New Wave Payments Inc.

(O/A “Nefin”)

AML / CTF Policy

Document version: 0.5

Revision history

Version	Revision Date	Revised by	Changes	Recommendations
0.5	April 6th, 2024	Ihor Kreshchenko, Advapay	Original draft created	None

Document properties

Company name	**New Wave Payments Inc.**
Title	AML / CTF Policy
Owner Name	
Owner Title	Compliance Officer
Date Created	April 6th, 2024

Introduction

NEFIN is an Ontario corporation, with registration number 1000680292. Nefin acknowledges the importance of fulfilling specific obligations as required by the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and associated regulations, such as reporting, record keeping, knowing your clients, and having a compliance program implemented, to help combat money laundering and terrorist activity financing in Canada.

MSB (Money Services Business)

Nefin Limited is an MSB in Canada because it offers one or more of the money services business services and has a place of business in Canada. MSBs are subject to regulations and oversight by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to prevent money laundering and terrorist financing. Money services businesses must implement a compliance program that will help to ensure the regulatory requirements are met.

Money Laundering

Money laundering is the process of disguising the proceeds of illegal activities as legitimate funds. The term "money laundering" refers to the practice of taking "dirty" money obtained through criminal activity, and making it appear as though it was earned through legal means.

The process of money laundering typically involves three stages:

1. Placement: This is the initial stage in which the illegal proceeds are introduced into the financial system. The goal is to get the funds into the legitimate financial system as quickly and discreetly as possible, often through cash deposits or wire transfers.
2. Layering: This stage involves moving the funds through a series of transactions and accounts to create a complex web of financial transactions that makes it difficult to trace the original source of the funds. This can involve transferring the funds through multiple accounts or making investments in different types of assets.
3. Integration: This is the final stage in which the "clean" funds are reintroduced into the economy and used to purchase assets or conduct business. The goal is to make the funds appear as though they were obtained through legitimate means, and to prevent law enforcement from tracing the funds back to their illegal origins.

Money laundering is a serious criminal offense that can have serious consequences. It is often associated with organized crime, drug trafficking, and terrorism financing, and is subject to strict laws and regulations in most countries.

Terrorist Financing

Terrorist financing refers to the practice of providing financial support or resources to terrorist organizations or individuals in order to facilitate or carry out acts of terrorism. This can include

providing money, weapons, or other resources to individuals or groups that engage in terrorist activities.

Terrorist financing is a serious criminal offense that is often closely linked to money laundering. It is used to support a range of terrorist activities, including the planning and execution of attacks, the recruitment of new members, and the purchase of weapons and other resources.

To combat terrorist financing, many countries have implemented strict laws and regulations designed to prevent the flow of funds to terrorist organizations. Financial institutions are required to monitor transactions and report any suspicious activity to law enforcement authorities. Governments also work closely with international organizations to share information and coordinate efforts to combat terrorist financing on a global scale.

Preventing terrorist financing is a critical part of the overall effort to combat terrorism and maintain global security. By disrupting the flow of funds to terrorist organizations, law enforcement and financial institutions can help prevent acts of terrorism and protect the safety and security of citizens around the world.

Compliance Program

A compliance program is a program established and implemented by a reporting entity (RE) and is intended to ensure their compliance under the PCMLTFA and associated Regulations. A compliance program forms the basis for meeting all your reporting, record keeping, client identification and other know-your-client requirements under the PCMLTFA and associated Regulations. All REs must establish and implement a compliance program.

Specifically, all REs must implement the following elements of a compliance program by:

- appointing a compliance officer who is responsible for implementing the program;
- developing and applying written compliance policies and procedures that are kept up to date and, in the case of an entity, are approved by a senior officer;
- conducting a risk assessment of your business to assess and document the risk of a money laundering offence or a terrorist activity financing offence (ML/TF) occurring in the course of your activities;
- developing and maintaining a written, ongoing compliance training program for your employees, agents or mandataries, or other authorized persons;
- instituting and documenting a plan for the ongoing compliance training program and delivering the training (training plan); and
- instituting and documenting a plan for a review of the compliance program for the purpose of testing its effectiveness, and carrying out this review every two years at a minimum (two-year effectiveness review).

