VIDIA Corporation Inc

Anti-Money Laundering

&

Counter Terrorist Financing

Procedures for Compliance Staff

Implementation Date: December 2024

Version Number: 1.0

Last Updated: December 2024

Next Update: December 2025

Document Classification: Confidential

1 Table of Contents

22 42

2 Compliance Officer

This document provides procedural guidance for Vidia Corporation Inc Compliance Officer and any delegates performing tasks on the Compliance Officer's behalf.

3 Staff

For the purposes of this document, references to staff and employees include any other third-party companies that perform relevant functions including customer interactions, customer identification, and transaction related functions.

4 AML Compliance Program Updates

The Compliance Officer will update the anti-money laundering (AML) and counter terrorist financing (CTF) compliance program:

- Annually in the fourth quarter of every calendar year;
- Where there are changes to Vidia Corporation's business model;
- Where there are changes to Canadian AML or CTF legislation;
- Following AML Compliance Effectiveness Reviews, which are required every two years in order to address any deficiencies identified by the reviewer;
- Following regulatory reviews to address any deficiencies identified by the regulator; and
- In the event of internal process or performance issues that have been identified by Vidia Corporation as requiring remediation.

All program updates will be logged and tracked by the Compliance Officer. Records of program updates will be maintained for a minimum of five years.

The Compliance Officer will communicate relevant changes to staff members in a manner that ensures that all staff are aware of changes and able to perform their roles effectively.

5 AML Compliance Training & Training Plan

Vidia Corporation mandates all employees and contractors participate in, complete, and adhere to its AML and CTF training as a condition of continued employment.

The Compliance Officer will ensure that all staff have received sufficient training to be effective in their roles. Minimum standards for training are set out in the AML & CTF Compliance Policy. In instances where staff are performing specialized roles, or where the Compliance Officer has observed performance issues relating to compliance tasks, additional training will be provided.

The Compliance Officer or a delegate, will maintain a training plan consisting of the following:

- training recipients;
- training topics and materials;
- training methods for delivery; and
- training frequency.

The Compliance Officer or a delegate, will also maintain records of all training sessions conducted, including training sessions outside of new hire and annual employee training for a minimum of five years. The Compliance Officer will also maintain records of all external training sessions attended by the Compliance Officer and/or designates for the purpose of maintaining up to date knowledge of Canadian AML and CTF legislation and best practices.

6 AML Compliance Effectiveness Reviews & Plan

Vidia Corporation must also institute and document a plan that describes the scope of the review, which must include all the elements of our AML and CTF compliance program. The breadth and depth of the review for each element may vary depending on factors such as the complexity of our business, transaction volumes, findings from previous reviews, and current ML/TF risks. This plan should include the rationale that supports the areas of focus, the time period that will be reviewed, the anticipated evaluation methods, and sample sizes.

The Compliance Officer will ensure that an AML Compliance Effectiveness Review is conducted at least every two years, and that subsequent will commence within two years of the start date of the previous review. The resulting report will be signed-off by Senior Management within 30 days of issue.

The minimum standards are defined in the AML & CTF Compliance Policy. At a minimum the following must be completed:

- A review of our AML policy and procedure;
- A review and testing the effectiveness of our risk assessment;
- Interviews with the front desk staff to determine their knowledge of the legislative requirements and company's policies and procedures;
- A review of the criteria and process for identifying and reporting attempted suspicious transactions and suspicious transactions;
- A sampling of virtual currency transactions followed by a review of the reporting of such transactions (if applicable);
- A test of the record keeping system for compliance with the legislation;
- A test of the customer/client identification procedures for compliance with the legislation; and
- Any areas of the business that are known to be high risk and require enhanced monitoring.

In addition to ensuring that these standards are met, the Compliance Officer will ensure that all reviewers are sufficiently qualified by requesting a copy of the curriculum vitae (CV) for all reviewers prior to selecting a third-party reviewer.

At minimum, each reviewer must:

- Demonstrate sufficient understanding of the Canadian regulatory context;
- Have sufficient experience in conducting AML Compliance Effectiveness Reviews in Canada; and
- Have maintained up to date training and professional qualifications; including, but not limited to, the Certified Anti-Money Laundering Specialist designation.

Records maintained by the Compliance Officer will include:

- A copy of the final report;
- A record of senior management sign-off on the final report;
- A copy of the agreement between Vidia Corporation and the reviewer;
- Copies of the CVs for all reviewers to ensure that each reviewer is sufficiently qualified to perform the review; and
- A record of any updates made to Vidia Corporation's compliance program to address deficiencies identified by the reviewer.

All records relating to AML Compliance Effectiveness Reviews are maintained for a minimum of five years.

7 FINTRAC Registration & Communication

The Compliance Officer will maintain Vidia Corporation's registration with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) by:

- Ensuring that the renewal of the registration is completed in the time and manner specified by FINTRAC (generally every two years);
- Updating relevant information, including business activity information and key employee information within 30 days following any changes to Vidia Corporation's business activities or key personnel;
- Responding to any FINTRAC requests for clarification regarding the MSB registration within the required timeframes (generally 30 business days); and
- Cancelling the MSB registration with FINTRAC if Vidia Corporation ceases to offer MSB services in Canada. This must occur within 30 days after the date Vidia Corporation stops offering MSB services.

Updates and renewals of Vidia Corporation's FINTRAC registration are completed using the online money services business (MSB) registry portal[1]. The Compliance Officer will maintain records of all updates and renewals for five years.

Additional communication with FINTRAC may include examinations, compliance assessment reports, and other information requests. In all cases, the Compliance Officer, or a designate, will act as the liaison with FINTRAC. Records of all FINTRAC communication, including Vidia Corporation's responses, will be maintained for a minimum of five years.

[1] https://www9.fintrac-canafe.gc.ca/msb-esm/secure/registration/registration/

The Compliance Officer will ensure that records that may be required by FINTRAC are stored in a manner that they can be retrieved, and communicated to, the regulator in a timely manner. Generally, Vidia Corporation will have 30 calendar days from the date that a request is sent by FINTRAC to assemble and submit information. Where Vidia Corporation receives a confirmation from FINTRAC that information has been received, this confirmation will be maintained as part of Vidia Corporation's records of correspondence with FINTRAC.

The Compliance Officer receives regular email updates from FINTRAC, including news releases. Calendar entries are used to track regulatory tasks including updates and renewals.

8 Ministerial Directives

Under Part 1.1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), which came into force on June 19, 2014, the Minister of Finance may:

- Issue directives that require reporting entities to apply countermeasures to transactions coming from or going to designated foreign jurisdictions or entities; and
- Recommend the introduction of regulations to restrict reporting entities from entering into a financial transaction coming from or going to designated foreign jurisdictions or entities.

These authorities allow the Minister of Finance to take steps to protect Canada's financial system from foreign jurisdictions and foreign entities that are considered to present high risks for facilitating money laundering and terrorist financing.

The Compliance Officer will maintain an awareness of such directives by regularly reviewing FINTRAC's website[2] and subscribing to FINTRAC's mailing list[3].

8.1 Ministerial Directive on the Democratic People's Republic of Korea (DPRK), Also Known as North Korea

This Ministerial Directive requires that all transactions to and from North Korea be treated as high risk, regardless of the amounts of the transactions. In addition, FINTRAC's expectation is that Vidia Corporation implements specific measures to mitigate the risk posed by these transactions and document the measures taken.

When conducting these transactions, regardless of the transaction amounts, the measures that are taken to mitigate the risk may include:

[2] http://www.fintrac.gc.ca/obligations/directives-eng.asp
[3] http://www.fintrac.gc.ca/contact-contactez/list-liste-eng.asp

- Keeping a record of all transactions to and from North Korea, regardless of the amount.
    - This record must include details such as the customer's name and address, the amount, currency, date and type of transaction.
    - If the customer is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the customer is an entity, the nature of their principal business.
    - If the transaction is an electronic funds transfer, recording the ordering customer and the beneficiary, as well as their addresses, the amount, currency and date of transaction.
    - If the ordering customer is a person, their date of birth and the nature of their principal business or their occupation, as applicable; and if the ordering customer is an entity, the nature of their principal business.
- These details must specify whether funds are coming from, or destined to North Korea;
- Ensuring that the information about the identity of these customers is up to date;
- Exercising customer due diligence, including asking for the:
    - Source of the funds;
    - Purpose of transactions; and
    - Beneficial ownership (if the client is an entity);
- Conducting enhanced ongoing monitoring of the customer and/or the business relationship and/or the account involved in the transaction;
- Keeping records related to all of the above actions; and
- Reporting suspicious transactions (if applicable).

