PALMEX GROUP INC
ANTI-MONEY LAUNDERING & COUNTER TERRORIST FINANCING PROCEDURES FOR ALL STAFF

Implementation Date: August 2025

Version Number: 1.0

Last Updated: August 2025

Next Update: August 2026

Approved By: Petros Kattou, Compliance Officer

Senior Officer Approval for Program: Petros Kattou, Director

Document Classification: Confidential

Table of Contents

1 Staff

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

All procedures listed in this document are mandatory. In addition to reading this document, all employees are required to complete training at least annually.

2 Staff Procedure

As a Foreign Money Services Business (FMSB) we are required under Canadian legislation to have an anti-money laundering (AML) and counter terrorist (CTF) compliance program. This procedure should be read in conjunction with PALMEX GROUP INC (PALMEX)'s Canadian AML & CTF Policy and Risk Assessment. Additional procedures applicable to compliance staff only are documented in a separate procedure.

This procedure has been designed to assist staff who deal directly with our customers and our transactions. We are required to verify, collect, and record information about our customers and transactions. Violations of this procedure can have severe negative consequences for PALMEX. Any questions or concerns about this procedure should be directed to the Compliance Officer.

3 Money Laundering & Terrorist Financing

Money laundering is the process of taking money obtained by committing a crime and disguising the source to make it appear legitimate. Under the Criminal Code of Canada, it is illegal to launder money or to knowingly assist in laundering money. Under the PCMLTFA and Regulations, we must take steps to be sure that our business is not used to launder money and if we suspect that money laundering may be taking place, we must report it.

Terrorist financing[1] is the process of moving funds in order to pay for terrorist activities. Unlike money laundering, the source of the funds is not always criminal, but the intended use of the funds is criminal. Under the Criminal Code of Canada, it is illegal to knowingly assist in the financing of terrorism, including the possession of terrorist funds or property. If we know or suspect that we have terrorist property in our possession, it must be reported immediately.

[1] We also consider proliferation financing under terrorist financing. This refers to the act of providing funds or financial services which are used to aid in the manufacturing or acquisition of weapons in contravention of national laws.

3.1 How Money Laundering & Terrorist Financing Work

Money laundering is described as having three phases by the Financial Action Task Force ('FATF'). These are *Placement*, *Layering* and *Integration*[2].

Terrorist financing, as opposed to money laundering can, occur with legitimate funds, meaning funds which are not the proceeds of crime. Legitimate funds can be transferred and used by those who would commit terrorist activities. In this, it can be said that terrorist financing most often acts in the 'Layering' and 'Integration' phases described by the FATF. However, rather than luxury items, the funds are used for the commission or support of terrorist activities and/or organizations. These phases are described in detail below:

Placement: In the initial, or placement stage of money laundering, the launderer introduces illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.

Layering: After the funds have entered the financial system, the second, or layering stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channeled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.

Integration: Having successfully processed funds through the first two phases the launderer then moves them to the third stage, integration, in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

While it is useful to understand these stages, it is not necessary to identify the stage, or even to know that money laundering is taking place, to consider a transaction to be suspicious. It is enough to have "reasonable grounds to suspect" that money laundering may be occurring, based on the facts, context and indicators present. If something seems unusual, trust your instincts, and escalate the issue to the Compliance Officer. In any instance where there are reasonable grounds to suspect that a transaction may be related to money laundering or terrorist financing, it must be escalated to the Compliance Officer for review.

[2] http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

4 Customers

Before customers initiate applicable transactions (described below), we must conduct identification measures before those transaction can be completed. In these cases, we collect identification information and information about the customer (individuals and organizations).

For customers where there is an existing authenticated and up to date customer profile, it is not necessary to re-identify the customer at the time of a transaction.

Periodically (based on risk level), customer information and identification (if applicable) is updated.

5 Customer Authentication & KYC

PALMEX takes steps to collect Know Your Customer (KYC) and authentication information for all customers. All individuals who apply to become a user of our services undergo an onboarding process comprised of a questionnaire, submission of customer identification and providing us with the nature and purpose of the relationship with PALMEX.

PALMEX will not open nor maintain an anonymous profiles or profiles in a fictitious name nor will a profile be setup without full KYC being completed.

In cases that we cannot identify a customer, we must document the reasons that the customer could not be identified and our efforts to identify them. PALMEX will not open nor maintain an anonymous account or an account in a fictitious name nor will an account be opened without full KYC being completed.

6 Enhanced Customer Identification & KYC

In some cases, we need additional information in regards to identify our customers and record specific information about the customer. These situations are not negotiable. If we are not able to identify the customer, based on our current business model, we must decline the following types of transactions as it applies to our business model:

- Large virtual currency transactions (valued at CAD 10,000 or more in a single transaction or multiple transactions within 24 hours); and
- Virtual currency transactions valued at CAD 1,000 or more.