Business Model Summary

- Nefin is global financial technology company that provides financial services to businesses including:
    - Multicurrency accounts
    - Foreign exchange
    - Payment services
    - Card issuance via third-party providers
- Nefin operates using b2b model.
- Nefin enables its business customers in Canada and other developed countries to open a multicurrency account and utilize it for treasury management, foreign exchange and payments to counterparties located mainly in the emerging markets.
- Expansion will be driven by the market opportunities in other countries.
- Business payments is a key service for Nefin at this time.
- Clients of Nefin can also receive payments from their counterparties as part of the normal course of business.
- Nefin currently supports the following currencies: CAD, EUR, USD, GBP, SGD, HKD, AED, JPY, AUD, CHF, CNY, SEK, NZD, MXN, and other Tier-1 and Tier-2 currencies
- Foreign exchange services are offered through partnership with liquidity providers and correspondent banks in Canada and abroad.
- Nefin does not accept cash from customers.
- Nefin does not participate in, endorse, or otherwise affiliate with ICOs or other cryptocurrencies which may be considered securities.
- Nefin does not engage directly with any store of value, currency, or other product which may constitute a security.
    - Nefin clients may be offered services or products related to securities via Nefin partnership with appropriately licensed service providers.
- Nefin does not list, participate in, endorse, or otherwise affiliate with security tokens.
- Business clients are defined as businesses that have a current contractual relationship with Nefin;
- Further explanation of mandataries, clients, customers and their relationship to Nefin is contained in this document and other policies in the compliance and operational suite.

Regulatory Overview

- Nefin is a Canadian money services business, operating under registration number M24151114 providing the MSB activities of money transferring, foreign exchange dealing and payment services within Canada and worldwide.
- Note that Nefin does not provide:
    - Money orders

  - Traveler's cheques
  - Cheque cashing
  - Issuing and redeeming money orders
  - Casino or gambling services
  - Crowdfunding services
  - Virtual currency exchange
- Nefin and related entities, strive to follow the rules and regulations defined by Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and adopt MSB best practices where possible.
- Nefin is required to:
  - Report eligible transactions
  - Identify clients according to MSB guidelines
  - Facilitate independent review of our compliance program
  - Facilitate regular training of employees with regard to AML/CTF
  - Maintain a risk assessment and risk-based approach to service delivery
- FINTRAC provides regulatory oversight to the MSB industry and Nefin is registered with FINTRAC as noted above.
- Nefin has implemented a compliance regime that references the requirements for MSBs under the PCMLTFA.
- Nefin may be subject to audits by FINTRAC, the Canadian Securities Commission or other regulatory entities.
- Nefin supports the efforts of FINTRAC to mitigate and curtail illicit activity and will provide reasonable assistance to FINTRAC, and its designates in the event of an audit or reportable event.

Non-compliance

- Compliance with FINTRAC guidelines is not optional. Non-compliance with regulations and legislation may result in criminal or administrative penalties.
- Criminal penalties may include:
  - Failure to report suspicious transactions: up to $2 million and/or 5 years imprisonment.
  - Failure to report a large cash transaction or an electronic funds transfer: up to $500,000 for the first offence, $1 million for subsequent offences.
  - Failure to meet record keeping requirements: up to $500,000 and/or 5 years imprisonment.
  - Failure to provide assistance or provide information during compliance examination: up to $500,000 and/or 5 years imprisonment.

  - Disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.
- Administrative penalties may include:
  - A minor violation: $1 to $1,000 per violation
  - A serious violation: $1 to $100,000 per violation
  - A very serious violation: $1 to $100,000 per violation for an individual and/or $1 to $500,000 per violation for an entity
- Internally, employees found or suspected of non-compliance with this policy, or any regulations/legislation may be subject to disciplinary procedures inclusive of dismissal.

Flow of Funds

Below is the described Flow of Funds. The specific implementation may vary depending on the jurisdiction and currency pair, but generally, it consists of three steps, the sequence of which can also change from case to case.

Regardless, the steps are as follows:

1. Receipt of funds by our client from their counterparty in CAD or one of the main Western currencies (USD or EUR, less commonly GBP or CHF).
2. Currency exchange to the currency in which our client makes purchases - either directly or through a transition via USD.
3. Payments to suppliers, either directly from the correspondent account or through an external MTO (Money Transfer Operator). In some cases, the third step can be combined with the first.