In the case that we suspect, but do not know that a transaction is related to North Korea, the transaction will be treated as high risk. In its Operational Brief[4] on the subject, FINTRAC provides several relevant indicators:

- **Transactions Involving Front or Shell Companies**: North Korean entities and individuals have made use of front and shell companies in various jurisdictions to mask their involvement in the international financial system. Such companies may have the following characteristics:
    - The lack of their own online presence, such as a company website indicating normal business-related information such as products and services, contact information, and physical geographic location.
    - A corporate name which is overly generic, non-descriptive, or easily mistaken with that of another better-known corporate entity. Additionally, the corporate name may be regularly misspelled in different ways.
    - A pattern of sending or receiving international EFTs to or from Canadian businesses that operate in sectors or industries unrelated to each other.

[4] http://www.fintrac.gc.ca/intel/sintel-eng.asp

    - Transactional patterns which are exclusively one-directional; e.g., the company only sends but never receives EFTs, or vice versa.
    - Transactional patterns in which the same observed activity (e.g., sending EFTs) and the Canadian recipients remain consistent, but the foreign ordering company changes over time, particularly if the sending companies are from the same jurisdiction or geographic area.
- **Transactions Involving Particular Jurisdictions**: North Korean entities and individuals have been observed using particular jurisdictions from which to access the international financial system. While the jurisdictions discussed below are not an exhaustive list, transactions to or from these areas, in combination with other indicators, should be considered when deciding to report a suspicious transaction report to FINTRAC:
    - Liaoning Province, China shares a land border with North Korea, and both companies and financial institutions in this jurisdiction have been reported to engage in financial activity and other business dealings with North Korean companies and China-based front companies (see Appendix I for a list of cities in Liaoning province). FINTRAC also notes that there is a substantial amount of Canada-linked EFT reporting to a number of these cities, in particular Dalian, China and Shenyang, China.
    - Jilin Province, China also shares a land border with North Korea, and has been associated with companies employing North Korean guest workers in the food processing and manufacturing sectors. FINTRAC notes that there is also a substantial amount of EFT reporting to Changchun, the capital of Jilin province (See Appendix I for a list of cities in Jilin province).
    - Hong Kong has also been associated with North Korean financial activity. While this is not unexpected given Hong Kong's role as a major centre of global finance, transactions to or from Hong Kong that display other indicators, particularly those indicating possible use of shell companies, may warrant additional scrutiny.

While we do not conduct transactions with North Korea, or any touchpoints connecting a transaction to North Korea, where the facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to North Korea, an STR will be submitted to FINTRAC, and the reasons will be noted in the freeform section of the report.

8.2 Ministerial Directive on the Islamic Republic of Iran

This Ministerial Directive requires that all transactions to and from Iran be treated as high risk, regardless of the amounts of the transactions. In addition, FINTRAC's expectation is that Vidia Corporation implements specific measures to mitigate the risk posed by these transactions and document the measures taken.

When conducting these transactions, regardless of the transaction amounts, the measures that are taken to mitigate the risk may include:

- Treat every financial transaction originating from or bound for Iran, regardless of its amount, as a high-risk transaction;
- Verify the identity of any customer (person or entity) requesting or benefiting from such a transaction;
- Exercise customer due diligence, including ascertaining the source of funds in any such transaction, the purpose of the transaction and, where appropriate, the beneficial ownership or control of any entity requesting or benefiting from the transaction;
- Keep and retain a record of any such transaction;
- Determine whether there are reasonable grounds to suspect the commission or attempted commission of a money laundering or terrorist financing offence and report all suspicious transactions to FINTRAC;
- Reporting all other reportable transactions[5] (if applicable).

In the case that we suspect, but do not know that a transaction is related to Iran, the transaction will be treated as high risk. In its Guidance[6] on the subject, FINTRAC provides several relevant indicators:

- Payment for products by electronic funds transfers (EFTs) that include an Iranian originating or destination address;
- Receiving Iranian rial as part of a transaction; or
- Accepting bank drafts or other negotiable instruments that include an Iranian rial component.

To be clear, this MD does not apply to transactions where there is no suspicion or explicit connection with Iran and there is no evidence of the transaction originating from or being bound for Iran. A couple of examples were provided in the FINTRAC Guidance:

- A client who has previously sent funds to Iran requests an outgoing EFT, where the transaction details do not suggest that this transaction is bound for Iran and you are unable to obtain further details about the transaction destination; or
- The client's identification information is the only suggestion of a connection to Iran (for example, a transaction where the conductor's identification document is an Iranian passport).

While we do not conduct transactions with Iran or any touchpoints connecting a transaction to Iran, where the facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to Iran, an investigation will be conducted and if there is a connection, an STR will be submitted to FINTRAC using the related Ministerial Directive code IR2020 leaving Parts G and H blank. If during the investigation the Compliance Officer determines that there are reasonable

[5] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng
[6] https://www.fintrac-canafe.gc.ca/obligations/dir-iri-eng

grounds to suspect the transactions are related to money laundering or terrorist financing, then we will submit a second STR with the reasons as to why, noted in the freeform section (Part G) of the report.

8.3 Ministerial Directive Associated with Russia

This Ministerial Directive requires that all transactions to and from Russia be treated as high-risk. In addition, FINTRAC's expectation is that Vidia Corporation implements specific measures to mitigate the risk posed by these transactions, and documents the measures taken.

When conducting these transactions, regardless of the transaction amounts, the measures that are taken to mitigate the risk may include:

- Treat every financial transaction originating from or bound for Russia regardless of its amount, as a high-risk transaction;
- Verify the identity of any customer (person or entity) requesting or benefiting from such a transaction;
- Exercise customer due diligence, including ascertaining the source of funds in any such transaction, the purpose of the transaction and, where appropriate, the beneficial ownership or control of any entity requesting or benefiting from the transaction;
- Keep and retain a record of any such transaction;
- Determine whether there are reasonable grounds to suspect the commission or attempted commission of a money laundering or terrorist financing offence and report all suspicious transactions to FINTRAC; and
- Reporting all other reportable transactions[7] (if applicable).

In the case that we suspect, but do not know that a transaction is related to Russia, the transaction will be treated as high-risk. In its Guidance[8] on the subject, FINTRAC provides several relevant indicators:

- Electronic funds transfers, remittances or other transfers that include a Russian originating or destination address - this may include transactions where the ordering person or entity, beneficiary, or third-party details are Russian;
- The activities of representatives of the Government of Russia (for example, transactions on an Embassy of Russia's bank account in Canada);
- Receiving Russian ruble as a deposit to an account or for a virtual currency transaction;
- Conducting a foreign currency or virtual currency exchange transaction that includes Russian ruble; and

[7] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/1-eng

[8] https://fintrac-canafe.canada.ca/obligations/dir-rus-eng

- Accepting bank drafts or other negotiable instruments that include a Russian ruble component.

To be clear, this MD does not apply to transactions where there is no suspicion or explicit connection with Russia and there is no evidence of the transaction originating from or being bound for Russia. A couple of examples were provided in the FINTRAC Guidance:

- A customer who has previously sent funds to Russia requests an outgoing EFT, where the transaction details do not suggest that this transaction is bound for Russia, and you are unable to obtain further details about the transaction destination;
- The customer's identification information is the only suggestion of a connection to Russia (for example, a transaction where the conductor's identification document is a Russian passport); or
- The details of customer are Russian, but there are no additional details on the entity involved, or the sender of, or the recipient to, the transaction, to suggest the transaction is associated with Russia.

For further clarity, if the details of our customer in Canada include a Russian address and the customer requests that funds be sent to a beneficiary in a country other than Russia, where additional facts, context and indicators (for example, beneficiary account details) point to an association with Russia, then this transaction must be considered as bound for Russia, and treated accordingly.

