$10k same-day cross-funding; >3 beneficiary changes in 7 days; wallet risk score ≥ X; mixer exposure ≥ Y% (PLACEHOLDER).

Signals - Statistical/ML: anomaly scores on value/frequency/counterparty graphs; mule clustering; ATO likelihood.

Thresholding: start conservative; monthly point-in-time back-testing and tuning.

Case workflow: Triage → Investigate → Disposition (Approve/Decline/Hold) → Recovery/Chargeback → Reporting (STR/VCTR/EFTR/LCTR). SLA: triage < 4h; decision < 24h for high risk.

Linkages: When indicators suggest ML/TF, escalate under AML Monitoring; consider STR.

13.7 Escalation & External Reporting

Escalation ladder: Analyst → Fraud Lead → CAMLO; emergency freeze authority held by CAMLO or delegate.

Evidence preservation: Export logs (device/IP, auth, chats/calls), blockchain traces, bank confirmations; hash artifacts; restrict editing.

External: Law-enforcement engagement as appropriate; civil recovery; notify platforms (exchanges/PSPs) where needed.

Client notifications: Risk-based; avoid tip-off in STR contexts.

13.8 Prohibited/Restricted Sectors

Prohibited: unlicensed MSBs/PSPs; mixers/tumblers; privacy-coin services; shell banks; darknet markets; sanctioned entities/persons.

Restricted (EDD + Senior approval): gambling, offshore FX, high-risk crypto exchanges, precious metals wholesalers with cash dominance, freight forwarders with high-risk corridors, NGOs in conflict zones.

Appendix A: Key Regulatory References

1. Statutes and Regulations

Reference	Description
Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)	The primary Canadian legislation governing AML/ATF obligations for reporting entities, including MSBs and dealers in virtual currency.
Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (PCMLTFR)	The accompanying regulations to the PCMLTFA that define reporting thresholds, verification standards, recordkeeping obligations, and more.
Criminal Code of Canada	Provides definitions and offences relating to money laundering and terrorist financing under federal criminal law.
Income Tax Act – s. 241	Governs confidentiality and data disclosure rules relevant to CRA and FINTRAC coordination.

2. Regulatory Guidelines and Publications

Issued By	Reference/Link	Description
FINTRAC	FINTRAC Guideline 4 – Compliance Program	Outlines the five elements of an effective compliance program for MSBs and other reporting entities.
FINTRAC	FINTRAC Reporting Overview	Comprehensive resources and forms for STRs, LCTRs, EFTRs, VCTRs, and other reporting types.
FINTRAC	MSB Registration Portal	Portal for registering, renewing, and updating Money Services Businesses in Canada.
FINTRAC	Sector-specific guidance (Virtual Currencies, MSBs, Securities)	Additional compliance guidance based on business model and asset classes.

3. International Standards and Best Practices

Organization	Reference	Description
Financial Action Task Force (FATF)	FATF Recommendations	International AML/ATF standards adopted by Canada and referenced in domestic regulation.
Egmont Group	Principles for Information Exchange	Framework for cross-border sharing of financial intelligence.
Basel Committee on Banking Supervision	Sound Management of Risks Related to ML/TF	Global guidelines for financial institutions in risk-based AML implementation.

4. Industry Training and Certification Bodies

Organization	Purpose
Association of Certified Anti-Money Laundering Specialists (ACAMS)	Training, certification, and ongoing professional education in AML/ATF compliance.
Canadian Institute of Financial Crime Analysis (CIFCA)	AML-focused training for Canadian MSBs and fintechs.

5. Other References

Source	Reference
Government of Canada – Sanctions List	Canadian Sanctions and Terrorist Listings
Office of the Privacy Commissioner of Canada (OPC)	Guidance on Privacy Obligations in AML Context
Canada Revenue Agency (CRA)	Reporting and Tax Obligations of MSBs

Appendix B: Forms and Templates

A. Know Your Client (KYC) / Customer Due Diligence Forms

Form Name	Purpose
KYC – Individual Client Profile Form	Collects client identification, risk rating, and verification method for individuals
KYC – Corporate/Entity Client Profile Form	Gathers business information, beneficial ownership, directors, and structure
Identity Verification Checklist	Ensures accepted documents are collected per FINTRAC standards
Beneficial Ownership Declaration	Confirms direct or indirect ownership of 25% or more in an entity
PEP/Head of International Organization Declaration Form	Screening and disclosure form for PEPs and related parties
Source of Funds / Wealth Declaration	Used for high-risk clients to assess legitimacy of funding

B. Enhanced Due Diligence (EDD) Forms

Form Name	Purpose
High-Risk Client EDD Assessment Template	Captures rationale and supporting evidence for high-risk categorization
Jurisdiction Risk Evaluation Form	Records sanctions, FATF status, and geographic risk factors
EDD Monitoring & Escalation Checklist	Ensures approval and controls are applied to high-risk clients

C. Transaction Monitoring and Reporting Forms

Form Name	Purpose
Unusual Activity Identification Form	Internal report template for recording suspicious behavior or patterns
STR (Suspicious Transaction Report) Internal Draft	Internal draft template before FINTRAC submission
LCTR Record Log	Template to document large cash transactions and supporting ID
VCTR and EFTR Reporting Tracker	Tracks currency and international transfer filings and rationale
Internal Escalation Record	Documents who was notified and actions taken in response to red flags

Fraud Red Flags & Decision Tree	Alerting to potential fraud activity

D. Risk Assessment Tools

Form Name	Purpose
Client Risk Scoring Matrix	Assigns a risk score based on customer type, geography, and transaction profile
Product and Service Risk Evaluation Template	Evaluates inherent ML/TF risks of each product class (e.g., OTC crypto)
Geographic Risk Mapping Sheet	Ranks regions or countries by regulatory risk and exposure level
Risk Assessment Summary Report	Documents annual compliance risk assessment and methodology used

E. Training and Certification Forms

Form Name	Purpose
Employee AML/ATF Training Log	Tracks who completed mandatory training and when

F. Internal Audit and Compliance Review Templates

Form Name	Purpose
Internal Audit Checklist – AML Program	Comprehensive review tool for program control testing
Independent Review Engagement Letter	Used when hiring third-party auditors or consultants
Compliance Deficiency Log	Records findings, severity level, and remediation timeline
Corrective Action Plan Template	Structured plan with ownership, timeline, and resolution notes

G. Law Enforcement and Regulatory Communications

Form Name	Purpose
Regulatory Contact Log	Records interactions with FINTRAC, CRA, or law enforcement
Response to Information Request Template	Standardized format for producing requested records securely

Incident Report Escalation Memo	Summarizes major breaches or investigations escalated to executives