Step 1. Incoming payment

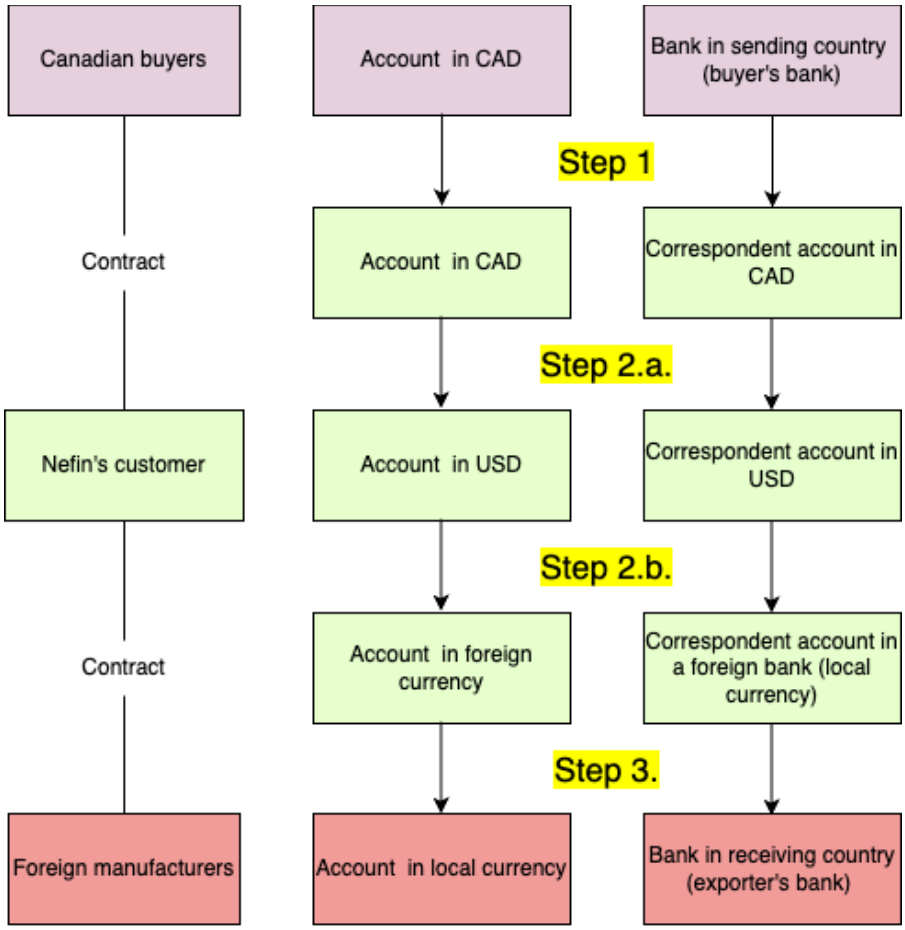
- Clients of Nefin will accept payments in various currencies, including CAD, EUR, USD, GBP and CHF.
- Their end-customers will pay from their accounts opened in regular Canadian banks to accounts of Nefin's customers opened in Nefin. In order to accept customers' funds Nefin opens segregated accounts in banks and financial institutions in abovementioned currencies.
- Nefin intends to use both omnibus/pooled accounts and accounts with dedicated vIBANs / account numbers.

Step 2. Currency exchange

- At this step customers of Nefin can exchange their funds received in CAD or another major western currency to the currency in which pay-out will be made, or USD (in the case if payout will be made through an external monet transfer operator).
- Currency exchange can be performed by a correspondent bank, or separate liquidity provider (B2B online currency exchange platform).

Step 3. Payout

- There are three payout methods which are considered depending on a currency pair and remittance corridor.
    - A. At the step 2 funds are converted to USD, and then transferred via an external money transfer operator.
    - B. At the step 2 funds are converted to a currency of supplier, and then transferred via SWIFT.
    - C. Supplier gets immediately paid from a correspondent account in his currency, which is possible thanks to holding additional own funds (working capital) on a correspondent account in supplier's currency. At the end of the day the account balance is replenished with one SWIFT transfer.



Regulatory Outlook

- Our primary regulatory focus is on FINTRAC MSB requirements; however other requirements worth noting are:
    - FATF Recommendations
        - FATF recommendations are non-binding and represent “best practice” for FIUs and the entities they regulate.
        - Recommendation 16 SPECIFICALLY addresses virtual asset service providers and remittance providers:
- Payment Service Providers (PSP) must register with local FIU.
- FIUs should supervise/regulate PSPs
- PSPs should implement a customer identification program where clients are identified at a threshold of $1,000.00 in usage or greater.
- PSPs should provide KYC and other information to law enforcement and similar 3rd parties on request.
- PSPs should comply with international requests for information from law enforcement and regulatory bodies.