As a practice, we do not conduct transactions with Russia. Where facts, context, and indicators lead the Compliance Officer to believe that a transaction may be related to Russia, an investigation will be conducted to make a determination (i.e. research the origin of funds to determine if the details about the sender, beneficiary or entities involved in a transaction, indicate that the transaction is originating from for Russia). An assessment will also be conducted to determine whether there are reasonable grounds to suspect the commission or attempted commission of a money laundering or terrorist activity financing offense. An ASTR or STR will be submitted to FINTRAC with the reasons noted in the freeform section of the report where reasonable grounds has been met.

9 Reporting

Certain types of transactions must be reported to FINTRAC. Reporting to FINTRAC should always be completed by the Compliance Officer, or a designate, which is a person that has been trained to submit reports in the Compliance Officer's absence. All other employees should use the internal forms included in this program to submit reports to the Compliance Officer. All reports have specific timelines in which they must be submitted to FINTRAC. All internal reports should be submitted to the Compliance Officer on the same day that the incident or transaction takes place.

Reportable transactions are detected by:

- Vidia Corporation's electronic platforms; and/or
- Vidia Corporation employees.

Reports submitted by staff members are reviewed as soon as possible. Where there are issues with the reports, such as missing or incomplete information, the Compliance Officer will conduct follow up coaching sessions. The Compliance Officer will also work with the staff member to contact the customer (where possible) in order to obtain any missing or incomplete information.

Reports are submitted to FINTRAC electronically using FINTRAC's Web Reporting System, where possible. In all reports with optional fields, these fields should be considered to be mandatory if Vidia Corporation has the information on file. Failure to include the information in a report will be considered a deficiency during an effectiveness review or a regulatory examination. This includes the following information related to transactions conducted through our platform:

- every reference number that is connected to the transaction;
- type of device used by person who makes a request online;
- number that identifies device;
- internet protocol address (IP address) used by device;
- person's or entity's username; and
- date and time of person's online session in which request is made.

9.1 Electronic Funds Transfers

Reportable electronic funds transfers (EFTs) include the transmission of funds or instructions sent out of (outgoing) or into (incoming) Canada for transactions valued at CAD 10,000 or more. These may be either a single transaction or multiple transactions within the same 24-hour period. The static 24-hour period we have chosen for calculating this is between 12:00am – 11:59pm ET. The report type is an Electronic Funds Transfer Report (EFTR) and must be reported where we know the transactions multiple transactions within a static 24-hour window, that total CAD 10,000 or more:

- were initiated by the same person or entity;
- were initiated on behalf of the same person or entity (third-party); or
- are for the same beneficiary (person or entity); or

Where we receive two or more international EFTs that total CAD 10,000 or more within a static 24-hour window, and we know that the transactions:

- were initiated by the same person or entity; or
- are for the same beneficiary (person or entity).

There are exceptions to the 24-hour rule for EFTs that applies if we send or receive a bundled EFT, that is an EFT with more than one beneficiary. The 24-hour rule will not apply for any of the amounts under CAD 10,000 included in a bundled EFT if it

was sent at the request of a public body, a very large corporation, or the administrator of a federally or provincially regulated pension fund.

In this context, a public body means any of the following or their agent:

- A Canadian provincial or federal department or Crown agency;
- An incorporated Canadian municipal body (including an incorporated city, town, village, metropolitan authority, district, county, etc.); or
- A hospital authority. A hospital authority means an organization that operates a public hospital and that is designated to be a hospital authority for GST/HST purposes. For more information on the designation of hospital authorities, refer to GST/HST Memoranda Series, Chapter 25.2, Designation of Hospital Authorities.

Also in this context, a very large corporation is one that has minimum net assets of $75 million on its last audited balance sheet. The corporation's shares have to be traded on a Canadian stock exchange or on a stock exchange outside Canada that is designated by the Minister of Finance. The corporation also has to operate in a country that is a member of the Financial Action Task Force (FATF).

Vidia Corporation uses the last rate provided by the Bank of Canada available at the time of the transaction to determine if the CAD 10,000 or more threshold is met for the transaction to be reportable as an EFT transaction.

If there is no Bank of Canada rate published for the currency of the transaction, Vidia Corporation uses the actual exchange rate applied when the transaction is processed for determination of whether it is reportable.

The reporting obligation falls to Vidia Corporation because we maintain the relationship with the customer. Reportable EFTs must be submitted to FINTRAC within 5 working days from the date on which the transaction(s) took place.

Where there is an EFT valued at CAD 100,000 or more, the Compliance Officer or a designate will ensure that a politically exposed person (PEP) or head of an international organization (HIO) determination has been conducted. Where possible, the source of funds will also be requested and documented. This is discussed in greater detail under the PEP and HIO Check section.

These transactions are detected via system parameters related to transaction amounts. The Compliance Officer will consider whether any additional reporting (STR) is required when filing an EFTR.

The Compliance Officer will maintain records of:

- All EFTRs filed with FINTRAC;
- All reconciliations conducted to determine whether or not transactions are reportable by Vidia Corporation; and

- Records of Politically Exposed Person (PEP) determinations and related information for EFTs valued at CAD 100,000 or more.

All records relating to EFTRs will be maintained for a minimum of five years.

9.1.1 Travel Rule (EFT)

The travel rule is the requirement to ensure that specific information is included with the information sent or received in an electronic funds transfer (EFT), including international EFTs. To meet the travel rule, Vidia Corporation must always include the following information when sending or receiving an international EFT:

- the name, address and account number or other reference number (if any) of the person or entity who requested the transfer (originator information);
- the name and address of the beneficiary; and
- if applicable, the beneficiary's account number or other reference number.

Where such information is not present, we will take reasonable measures to obtain the required information, which is done by requesting it from the issuing financial institution. Where we are unable to obtain the information, we will reject the transaction.

9.2 Large Virtual Currency Transactions

Large Virtual Currency Transaction Reports have to be submitted to FINTRAC when we receive virtual currency from a customer in an amount equivalent to CAD 10,000 or more in a single transaction, or multiple transactions in the same 24-hour period that total CAD 10,000 or more. We use the exchange rates published by our liquidity partners as our sources for determining the exchange rate for the virtual currency being transacted.

The Compliance Officer will emphasize with all staff that third party determinations must be conducted in the case of large virtual currency transactions. This involves asking the customer whether they are completing the transaction on their own behalf, or on behalf of another person or organization. If the transaction is being conducted on someone else's behalf, staff members will collect additional information about the person or organization on whose behalf the transaction is being conducted and their relationship to the person conducting the transaction.

If the person completing the transaction states that there is no third party, but they appear to be taking directions from another person, staff are encouraged to report to the Compliance Officer. A suspicious transaction report may also be considered in these cases.

These transactions are detected automatically within our IT system, and reviewed by the Compliance Officer or designate. At the time of review, the Compliance Officer will consider whether any additional reporting (i.e., EFTR, STR) is required.

The Compliance Officer will maintain records of:

- All Large Virtual Currency Transactions Reports filed with FINTRAC;
- All third party determinations for such transactions;
- All PEP determinations (where the transaction triggers business relationship requirements) and
- Any suspicion of third party involvement where the customer has stated that there is no third party involvement.

Large Virtual Currency Transaction Reports must be submitted to FINTRAC within 5 working days after the day on which the person or entity transfers or receives the amount.

All records relating to Large Virtual Currency Transaction Reports will be maintained for a minimum of five years.

9.2.1 Third Party Determinations (Virtual Currency)

A third-party determination must be completed any time a LVCTR is required. This means that we ask the customer if the transaction is being conducted on behalf of any other individual or organization.

If so, we must collect and record information about the individual or organization on behalf of which the transaction is being conducted. This includes:

- The third party's name, address, and occupation or nature of principal business;
- Their date of birth, if the third party is a person;
- The incorporation number and its jurisdiction of issue, if the third party is a corporation; and
- The nature of the relationship between the individual and the third party.

We must keep records in relation to third party determination for at least five years following the date they were created. If there is no third party, we must still record in the system that a third party determination was completed.

9.2.2 Travel Rule (Virtual Currency)

The travel rule refers to specific information that should be included with the information sent or received for certain transactions. The travel rule information for virtual currency transfers includes the following:

- the name, address and, if any, the account number or other reference number of the person or entity who requested the transfer; and
- the name, address and, if any, the account number or other reference number of the beneficiary.

In the absence of mature global technology solutions, we will accept all transactions based on the information provided by the. Where there are additional red flags compliance will investigate and take appropriate action, which may include returning (rejecting) the transaction, or suspending the transaction until additional

information and/or documentation has been received. The Compliance Officer will monitor for service providers that are working to provide a solution.

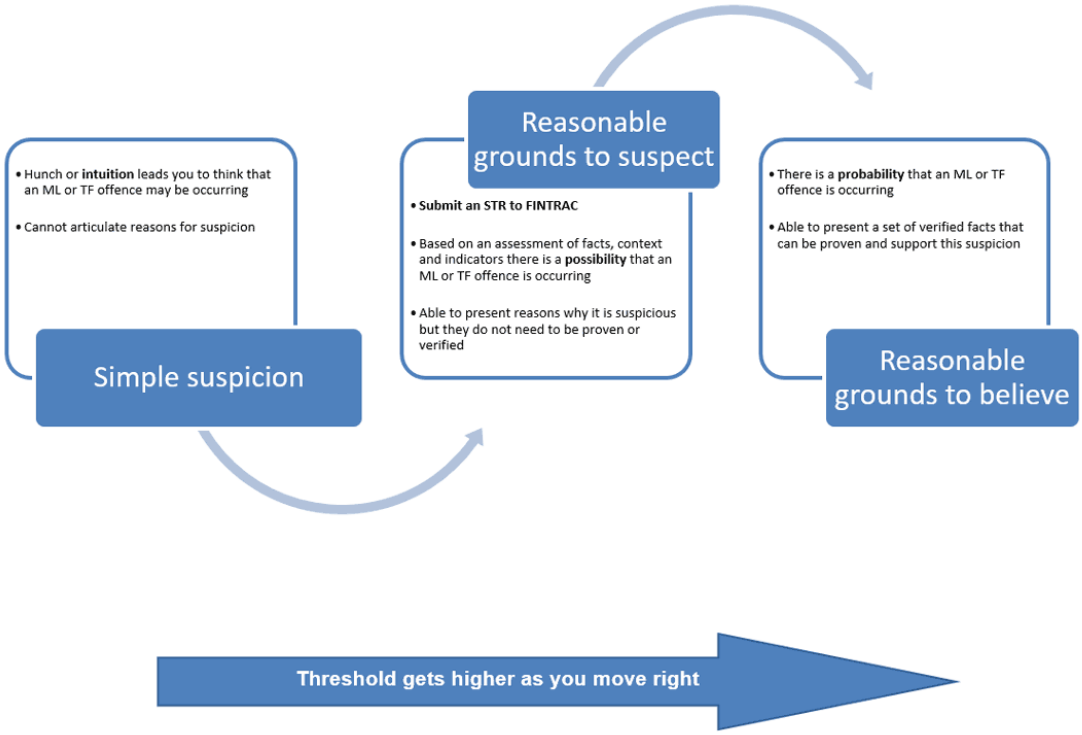
9.3 Suspicious Transactions & Attempted Suspicious Transactions

Suspicious Transaction Reports (STRs) and Attempted Suspicious Transaction Reports (ASTRs) are submitted to FINTRAC where there are 'reasonable grounds' to suspect that an activity is related to money laundering or terrorist financing. These reports must be submitted whether or not the transaction or activity is completed. ASTRs are used for transactions that are not completed (whether the transaction is declined by Vidia Corporation or cancelled by the customer). These reports must be submitted to FINTRAC as soon as practicable after completing the measures required to determine that reasonable grounds to suspect it may be related to a money laundering or terrorist financing offense.

As soon as practicable is a time period that falls in-between immediately and as soon as possible within which a suspicious transaction report (STR) be submitted to FINTRAC. In this context, the report must be completed promptly, taking into account the facts and circumstances of the situation. While some amount of delay is permitted, it must have a reasonable explanation. The completion and submission of the report should take priority over other tasks.

9.3.1 Reasonable Grounds to Suspect

Understanding the differences between the thresholds can help clarify what reasonable grounds to suspect means and how it can be operationalized within your compliance program. See the diagram below for an overview of the different thresholds.



Simple suspicion is a lower threshold than reasonable grounds to suspect and is synonymous with a "gut feeling" or "hunch". In other words, simple suspicion means that we have a feeling that something is unusual or suspicious, but do not have any facts, context or indicators to support that feeling or to reasonably conclude that an ML/TF offence has occurred. Simple suspicion could prompt us to assess related transactions to see if there is any additional information that would support or confirm your suspicion.

Reasonable grounds to suspect is the required threshold to submit an STR to FINTRAC and is a step above simple suspicion, meaning that there is a possibility that an ML/TF offence has occurred. We do not have to verify the facts, context or ML/TF indicators that led to our suspicion, nor do we have to prove that an ML/TF offence has occurred in order to reach reasonable grounds to suspect. Our suspicion must be reasonable and therefore, not biased or prejudiced.

Reaching reasonable grounds to suspect means that we consider the facts, context and ML/TF indicators related to a financial transaction and, after having reviewed this information, we conclude that there are reasonable grounds to suspect that this particular financial transaction is related to ML/TF. We must be able to demonstrate and articulate our suspicion of ML/TF in such a way that another individual reviewing the same material with similar knowledge, experience, or training would likely reach the same conclusion.

The explanation of our assessment should be included in the narrative portion, Part G, of the STR. Many factors will support our assessment and conclusion that an ML/TF offence has possibly occurred; they should be included in our report to FINTRAC.

Reasonable grounds to believe is a higher threshold than reasonable grounds to suspect and is beyond what is required to submit an STR. Reasonable grounds to believe means that there are verified facts that support the probability that an ML/TF offence has occurred. In other words, there is enough evidence to support a reasonable and trained person to believe, not just suspect, that ML/TF has occurred. For example, law enforcement must reach reasonable grounds to believe that criminal activity has occurred before they can obtain judicial authorizations, such as a production order.

If we are in receipt of a production order, by law enforcement, we must perform an assessment of the facts, context, and ML/TF indicators to determine whether we have reasonable grounds to suspect that a particular transaction is related to the commission of ML/TF.

9.3.2 Measures for Establishing Reasonable Grounds to Suspect

In order to submit an STR to FINTRAC, we will need to ensure that we have completed the measures that enable us to reach the reasonable grounds to suspect threshold, meaning that there is a possibility that an ML/TF offence has occurred.

These measures include:

- screening for and identifying suspicious transactions via our IT system;
- assessing the facts and context surrounding the suspicious transaction;
- linking ML/TF indicators to our assessment of the facts and context; and
- explaining our grounds for suspicion in an STR, where we articulate how the facts, context and ML/TF indicators allowed us to reach our grounds for suspicion.

A fact, for the purpose of completing an STR, is defined as an event, action, occurrence or element that exists or is known to have happened or existed — it cannot be an opinion. Facts known to Vidia Corporation could also include account details, particular business lines, the client's financial history or information about the individual or entity (for example, that the individual has been convicted of a designated offence or is the subject of a production order, or that an entity is being investigated for fraud or any other indictable offence).

Context, for the purpose of completing an STR, is defined as information that clarifies the circumstances or explains a situation or transaction. This type of information is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario.

Indicators are potential red flags that can initiate suspicion and indicate that something may be unusual without a reasonable explanation. Red flags typically stem

from one or more facts, behaviours, patterns or other factors that identify irregularities related to a client's transactions. These transactions often present inconsistencies with what is expected or considered normal based on the facts and context you know about your client's transactional activities.

9.3.3 Internal Timelines for Completing Investigations Related to Potential STRs/ASTRs

FINTRAC expects that we are prioritizing our highest risk investigations and transaction reviews, and that we are not giving unreasonable priority to other transaction monitoring or compliance-related tasks. In an examination FINTRAC may question delayed reports. In order to ensure we are submitting STRs and ASTRs "as soon as practicable," we have set out guidelines that establish what is practicable for our business.

The following parameters are used as guidance for determining what is a reasonable timeframe for prioritizing and completing investigations, and related STR/ASTR submissions. These are based on factors including the complexity, size, risk level, and other factors present when establishing reasonable grounds to suspect (RGS) a money laundering or terrorist financing related offence[9].

- High Priority (investigated and submitted within 1-2 business days):
    - STR accompanying a terrorist property report (TPR)[10];
    - Terrorism or other national security related concern;
    - Sanctions evasion; or
    - Other time sensitive situations, such as child sexual abuse material (CSAM), and human trafficking or smuggling.