- Travel Rule (FINTRAC) / (BSA) rule [31 CFR 103.33(g)]
  - Commonly known as the "travel rule" this requires financial institutions to share the following information for any transaction involving one or more financial institution:
    - Transmitter name
    - Transmitter account number
    - Transmitter address
    - Transmitter banking/financial institution details
    - Amount of transaction
    - Date of transaction
    - Recipient banking/financial institution details
    - Recipient name
    - Recipient account number
    - Recipient address
- As such, Nefin observes and implements "best practice" with regard to AML/CTF regulations wherever feasible in the course of our business.

Accountability and Commitment

- Nefin is committed to deterring and combating money laundering/terrorist financing both in our systems and the world at large.
- Nefin has adopted a risk-based approach and compliance strategy that is approved by executives.
- Per this policy, and other related policies Nefin is committed to full compliance with requirements that are designed to deter and detect actual/potential money laundering/terrorist financing (ML/TF) as well as other activities that enable/facilitate OR are related to ML/TF such as fraud.
- Nefin encourages and actively develops an internal culture of compliance and ethics among staff, see other policies for details.
- Nefin dedicates resources to compliance and risk management including implementing the below recommendations from FINTRAC for a sufficient compliance regime:
  - Appointment of a dedicated, knowledgeable Compliance Officer.
  - Development and maintenance of a risk management program.
  - Documented training program for all Nefin staff.
  - Development and application of internal policies, processes and other initiatives directly related to anti-money laundering/counter terrorist financing.
  - Regularly scheduled independent reviews to assess the efficacy and relevance of Nefin regime.
    - Note that an independent review is required every 2 years.
    - First independent review is due on 2025-04-12 (2 years from Date of MSB Registration)

- Nefin must renew our FINTRAC MSB registration every 2 years.
- If Nefin ceases offering MSB services for any reason, we must notify FINTRAC within 30 days of cessation of service.

Immunity from Prosecution

- Nefin recognizes that part of any effective compliance regime is protection for those who comply or attempt to comply in good faith.
- Nefin supports the requirement for personnel to identify and report suspicious or otherwise reportable transactions to FINTRAC and will attempt to protect said staff from civil and criminal proceedings where possible.

Appointment of Compliance Officer

- The PCMLTFA requires the appointment of a designated Compliance Officer to oversee the compliance regime.
- The Compliance Officer is responsible for managing the day-to-day compliance and anti-money laundering activities of the business and acts independently from all other departments/divisions reporting directly to the executive team.
- Duties and responsibilities of the Compliance Officer include, but are not limited to:
    - Administer and implement the risk management policies of the organization as a whole.
    - Oversee customer intake as it relates to brokers, mandataries, end customers, and other clients.
    - Complete risk assessments of new markets, industries, and clients as required.
    - Review external partnerships with vendors, acquirers, and other parties to ensure they are a fit for the risk appetite, brand, and policies of Nefin.
    - Monitor regulations in major jurisdictions and industries where Nefin, and their clients, conduct business for material changes.
    - Ensure policy suite is up to date and commensurate with regulation in industries/markets serviced.
    - Conduct periodic risk assessments and mitigate/avoid/transfer risk accordingly.
    - Facilitate AML training to all staff.
    - Engage in ongoing monitoring of transactions, web presence, websites, and reputation of Nefin and its clients to detect/act on suspicious activity.
    - Co-ordinate periodic independent reviews of the compliance regime.
    - Respond to 3rd party requests for information from law enforcement, regulatory bodies, and other external parties.
    - Report to management on compliance activities and the status of the compliance regime as a whole.
    - Engage in account opening and maintenance with suppliers and vendors.

- Respond to requests for information about corporate structure, ownership and licensing from suppliers.
- Delegate any of these tasks, or related tasks, to junior Compliance staff and oversee their administration and completion.

Nefin's Appointment of Compliance Officer

Date	Name	Role	contact
		Compliance Officer	

AML – CTF Administration Policies and Procedures

- The Nefin policy suite directly related to AML-CTF, and risk management is as follows:
  - AML – CTF Policy
  - Risk Assessment
  - Business Client Acceptance Policy
  - Country Acceptance Policy
  - Document Retention Policy
  - Customer Intake Process
  - Anti-Bribery, Corruption, Gifts, Hospitality Policy

Risk-based Approach

- Nefin employs a risk-based approach and therefore development and implementation of the compliance program is informed by the risk appetite of Nefin and our strategic partners.
- In accordance with regulations the Compliance team conducts risk assessments specifically related to money laundering and terrorist financing risks on all customers and counterparties.
- In addition to the risk assessment process, the Compliance team makes and implements recommendations to diminish risk to an acceptable level.
- Nefin's risk assessment results for clients are rated on a three-tiered system - low, medium, or high risk for Money Laundering:
  - Periodic reviews for clients are dependent on the file risk rating:
    - Low - 18 months;
    - Medium - 12 months; and
    - High - 6 months.

- This risk assessment process considers the following items:
    - Where are clients located?;
        - Where are their end customers or counterparties located?
    - How is service provided to these clients? (electronically, in person, etc.);
    - Types of service offered to clients;
    - Types of clients serviced; and
    - Type of end customers or counterparties using our clients' services.

- Nefin strives to mitigate risk whenever possible.
- Where risk cannot be sufficiently mitigated/transferred/avoided, Nefin may decline to engage in the risky activity.
- Effective risk assessment and mitigation is critical to maintaining positive associations/perceptions of the Nefin brand with our external partners including regulators, banks and payment processors. It is imperative to adhere to PCMLTFA and to avoid any negative effect on our brand, ensuring we do not contravene the PCMLTFA or other salient regulations and finally, deterring and decreasing the amount of illicit activity in the world at large?

Risk Assessment

- Nefin has prepared a separate Risk Assessment document, which complements, and should be read alongside, this Policy. The aim of the Risk Assessment is to identify, assess, and understand the risks facing the Firm from a business-wide perspective. This is critical for Nefin's development of effective controls and measures to mitigate identifiable risks wherever and however they present in Nefin's business.
- Broadly, the Risk Assessment intends to:
    - Identify the specific risks associated with money laundering and terrorism financing that Nefin might face. This includes understanding the nature of threats, potential vulnerabilities in products, services, customers, or transactions, and the potential consequences of these risks materializing.
    - Analyze the inherent risk exposure and the quality of existing controls by outlining the likelihood and impact of potential risks.
    - Understand the broader context of the risk landscape, considering factors like the regulatory environment, the socio-political situation, technological developments, and trends in the finance and technology sector. It also involves understanding the geographical factors affecting the Firm's operations and identifying high-risk jurisdictions.
    - Develop and adjust the Firm's AML/CTF programs in light of the assessment by revising policies, procedures, and controls so that they are tailored to manage and mitigate the specific risks faced.

  - Ensure compliance with AML/CTF laws and regulations applying to Nefin by helping to set mechanisms for reporting of suspicious activities, record keeping, and the sharing of necessary data with government authorities.
  - Develop strategies that manage and mitigate identified risks through strategies, including declining providing services to high-risk industries, customers, or transactions, severing relationships that pose unacceptable risk and alike.
  - Establish a process of continuous reflection, improvement, and adaptation that can address changes in the way money laundering and terrorist financing occur.
  - Maintain and bolster stakeholder confidence by demonstrating a strong commitment to preventing financial and organised crime.
- While the Risk Assessment provides a detailed risk assessment from a business-wide perspective, the purpose of this section is to highlight some of its key points.
- Note:
  - The Assessment provides a high-level view of Nefin's current position regarding industries serviced, geographies serviced, customer intake and service delivery.
  - Regulatory guidance, business strategy, operating model, and volumetric considerations were all factored in when determining inherent risk in each category.
  - The assessment may not be exhaustive/current, but all efforts are made to ensure it is regularly revisited and updated.
- Scheduled improvements to the Nefin AML/CTF regime include:
  - Optimization of the monitoring rules to reduce false positive matches and maximize effectiveness of monitoring
  - Optimization of automated methods to enhance KYC while keeping the account opening process seamless and straightforward for customers
  - Increased usage of automated methods for sanctions monitoring and compliance.

Types of Risk

- The Firm shall identify in its Risk Register and Assessment inherent risks facing the Firm and the sector in which it operates across the following categories:
  - Customer
    - Industry
    - Products/services provided within industry
    - Jurisdiction
  - Payment instruments
  - Transaction risk
  - Operations
  - Vendors/partners
  - Other

Customer Risk:

- Nefin only services business customers (i.e., the Firm does not currently serve individuals).
- Customers are identified and verified commensurate with current legislation at usage thresholds and are checked against watch lists at onboarding.
- Services are only provided to customers that pass Nefin's due diligence procedure.
- Customers that are a match to any applicable regulatory or government watch lists are not serviced under any circumstances.
- High-risk industries such as gaming, adult material, and cannabis are not currently served.