For the resolution of investigations and reports that are not deemed to be high priority, efficient resolution is, nonetheless expected:

- Small/Simple (investigated and submitted within 1-5 business days)
    - Involves 1 or 2 customers;
    - Involves 3 transactions or less; and/or
    - Clear facts, context, and indicators are present.
- Moderate (investigated and submitted within 5-15 business days)
    - Involves 3-5 customers;
    - Involves 5-10 transactions; and/or

[9] RGS does not require knowledge of a specific predicate offence, nor confirmation that any crime has occurred. The facts, context, and indicators need only be sufficient to establish reasonable grounds for suspicion. These are documented as part of the investigation process and included in the narrative section of the STR/ASTR.

[10] TPRs and other report types are required, where applicable, whether or not a STR/ASTR has been filed. In all cases where a TPR is filed, a corresponding STR must also be filed.

    - More complex facts, context and indicators.
- Large/Complex (investigated and submitted within 15-30 business days)
    - Involves more than 5 customers;
        - Involves more than 10 transactions; and/or
- The facts, context and indicators and are very complex.
- Exception (situations where there is not enough information to establish a determination of RGS)
    - Customers that transact infrequently (e.g., once a quarter), where additional insight into the customer's patterns is needed to make a determination;
    - Situations where the customer has not responded to requests for clarification or additional information;
    - Situations where enhanced due diligence is being conducted;
    - Situations where the Compliance Officer believes that additional information can be collected from the customer that would allow for a determination that there is not RGS.

In all instances, detailed notes related to ongoing investigations, related requests for clarification from the customer or other sources, and other measures, are maintained. These records include the timing of relevant events.

9.3.4 Submitting STRs & ASTRs to FINTRAC

When the Compliance Officer has decided that reasonable grounds to suspect have been established, an STR or ASTR must be submitted to FINTRAC as soon as practicable. Vidia Corporation has translated this to mean without delay. The STR or ASTR to be submitted will include the following information (if available):

- Who are the parties to the transaction?
    - List the conductor, beneficiary and holders of all accounts involved in the transaction.
    - Take reasonable measures to identify the conductor of the transaction. This means that you are expected to ask the client for this information unless you think doing so will tip them off to your suspicion.
    - Provide identifying information on the parties involved in the transaction. This could include the information you recorded to identify the conductor, as well as any information you have on the other parties to the transaction or its recipients.
    - List owners, directors, officers and those with signing authority, when possible. If the transaction involves a business, you could include information on the ownership, control and structure of the business in the STR.
    - Provide clear information about each individual or entity's role in each of the financial transactions described. It is important to know who is sending and receiving the funds and this may be relevant in Part G of the STR.

    - Explain the relationships among the individuals or entities (if known). This is very helpful to FINTRAC when trying to establish networks of individuals or entities suspected of being involved in the commission or attempted commission of a money laundering (ML) or terrorist financing (TF) offence.
- When was the transaction(s) completed/attempted? If it was not completed, why not?
    - Provide the facts, context and ML or TF indicators regarding the transaction.
- What are the financial instruments or mechanisms used to conduct the transaction?
- Where did this transaction take place?
- Why the transaction(s) or attempted transaction(s) are related to the commission or attempted commission of an ML or TF offence?
    - State the ML or TF indicators used to support your suspicion.
    - State the suspected criminal offence related to ML or TF, if known.
- How did the transaction take place?

Suspicious or attempted suspicious transactions do not have a minimum dollar threshold and may relate to any of Vidia Corporation's business activities. Reports are not limited to the business activities that define Vidia Corporation as a regulated entity in Canada.

For example, if a prospective customer calls and asks whether or not Vidia Corporation would be willing to send virtual currency to another country without them going through the identification requirements associated with the platform, this should be reported as an attempted suspicious transaction.

Employees are to report this type of transaction using the Unusual Transaction Form (Internal), which is submitted to the Compliance Officer on the same day that the transaction takes place.

The Compliance Officer will emphasize the following to all staff:

- It is important not to let the customer know that they are suspicious. It is against the law to deliberately "tip off" a customer about a potential investigation. Vidia Corporation and all staff are, however, protected under Canadian law from any action when we submit a report "in good faith." In most cases, even when a case goes to court, the customer will not know that this report has been filed.
- It is important to try to identify customers that conduct or attempt suspicious transactions. The customer may ask why we need their identification information. In such cases, let the customer know that it is company policy to collect this information. If this information is not used for additional marketing activities, let the customer know that as well (often customers are more concerned about privacy and security issues, and reassuring them may be helpful).

All transactions are reviewed manually in real time. The use of blockchain analytics tools are leveraged for the review of transactions. At the time of review, the Compliance Officer will consider whether any additional reporting (i.e., LVCTR) is required.

The Compliance Officer will maintain records of:

- All STRs and ASTRs filed with FINTRAC;
- All internal unusual transaction reports, including reports filed for transactions that were not reported to FINTRAC;
- All technology-based transaction monitoring alerts related to unusual transactions;
- A record of the reason that transactions escalated (via staff or via a transaction monitoring system) were not reported to FINTRAC, including the analysis that was conducted and the basis for each decision; and
- Records of any follow-up activity, including but not limited to updates to customer risk scores, additional transaction monitoring and the closing of customer accounts.

These records are currently maintained in electronic format and include the original transaction information and Compliance Officer decisions related to reporting.

Where an STR or ASTR is reported, the customer's risk rating will be manually changed to high risk. Where a customer is not considered high risk subsequent to the filing of an STR or ASTR, the rationale must be documented.

All records relating to STRs and ASTRs will be maintained for a minimum of five years.

9.4 Terrorist Property

Terrorist Property Reports (TPRs) are completed if Vidia Corporation is in possession of funds or property that belong to a terrorist (either an individual or an organization). Generally, Vidia Corporation would become aware of terrorist property via list screening that is conducted. This process involves matching our customer information against publicly a list published by the United Nations Security Council (UNSC)[11], which is a consolidated list of known terrorists and sanctioned individuals and organizations. This process is described under list screening.

It is also possible for staff to become aware through conversations with our customers that illegal activity may be taking place. In these cases, staff are instructed to escalate these reports to the Compliance Officer immediately. The Compliance Officer conducts an investigation to determine whether or not reports or the freezing of property is required. Staff use the Unusual Transaction Report (Internal) for this purpose.

[11] https://www.un.org/securitycouncil/content/un-sc-consolidated-list

TPRs are submitted immediately to FINTRAC as well as to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS)[12]. All TPRs are submitted via fax and copies of the faxed confirmations are maintained. TPRs are submitted to:

- FINTRAC, fax: 866-226-2346
- RCMP, Attn: Anti-Terrorist Financing Team, RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca
- CSIS Financing Unit, complete the form on this page: https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

The Compliance Officer will maintain records of:

- All TPRs filed;
- Fax confirmations for all TPRs sent to FINTRAC, CSIS and/or RCMP;
- All internal unusual transaction reports related to TPRs, including reports filed for transactions that were not reported;
- A record of the reason that transactions escalated (via staff or via a transaction monitoring system) were not reported, including the analysis that was conducted and the basis for each decision; and
- Records of any follow-up activity, including but not limited to updates to customer risk scores, additional transaction monitoring and the closing of customer accounts.

In the case that terrorist property is suspected, but the customer does not match any lists, an ASTR or STR will be submitted to FINTRAC.

If a transaction was attempted or completed, and it involved property that we know is owned or controlled by or on behalf of a terrorist group, or that we believe is owned or controlled by or on behalf of a listed person (for which we must submit a TPR), we should also submit an STR to FINTRAC. This is because Vidia Corporation has reached the threshold of reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence.

All records relating to TPRs will be maintained for a minimum of five years.

9.5 Multiple Reports

More than one report may be required for a single transaction. The Compliance Officer will ensure that all applicable report types are filed.

[12] Under subsection 83.1(1) of the Criminal Code, we must disclose without delay to the RCMP or CSIS the existence of property in our possession or control. Vidia Corporation has elected to submit TPRs to both law enforcement agencies.

For example: If a customer conducts a virtual currency transaction in which Vidia Corporation received CAD 12,000 of virtual currency as payment for an international remittance transaction, and the transaction is considered to be suspicious (for instance, if the customer provides identification documentation that appears false) then multiple reports may be required, including the following:

- EFTR,
- LVCTR, and
- STR/ASTR.

All reports must be completed in full and filed on time. The completion of one report does not negate or change the requirement to complete any other report type.

10 Responding to Law Enforcement Requests

There may be exceptional times when Vidia Corporation is required to disclose personal information, without an individual's consent, in order to comply with a subpoena, warrant, court order or other law enforcement request. Similarly, Vidia Corporation may disclose personal information without consent to a government institution or an investigative body for a purpose such as national security, national defence or the deterrence of terrorism, law enforcement, or in relation to a suspected money-laundering offence.[13]

If Vidia Corporation receives a request from law enforcement the Compliance Officer must be notified immediately. The Compliance Officer will comply with such request where the below criterial is met[14].

A request has to be in writing: In order to understand the request, the Compliance Officer will request a subpoena, Court Order or other evidence, if it has not been provided. This documentation protects the company and Compliance Officer in the request for information and the release of information under Canadian privacy law.

The person requesting information should be identified and the date of the request should be recorded. The request should be analyzed and clarification should be sought from the law enforcement officer if necessary before any information is disclosed. Exemptions under PIPEDA should also be analyzed by the Privacy Officer if applicable to the request.[15]

Once the supporting evidence of received and information request is understood, Vidia Corporation will comply with the information request in a format reasonable

[13] https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/
[14] There may be circumstances that prevent sharing of information even when such criteria are met (i.e. when information is protected by solicitor-client privilege.)
[15] https://www.priv.gc.ca/en/privacy-topics/accessing-personal-information/obligations-for-organizations/02_05_d_54_ati_02/

to the request such as having the individual review records in the office or providing paper copies of information. Vidia Corporation will retain copies of any and all information disclosed during this process for a minimum of five years.

It is possible that the individual concerned may request access to information related to this disclosure. If this happens, Vidia Corporation must notify the institution to which the information was disclosed. The institution has 30 days to respond.

Vidia Corporation may not respond to the individual's access request before either hearing back from the institution or until 30 days has passed since Vidia Corporation notified it; whichever occurs first.

If the institution objects to the release of the information to the individual based on permissible grounds, Vidia Corporation must withhold it. Vidia Corporation may not reveal that we communicated with the institution, or that it objected to the disclosure.

If we are in receipt of a production order, by law enforcement, we will perform an assessment of the facts, context, and ML/TF indicators to determine whether there is reasonable grounds to suspect that a particular transaction is related to the commission of ML/TF."

11 Voluntary Self-Declaration of Non-Compliance

If Vidia Corporation becomes aware of a non-compliance event, that leads to an issue in relation to reporting, client identification, record keeping, or effectively implementing an area of our compliance program, a voluntary self-declaration of non-compliance will be made to FINTRAC in writing, by the Compliance Officer.

The voluntary self-declaration of non-compliance must include the following:

- Our company name and the Compliance Officer's contact information;
- What is the issue and how it was discovered;
- For reporting issues, what type of report, the number of reports impacted or missed, and the time period during which the issue occurred;
- For reporting issues, the reason why the reports were not submitted, were late, or incorrect;
- For other issues: the period of time during which the issues occurred, the reason for their occurrence; and how the issue will be resolved and when it will be resolved.

The voluntary self-declaration of non-compliance is sent directly to: VSDONC.ADVNC@fintrac-canafe.gc.ca. A record will be retained by the Compliance Officer.

In cases where there are missing reports, the Compliance Officer (or delegate) will submit them without further delay.

12 Ongoing Monitoring

Ongoing monitoring is conducted in real time by the Compliance Officer or a designate for activities that may indicate that money laundering or terrorist financing could be taking place. Additionally, the use of blockchain analytic tools is leveraged at the time of a transaction which may result in an unusual activity alert.

Unusual activity is escalated to the Compliance Officer via electronic transaction monitoring alerts in the IT system and manually escalated by staff -based on their interaction with customers.

Where there is insufficient information present to determine whether or not a transaction is suspicious, additional investigations are conducted. These may include follow-up with Vidia Corporation's customers via phone, email or social media. All investigations are logged electronically. Detailed notes are used to ensure that all process steps are clear. Detailed notes are completed for each alert, whether or not the transaction is deemed to be suspicious.

Where transactions are deemed to be suspicious, the Compliance Officer or a delegate will file a STR or ASTR with FINTRAC as soon as practicable. Adjustments will also be made to the customer's risk level where required (if the customer has not already been designated as a high risk customer).

In some cases, the transaction may be suspended while Vidia Corporation contacts the customer to obtain additional information. Where the transaction is considered to be outside of Vidia Corporation's risk tolerance (as defined by the Compliance Officer) and mitigating documents or information cannot be obtained, the transaction may be rejected by Vidia Corporation.

Regardless of whether or not a transaction that has been escalated to the Compliance Officer is deemed to be suspicious and reported to FINTRAC, a record of the investigation steps and rationale for the reporting decision will be maintained for a minimum of five years.

Refer to Everypay Canada's Transaction Monitoring Procedures for more information.

12.1 Enhanced Due Diligence & Enhanced Ongoing Monitoring

For high risk customers and business relationships, the Compliance Officer or a delegate will conduct a full review of account activities. Where there is activity that is not consistent with the information on file about the customer and/or the stated purpose of the business relationship, the customer may be contacted for additional information.

Internet-based searches may also be performed at the time that enhanced due diligence is conducted. Specifically, the Compliance Officer or a delegate will make note of any findings related to:

- Money laundering or terrorist financing;
- Financial crime or serious crime;
- Discrepancies between publicly available information and information listed in the customer's profile; and/or
- Any other information that could affect Vidia Corporation's assessment of the customer's risk profile.

Vidia Corporation may request additional clarification or information from a customer where there are discrepancies between the customer profile and publicly available information.

All follow up activities are documented, including customer responses for additional information.

All records are maintained electronically, for a minimum of five years.

Where there is a high risk of money laundering offence or terrorist financing activity the customer will be assessed as high risk and we will conduct EDD. We will consider all the activity and accounts associated with a customer and we will review quarterly customer's activity over a reasonable threshold dollar amount that is in line with the customer's source of income. Our organization will document the results of our findings.

Refer to Vidia Corporation's KYC policy for more enhanced due diligence measures.

13 PEP & HIO Checks

MSBs are required to determine whether or not the customer is a Politically Exposed Person (PEP) or Head of an International Organization (HIO), or the close associate or family member of a PEP or HIO in the following cases:

- When we enter into a business relationship with a customer;
- When conducting periodic monitoring of business relationships;
- Upon detection of a fact about an existing business relationship that indicates a PEP or HIO connection;
- When we receive CAD 100,000 or more; or
- When we transfer CAD 100,000 or more;

PEPs may be foreign or domestic. The standards that apply will be slightly different, depending on whether the position that the person holds, or has held was within Canada (domestic) or outside of Canada (foreign).

Politically Exposed Foreign Persons (PEFPs), include anyone who holds or has held any of the following offices or positions in or on behalf of a foreign state:

- Head of state or head of government;
- Member of the executive council of government or member of a legislature;
- Deputy minister or equivalent rank;
- Ambassador, or attaché or counsellor of an ambassador;
- Military officer with a rank of general or above;
- President of a state-owned company or a state-owned bank;
- Head of a government agency;
- Judge of a supreme court, constitutional court or other court of last resort;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

A person determined to be a foreign PEP, is forever a foreign PEP (even after they no longer hold the position).

Domestic Politically Exposed Persons (PEPs) include anyone that holds or has held one of the offices or positions on behalf of the federal government or a provincial government:

- Governor General, lieutenant governor or head of government;
- Member of the Senate or House of Commons or member of a legislature;
- Deputy minister or equivalent rank;
- Ambassador, or attaché or counsellor of an ambassador;
- Military officer with a rank of general or above;
- President of a corporation that is wholly owned directly by Her Majesty in right of Canada or a province;
- Head of a government agency;
- Judge of an appellate court in a province, the Federal Court of Appeal or the Supreme Court of Canada;
- Leader or president of a political party represented in a legislature; or
- Holder of any other prescribed office or position.

It also includes anyone that holds or has held one of the following offices or positions in a municipal government:

- Mayor.

A person ceases to be a domestic PEP 5 years after they have left office.

The head of an international organization is a person who is either:

- the head of an international organization established by the governments of states; or
- the head of an institution established by an international organization.