Jurisdiction Risk:

- Customers with locations in high-risk jurisdictions are only accepted with the presence of enhanced due diligence. Customers are not accepted from countries subject to sanctions.
- Many customers are from low-risk countries (e.g., Canada) but there is exposure to medium and high-risk countries, including China, and LATAM jurisdictions which shall require mitigation controls to be in place.
- Ultimate beneficial owners of clients may reside in or visit restricted or banned locations without the knowledge of Nefin. Accordingly, enhanced due diligence will be required in circumstances arousing suspicion.

Payment Instruments Risk:

- All funds, client, and customer inclusive, are processed through recognised/reputable financial institutions and/or payment processors.
- Number of transactions are monitored and, where necessary controlled.
- Specific source of funds is not always known but all funds come from recognised financial institutions and/or payment processors.
- Purpose of transfer is known and supported by documentation (e.g. invoice).
- Onboarding is not conducted in a face-to-face exchange, which makes it more difficult to identify customers. All identification documents submitted as part of onboarding are checked for signs of fraud / transactions on behalf of a third party.

Transaction Risk:

- Transaction amounts are typically high and attractive for high volume money laundering; smurfing activity is prevented via velocity controls and transaction monitoring, including specific rules targeting smurfing (e.g., flagging a single, or group of transactions within a 24-hour period, that exceeds $10,000.00 CAD for further reporting).

- Wires are accepted from medium and high-risk countries upon appropriate extended due diligence. Wires are not accepted from shell banks, decreasing the risk of ML/TF.
- Cash is not accepted directly from customers or collection partners.
- Credit cards, debit cards, vouchers, bank drafts, email transfers, and cryptocurrencies are not currently accepted for payment.
- Ultimate source of funds is not always known, but funds pass through a known/reputable FI.
- Number and value of transactions are monitored and, where necessary, controlled. High volume clients may be subject to enhanced due diligence.
- Client KYC is reviewed in detail prior to acceptance.
- Bank wire slips are reviewed and name matching is performed. Purpose of payment, reference line, and other aspects are stringently reviewed. Documentation supporting purpose of transaction (i.e. an invoice) is required.
- Customers that attempt high-value wires in their first few transactions are subject to increased scrutiny and due diligence.

Risk Mitigation

- There are several points at which client risk is assessed and mitigated accordingly. These are:
    - Client intake and due diligence;
    - Identification of customers;
    - Enhanced due diligence for high-risk clients; and
    - Ongoing client monitoring.
        - Customer transaction monitoring and risk assessment.

- Many of the controls outlined below are described to a high level of detail in other documents -- please consult earlier sections of this Policy or the updated policy table for further information.
- It is Nefin's policy to conduct due diligence via the customer intake process on all clients regardless of their risk profile, references, or history with brokers and other 3rd parties that may be known to Nefin
- Full information regarding the client/merchant intake process is contained within the Customer Intake Process; this typically includes:
    - Confirmation of a client's business information/incorporation details.
        - Validation of the entity's current status in state/provincial/federal register.
        - Where client is deemed high risk OR online validation is not readily available, a copy of incorporation document may be requested.

    - Identification of information related to the business' reputation where possible.
    - Assessment of the inherent risk presented by the product/industry.

        - These address fulfillment times, prevailing regulations, product reputation, and other factors.

    - Ownership of the business.
        - Background checks on owners including watch lists, reputation, and business history.
        - This includes using information in the public and private domains as well as conducting checks on watch lists and excluded party lists.

    - Reason for account opening.
    - Review of any websites associated to the business.
    - Validation of the client address as compliant with VISA location guidelines/not being a shell.
    - Review of operational aspects of the business.
    - Review of regulatory risks presented by the client's industry and assessment of how to mitigate same.

- Where a prospective merchant/client is deemed potentially high risk, additional materials/information may be requested/reviewed including:
    - Industry references;
    - Copies of agreements with suppliers;
    - Bank statements/references;
    - Copy of incorporation document;
    - Government-issued identity documents for owners;
    - Share certificates/registers; and
    - Copies of supply agreements.

- All traffic and transactions are monitored by our Compliance team.
- Where concerning trends or suspicious indicators are present, the client, and their customers, may be subject to more stringent review.
- Where transaction amounts are high, enhanced due diligence is conducted.
- STRs, ASTRs, EFTRs or other reports will be filed according to internal process where required.