If the organization was established by means of a formally signed agreement between the governments of more than one country, then the head of that organization is a HIO. The head of an international organization or the head of an institution established by an international organization is the primary person who leads that organization, (i.e., a President or CEO).

In addition to PEFPs, PEPs and HIO, we consider prescribed family members of such persons that we know are closely associated, for personal or business reasons, with a politically exposed person or HIO as high risk customers.

Prescribed family members include:

- mother or father;
- child;
- spouse or common-law partner;
- spouse's or common-law partner's mother or father and
- brother,
- sister, and
- half-brother or half-sister (that is, any other child of the individual's mother or father).

Persons that are closely connected include:

- business partners with, or who beneficially owns or controls a business with, a PEP or HIO;
- in a romantic relationship with a PEP or HIO, such as a boyfriend, girlfriend or mistress;
- involved in financial transactions with a PEP or a HIO;
- a prominent member of the same political party or union as a PEP or HIO;
- serving as a member of the same board as a PEP or HIO; or
- closely carrying out charitable works with a PEP or HIO.

When an Vidia Corporation employee is aware that our customer is a PEFP, PEP, or HIO they will notify the Compliance Officer immediately, so that they can perform a risk assessment and adjust the customer's risk ranking accordingly. Foreign PEPs, their family members and close associates are automatically considered a high-risk customer.

When a risk assessment is required for a domestic PEP or HIO, the Compliance Officer will conduct a negative media search to determine if the domestic PEP should be considered not high or high risk. Record of the risk assessment should be stored electronically.

In the event that a customer is determined to be a PEP or HIO, the Compliance Officer will ensure that Senior Management is aware of the account and due to compliance policy will not onboard any client who is a PEP or will end a relationship with a customer who is determined to be a PEP during the course of the relationship.

The Compliance Officer must keep a record after we have determined that a person is a PEFP, a high-risk HIO, PEP, family member or close associate of one of these. The record must include:

- the office or position of the PEP or HIO;
- the name of the organization or institution of the PEP or HIO;
- the source of the funds;

- the source of wealth;
- the date of determination;
- the name of the member of senior management who reviewed the transaction or approved keeping the account open; and
- the date the transaction was reviewed.

As a best practice if our customer is a PEP because they are a family member or close associated, Vidia Corporation will take reasonable measures to record the nature of the relationship between our customer and the person that holds the office or position leading to the PEP designation.

13.1 Senior Management Sign Off

In the case that a PEFP or a high risk PEP or HIO, Senior Management must be notified, and sign-off documented within 30 days.

In order to document the decision and related rationale, the Compliance Officer sends email to Senior Officer and the Senior Officer responds. The Compliance Officer maintain a record of all such communication.

14 List Screening

We screen all customer at the time of each transaction against publicly available lists of known terrorist individuals, such as UNSC consolidated lists, and the Consolidated Canadian Autonomous Sanctions List, the Public Safety Canada list. Screening is completed via a third-party service provider at onboarding and periodically throughout our relationship with the customer thereafter.

Potential matches are resolved by the Compliance Officer or a delegate. The investigation of a potential match may require us to obtain additional information or documentation from the customer.

In the event that a list match is deemed to be a true match, the Compliance Officer will freeze the account and send reports to FINTRAC, CSIS and the RCMP.

The Compliance Officer will develop messaging for staff in dealing with the customer to explain the freezing of the assets (funds) and conduct an investigation to determine whether there are any other customers affiliated with the listed person or entity.

If our customer is not a listed person or entity, or we are not in possession of property belonging to the customer, an STR or ASTR should still be filed if there are reasonable grounds to suspect terrorist financing and/or terrorist activity.

Records of all investigations, including the rationale for match/no match decisions must be maintained for at least five years.

Refer to Vidia Corporation's KYC policy for more information on screening procedures.

15 Record Keeping

Vidia Corporation must maintain specific records in order to meet legislative obligations. These records may be maintained either on paper or electronically. The Compliance Officer will ensure that records retention policies and processes are sufficient in:

- Maintaining records required under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and its enacted regulations for at least five years; and
- Storing all official records in a form and manner that allows these records to be retrieved in a timely manner.

A full listing of the records that must be maintained as it pertains to our business is contained within an appendix to this procedure document.

Generally, if FINTRAC makes a request for any of such records, the information must be delivered to them within 30 calendar days.

16 Compliance Program Monitoring and Testing

Vidia Corporation should ensure the adequacy, adherence, and effectiveness of day-to-day AML & CTF compliance procedures, using a risk-based approach. Testing should identify any patterns, themes or trends in compliance controls that may indicate weaknesses. Compliance control processes should include verification of key information (including any significant remediation activities stemming from regulatory exams and effectiveness reviews).

This validation should be on a rotational basis and should be undertaken using a risk-based approach. This includes testing of both operational and independent oversight AML & CTF compliance controls.

The Compliance Officer (or designate) will plan and execute testing considering risk and business model changes. If possible, the testing should be conducted by someone outside of the Compliance department or someone not involved in the task that is being tested.

Where deficiencies are observed, the Compliance Officer (or designate) will ensure remediation action plans are created and tracked. Depending on the nature of the deficiencies observed, the Compliance Officer may report findings to Senior Management.

Refer to Vidia Corporation's Transaction Monitoring Policy for other Quality Control measures.

17 Appendix: Sample Compliance Officer Quick Reference

This chart has been developed to assist the Compliance Officer in meeting time sensitive requirements. It is not intended to be a full listing of all AML and CTF Compliance Responsibilities.

17.1 AML & CTF Program Maintenance

There are 5 key elements that must all be documented:

1. **Compliance Officer**: a person that is responsible for your compliance program, including communication with your regulators.
2. **Policies & Procedures**: documents that explain what you must do, and how you are meeting these obligations.
3. **Risk Assessment**: a document that describes and quantifies the risk that your business could be used to launder money or finance terrorism, as well as the controls that you have in place to prevent this from happening.
4. **Training & Training Plan**: for all staff that handle customers and/or transactions, this must be delivered regularly (at least annually, and more often if there are changes to Canadian legislation or your business model).
5. **AML Compliance Effectiveness Review & Plan**: a review is like an audit for compliance. The review must test all elements of your compliance program, as well as your operations (what you are actually doing). All reviews should include a formal report that describes the methodology and results.

The AML Compliance program should be updated at regular intervals. This chart can be used to help you keep track of upcoming deadlines.

What?	When?	Last Completed	Next Due Date
Vidia Corporation Inc Anti-Money Laundering and Counter Terrorist Financing Policy	Annual	December 2024	December 2025
Vidia Corporation Inc Anti-Money Laundering and Counter Terrorist Financing Procedures for Compliance Staff	Annual	December 2024	December 2025
Vidia Corporation Inc Anti-Money Laundering and Counter Terrorist Financing Procedures for All Staff	Annual	December 2024	December 2025
Vidia Corporation Inc Risk Assessment	Annual	December 2024	December 2025
Training Program	Annual	Q1 2025	Q1 2026
Compliance Testing and Monitoring	TBD	TBD	TBD

AML Compliance Effectiveness Review	Every Two Years	TBD	TBD
Management Sign Off on Review	Within 30 days of the review's issue	TBD	TBD

17.2 Training

You should keep a log of all AML and CTF Compliance Training (including training sessions that you take to keep your knowledge sharp). This format can be used to keep track of the training that took place within our organization. The content section should include how the training was delivered and what was covered. This can be a brief bullet point summary.

The category section should include the type of training (Annual Staff Training, New Hire Training, Compliance Officer Training, etc.) that was provided.

These records may be shared with reviewers, financial service partners and FINTRAC. They should be kept up to date at all times and go back at least two years.

Content	Delivered by (Person, Role & Organization)	Delivery Method (In person, webinar, phone, etc.)	Plan Date	Completed Date	Date Persons Trained	Type of Training	Next Planed Training Date	Type of Training

17.3 Reporting

The reports that you submit to FINTRAC and other agencies must be submitted within certain timeframes. Reports submitted to FINTRAC, with the exception of Terrorist Property Reports (TPRs) can be submitted via FINTRAC's electronic web reporting system[16]. The below are reports that apply to Vidia Corporation.