Residual Risk

- The residual risk is the overall risk remaining after factoring in the adequacy, appropriateness, and applicability of risk mitigation controls related to the risk factors identified.
- Nefin has a low-medium residual risk rating. This is because Nefin has some medium and high-rated risks that are inherent due to some clients coming from medium and high-risk

countries and dealing in medium-high risk industries; however, with mitigating controls, these risks are reduced. Without controls in place, risks will be heightened.

Training

- Nefin has implemented, and maintains, an ongoing AML-CTF training program to ensure all staff are familiar with the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and their obligations under this legislation.
- At minimum, all staff are required to complete this training within the first two weeks of being hired AND team training will be at least once annually.
- Training is administered internally and it consists of dedicated content provided by a third-party vendor, ABC Solutions Inc.
- The program itself consists of modules and an online testing component.
- An 80% or better is required to pass, employees are able to take the test until they pass however if an employee fails to pass within one rewrite their access to systems and normal job duties may be limited.
- Employees are required to digitally confirm they have been provided with, read, and understood all AML training documentation.
- Compliance staff must be appropriately certified and experienced, and maintain their CPE requirements for certification.
- Additional training and awareness materials may be prepared and distributed by the Chief Compliance Officer on an ad hoc basis.
- Compliance staff must be on the FINTRAC mailing list and regularly review all correspondence from FINTRAC.

Independent Review of the Program

- Nefin shall facilitate regular independent reviews of their AML-CTF regime by qualified auditors when required by FINTRAC guidelines.
- This review will take place once every two years and will assess internal control, transaction processing systems, and procedures.
- Where issues/deficiencies are identified Nefin will endeavor to remediate them in a timely fashion.
- A report of any completed audit will be retained for a minimum of 5 years and contain:
    - Description of the review's scope.
    - Review of policies and procedures.
    - Review of current training program.
    - Assessment of intake, record keeping, identity verification and other processes to ensure they are commensurate with FINTRAC guidance.
    - Summary of any deficiencies.

  - General findings.
- The Compliance Officer is responsible for the efficacy of the compliance program and will report on the external review to management within 30 days of completion.
- The first of these reviews is due by April 6th, 2026.
- Nefin complies with the reporting requirements delineated by FINTRAC.
- Reports are stored electronically for a minimum of 5 years and can be made available within 30 days of any request by FINTRAC representatives.
- Required reports are completed by the Compliance team and submitted to FINTRAC accordingly.
- Suspicious Transaction Reports (STRs) and Attempted Suspicious Transaction Reports (ASTRs) are filed within 30 days of suspicion arising.
- Terrorist Property Reports are filed immediately upon confirmation that a transaction or transactions is confirmed as related to a known terrorist or terrorist organization.
  - Notices may also be sent to RCMP and/or CSIS as dictated by FINTRAC.
- Where no transaction is confirmed but activity is considered related to terrorist property an STR/ASTR will be filed accordingly.
- Large cash transaction (LCT) reports are not filed as Nefin does not accept cash directly.
- Non-SWIFT Electronic Funds Transfer Reports (NS-EFTR) are to be filed within 5 days of Nefin processing the transaction according to the below:
  - A single, or group of transactions within a 24-hour period, that exceeds $10,000.00 CAD (or equivalent) and is processed to the benefit an entity/person outside Canada on behalf of a person/entity inside Canada.
  - A single, or group of transactions within a 24-hour period, that exceeds $10,000.00 CAD (or equivalent) and is processed to the benefit an entity/person inside Canada on behalf of a person/entity outside Canada.
- Large Virtual Currency Transaction Reports (LVCTR) are not filed as Nefin does not deal with cryptocurrencies.
- All reports filed with FINTRAC are confidential and Nefin staff will refrain from disclosing any details of reports, including whether they have been filed, to customers/clients or any person who does have a reasonable need to be informed.

Record Keeping

- Nefin complies with the record keeping requirements delineated by FINTRAC. The following records will be kept:
  - Reports – a copy of every report sent to FINTRAC.
  - Suspicious Transaction Reports.
  - Terrorist Property Reports.
  - Electronic Funds Transfer Reports.
  - Records of all transactions.

  - Foreign currency exchange transaction tickets.
  - Created or received internal memorandums about MSB/FMSB services.
  - Service agreement records.
- Where documents are collected and stored pursuant to customer intake and transaction monitoring, these are stored per the current Customer Document Retention Policy.
- Reports are stored for a minimum of 5 years after the end of a business relationship.
- Policies and procedures are kept up to date (several factors could trigger the need to update, such as changes in legislation, non-compliance issues, new services or products, or the two-year effectiveness review). Updates are tracked by the Last Updated tag and by Policy Version Number.