[16] http://www.fintrac.gc.ca/reporting-declaration/Info/f2r-eng.asp

Report Type	Applicability	Timing	Reported To	How is it submitted?
Electronic Funds Transfer Report (EFTR)	Applies to Vidia Corporation.	5 working days from the transaction date	FINTRAC	Electronically via FINTRAC's Web Reporting System
Large Virtual Currency Transaction Report (LVCTR)	Applies to Vidia Corporation.	5 working days after the day on which we receive the amount	FINTRAC	Electronically via FINTRAC's Web Reporting System
Suspicious Transaction Report (STR)	Applies to Vidia Corporation.	As soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing	FINTRAC	Electronically via FINTRAC's web reporting system
Attempted Suspicious Transaction Report (ASTR)	Applies to Vidia Corporation.	As soon as practicable after completing the measures that enabled a determination that there are reasonable grounds to suspect that the activity could be related to money laundering and/or terrorist financing	FINTRAC	Electronically via FINTRAC's web reporting system
Terrorist Property Report (TPR)	Applies to Vidia Corporation.	Immediately	FINTRAC, RCMP, CSIS	On paper (via fax), email and/or webform

If reports are submitted to FINTRAC via their web reporting system, you will receive an electronic confirmation that the report has been received. Keep a copy (either paper or electronic) for your records.

There are two ways to send a paper report to FINTRAC in such a way as to obtain an acknowledgment of receipt:

1) Fax: 1-866-226-2346; or
2) Registered mail to the following address: Financial Transactions and Reports Analysis Centre of Canada, Section A, 234 Laurier Avenue West, 24th floor, Ottawa ON, K1P 1H7, Canada

You may send your report by regular mail to the FINTRAC address above. However, FINTRAC will not send you any acknowledgement when your paper report has been received[17].

Terrorist Property Reports must also be sent to the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS)[18]:

- RCMP, Attn: Anti-Terrorist Financing Team, RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca
- CSIS Financing Unit, complete the form on this page: https://www.canada.ca/en/security-intelligence-service/corporate/reporting-national-security-information.html

17.4 Record Keeping

It is important to keep records of everything that you are doing to meet your compliance requirements. Certain records are called out specifically within the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFR) and its enacted regulations. These include:

- Certain records created in the normal course of business:
    - The initiation of the sending of funds at the request of a person or entity in the amount of $1,000 or more, a record of:
        - The date of the transmission;
        - The type and amount of each type of funds that is involved in the transmission;
        - The person's or entity's:
            - Name;
            - Physical address;
            - Telephone number,
            - The nature of their principal business or their occupation; and
            - In the case of a person, their date of birth.
        - The exchange rates used and their source;

[17] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide5/5-eng

[18] https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/Guide5/5-eng

        - The name and address of each beneficiary;
        - The number of every account that is affected by the transaction; and
        - Every reference number that is connected to the transaction and has a function equivalent to that of an account number.
    - The final receipt of funds at the request of a person or entity in the amount of $1,000 or more, a record of:
        - The date of the remittance;
        - The date of the receipt;
        - The type and amount of each type of funds that is involved;
        - The name of the person or entity who requested the remittance;
        - Each beneficiary's:
            - Name;
            - Physical address;
            - Telephone number;
            - The nature of their principal business or their occupation; and
            - In the case of a person, their date of birth.
        - The exchange rates used for the remittance and their source;
        - if the remittance is in funds, the type and amount of each type of funds involved;
        - if the remittance is not in funds, the type of remittance and its value, if different from the amount of funds finally received;
        - The number of every account that is affected by the transaction;
        - Every reference number that is connected to the transaction and has a function equivalent to that of an account number.
    - Records of virtual currency transactions of CAD 1,000 or more, including the virtual currency exchange transaction ticket details:
        - The date of the transaction;
        - The name and address of the person or entity that requests the exchange;
        - The nature of their principal business or their
        - The date of birth;
        - The type and amount of each type of funds and each of the virtual currencies involved in the payment made and received by the person or entity that requests the exchange;
        - The method by which the payment is made and received;
        - The exchange rates used and their source;
        - The number of every account that is affected by the transaction, the type of account and the name of each account holder;

            - Every reference number that is connected to the transaction and has a function equivalent to that of an account number; and
            - Every transaction identifier, including the sending and receiving addresses.
- Complete customer identification information;
- Complete records for Politically Exposed Persons (PEPs) and related information;
- A copy of every report sent to FINTRAC:
    - Suspicious Transaction Reports;
    - Terrorist Property Reports;
    - Large Cash Transaction Reports;
    - Large Virtual Currency Transaction Reports;
- Records of large virtual (VC) currency reports:
    - the date we received the VC;
    - for any person involved in the transaction (including the person from whom you received the VC), their name, address, date of birth, and their occupation, or in the case of a sole proprietor, the nature of their principal business;
    - for any entity involved in the transaction (including the entity from which you received the VC), their name, address and the nature of their principal business;
    - the type and amount of each VC involved in the receipt;
    - the exchange rates used and their source;
    - if an account was affected by the transaction, include:
        - the account number and account type; and
        - the name of each account holder;
    - every reference number related to the transaction that is meant to be equivalent to an account number; and
    - every transaction identifier (this may include a transaction hash or similar identifier, if applicable), and every sending and receiving address;
- Internal unusual transaction forms (whether or not they were reported to FINTRAC by the Compliance Officer) and a record of the Compliance Officer's investigation process, including a rational that describes why the transaction or attempted transaction was or was not reported to FINTRAC;
- A record of the content, date and completion/attendance of any AML or CTF related training sessions, including internal staff training sessions and any quiz score results;
- AML Compliance Effectiveness Review reports, including a record of Senior Management sign-off on the final report;
- All FINTRAC correspondence and reporting;
- All internal memorandums;
- All AML and CTF compliance program documents, including policies, procedures and our Risk Assessment;
- All customer risk ranking documentation;

- All records of enhanced due diligence for higher risk customers;
- All records of transaction monitoring for higher risk customers;
- Records related to business relationships; and
- Copies of signed agreements with our service providers.

18 Appendix: Sample Compliance Remediation & Update Log

This sample log format can be used to track the remediation of any AML or CTF compliance issues. Issues are generally discovered in five ways:

1) Annual program review;
2) Self-discovery;
3) AML Compliance Effectiveness Review;
4) FINTRAC Examination; or
5) Other (Include all details of compliance issue discovery).

The issues that pose the greatest risk to our company should be considered the highest priority for remediation. Any issues that form part of a formal findings letter from FINTRAC will also be considered the highest priority.

This log is maintained by the Compliance Officer or a designate and can be used to provide updates to Senior Management and the Board of Directors (if applicable).

Reason for Update	Date of Update	Description of the Update	Documents Updated	Compliance Officer Approval	Updated Documents Shared with All Staff	Additional Notes (If Applicable)

The content in this log may be in point form, but should be detailed enough that the issue and the steps taken to fix it are clear to someone that was not involved in the process. The cause of the issue should be included in the description if the cause is known.

This log can also be used by the Compliance Officer to track the updates to the AML Compliance program documents. If the program is reviewed and no significant changes are made to a document, then there should still be a line item that states that the program was reviewed, and no significant changes were made.

This document may be used to evidence to reviewers and regulators that regular program updates have occurred.

19 Appendix: Sample Compliance Program Monitoring & Testing Log

Category	Sub Category	Testing Performed	Results	Date	Testing Conducted By	Results Reviewed By / Reported To	Follow Up (If Applicable)
AML/CTF Program	Compliance Officer Appointment						
AML/CTF Program	Policy & Procedures						
AML/CTF Program	Risk Assessment						
AML/CTF Program	Training						
AML/CTF Program	AML Compliance Effectiveness Review / Audit						
Operations	Customer Identification, KYC and Recordkeeping (Including Business Relationships)						
Operations	Name Screening						
Operations	Transaction Monitoring						
Operations	Enhanced Transaction Monitoring (High Risk Customers & Business Relationships)						
Operations	Enhanced Due Diligence (High Risk Customers & Business Relationships)						
Operations	Reporting: Suspicious and Attempted Suspicious Transactions						
Operations	Reporting: Terrorist Property						

Category	Sub Category	Testing Performed	Results	Date	Testing Conducted By	Results Reviewed By / Reported To	Follow Up (If Applicable)
Operations	Unusual Transactions (Flagged But Not Reported to FINTRAC)						