Client Intake and Authentication

- Nefin primary clients are business entities domiciled in Canada and other developed countries.
- Nefin offers services to clients in an online/non-face to face fashion.
- The customer intake procedure applies to all clients regardless of application method and is guided by FINTRAC guidelines to identify organizations.
- Where dictated by risk level additional due diligence may apply.
- Organizations are confirmed via the relevant state/provincial/federal registry records, or by requesting a copy of the incorporation documentation from the client.
- Ownership is self-reported by the client.
  - Where a client is designated high risk, share certificates or a shareholder register may be requested.
  - Any individual that owns 25% or more of an organization needs to provide their full name and address at minimum.
    - Clients provide date of birth, identity document details and a Proof of address document.
  - Owners are given the opportunity to self-report if they, or any of their staff, are politically exposed persons.
- Using SumSub entity names and owners are checked against multiple watch lists including the OFAC SDN list.
  - Where a possible match is identified additional information will be requested from the client and enhanced due diligence conducted.
  - Nefin does not knowingly transact with excluded parties.
  - Positive matches will be denied service, all other outcomes result in enhanced due diligence and monitoring.
- Refer to client intake policy for a complete intake process

Mandataries

- A mandatary is a person that has been given the authority to conduct business for another.
- A mandatary may be used to validate information, such as identity information, of customers per FINTRAC guidance.
- In the Nefin business model some clients may be mandantaries.
- Nefin will work with new clients/vendors to provide training and guidance as to what information to collect on each client and how to collect it.
- Information collected by the agent is relayed to Nefin securely and not stored by the client/vendor.
    - Agents may be required to update their storage protocols, security, and privacy practices to be approved as agents.
- Nefin has no active mandantaries at this time.

Politically Exposed Persons

- Nefin takes reasonable measures to independently determine if a client is designated as a:
    - Politically exposed person (PEP)
    - Politically exposed foreign person (PEFP)
    - Relative or close associate of a PEP/PEFP (RCA)
- These measures apply to the following scenarios:
    - Client application/new client intake
    - Business entity application
    - New customer making a high value purchase
    - Any transaction, or group of transactions within a 24-hour period, that exceeds $10,000.00 CAD or equivalent conducted by one client
- Where a transaction/group of transactions is suspected to have been conducted by a PEP/PEFP/RCA the transaction is reviewed with attention to:
    - Is the customer's name a match to the OSFI/OFAC watch lists?
    - Can the customer identity be validated by public records or social media?
    - Does the purchase size make sense?
    - Where is the customer located? Where is the merchant located?
    - What payment instrument was used for the transaction? Is this a high-risk payment instrument?
- If the customer is deemed to be a PEP/PEFP/RCA a record of the transaction will be prepared within 14 calendar days including:
    - Office or position of the customer/client
    - Source of funds (if known)
    - Date PEP/PEFP/RCA status confirmed
    - Source used to confirm client/customer status

    - Name of staff member that completed the review
    - Date the transaction(s) was reviewed
- PEP activity will be reviewed on an ongoing basis to ensure risk is managed accordingly
- All PEP accounts must be approved by Nefin' Compliance Officer.
- All PEP accounts will be rated as High Risk with a full file review every 6 months.
- Currently Nefin has no active PEPs

Transaction Records

- Nefin stores an electronic record of all transactions processed through our systems regardless of type, status, or amount.
- All transaction records are stored for a minimum of 5 years per FINTRAC guidelines, and will be stored for the lifetime of the Nefin business unless a client/customer specifically requests the deletion of their information per the terms governing privacy and consent in their jurisdiction.
- Any questions regarding destruction of records can be directed to info@bojrails.com.

Monitoring

- Nefin utilizes third-party providers such as Sumsub to monitor all transactions in real time.
- Additionally, Nefin reviews transactions weekly to ensure transactions that present a risk of money laundering or terrorist financing based on location or amount are reviewed in full.
- Enhanced due diligence is conducted on clients that transact in high volumes every day via internal reporting and operational procedures.
- High volume/high velocity transfers from customers are reviewed weekly by our compliance team.
- Ongoing monitoring for sanction, PEP, and adverse media is conducted by Sumsub software with daily alert checks conducted by Nefin compliance team.

Next Update

April 6th, 2025.