In other cases, we must take reasonable measures to attempt to identify the customer, if it is possible to do so, without letting the customer know that we may have suspicions about the nature of their activities. These include:

- Suspected money laundering or terrorist financing activity; and
- Terrorist property.

While under Canadian law we are only required to identified customers in the cases above, it is our standard process to steps to collect know your customer (KYC) information for all customers. All individuals, customers and corporate entities who apply to become a user of our services undergo an onboarding process comprised of an online questionnaire, submission of customer identification and providing us with the nature and purpose of their relationship with PALMEX.

6.1 Dual Process Method of Identification for Individuals

PALMEX confirms the identity of a customer, that is an individual, by referring to information from reliable and independent sources, and the information must be valid and the most recent. In order to qualify as reliable, the sources should be well-known and considered reputable.

Independent, means the sources providing the information cannot be us (as the reporting entity) or the customer, and the documents referred to cannot be from the same source. For example, reliable and independent sources can be the federal, provincial, territorial, and municipal levels of government, crown corporations, financial entities, or utility providers.

Under the dual process method, we can refer to any two of the following options:

- Documents or information from a reliable source that contain the customer's name and address;
- Documents or information from a reliable source that contain the customer's name and date of birth; or
- Documents or information that contain the customer's name and confirms that they have a deposit, credit card or other loan account with a financial entity.

The table below provides examples of the sources and documents that can be referred to when confirming a customer identification. In order to meet the standards of the dual process method, we must rely on two documents provided by the customer, but each document referred to cannot be from the same column.

Documents or information to verify name and address Column A	Documents or information to verify name and date of birth Column B	Documents or information to verify name and confirm a financial account Column C
Issued by a Canadian government body: Any card or statement issued by a Canadian government body (federal, provincial, territorial, or municipal):	Issued by a Canadian government body: Any card or statement issued by a Canadian government body (federal, provincial, territorial, or municipal)	Confirm that your customer has a deposit account, credit card or loan account by means of: • Credit card statement; • Bank statement; • Loan account statement (for example: mortgage);

Documents or information to verify name and address Column A	Documents or information to verify name and date of birth Column B	Documents or information to verify name and confirm a financial account Column C
• Canada Pension Plan (CPP) statement; • Property tax assessment issued by a municipality; or • Provincially-issued vehicle registration. Benefits statement • Federal, provincial, territorial, and municipal levels. CRA documents: • Notice of assessment; • Requirement to pay notice; • Installment reminder/receipt; • GST refund letter; or • Benefits statement.	• Canada Pension Plan (CPP) statement of contributions; • Original birth certificate; • Marriage certificate or government-issued proof of marriage document (long-form which includes date of birth); • Divorce documentation; • A permanent resident card; • Citizenship certificate; or • Temporary driver's license (non-photo).	• Cheque that has been processed by a financial institution; • Telephone call, email or letter from the financial entity holding the deposit account, credit card or loan account; • Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months); or • Use of micro-deposits to confirm account.
Issued by other Canadian sources: • Referring to the customer's Canadian credit file that has been in existence for at least 6 months; • Utility bill (for example, electricity, water, telecommunications); • T4 statement; • Record of Employment; • Investment account statements (for example, RRSP, GIC); or • Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months).	Issued by other Canadian sources: • Referring to a customer's Canadian credit file that has been in existence for at least 6 months; • Insurance documents (home, auto, life); or • Identification product from a Canadian credit bureau (containing two trade lines in existence for at least 6 months).	
Issued by a foreign government: • Travel Visa.		

Where we use the dual process method to confirm the identity of a customer, we must record certain information. Specifically:

- The customer's full name (no initials, short forms or abbreviations);
- The customer's occupation (this should be as detailed as possible and be full form, without abbreviations or acronyms);
- The customer's date of birth (if this appears on the identification document, the date of birth that we record must match the document);
- The customer's full home address (post boxes, office addresses and general delivery addresses are not acceptable for this purpose; if the customer wishes to provide a separate mailing address, we can collect this as well, but we must always record the full home address);
- The name of the two different sources that were used to identify our customer;
- The type of information (for example, utility statement, bank statement, marriage license, CRA notice of assessment, etc.) that was referred to;
- The account number associated with the information;
- If there is no account number, you must record a reference number that is associated with the information; and
- The date we verified the information.

All customers must provide a government-issued photo identification and proof of address during onboarding which is passed to a third-party service provider called Trulioo[3]. During the onboarding process, users will be asked to take a photo of the front and back of their ID, and provide proof of address, as well as a selfie for additional assurance. This data is used to compare against the information previously provided as part of the customers profile and is verified by Trulioo to ensure the information uploaded is reliable, independent, valid and recent. PALMEX is given a pass/fail response from Trulioo.

6.2 Business Relationships

We have a business relationship with any individual customer that has completed two or more transactions that require us to identify the customer. In these cases, we must ask about the purpose of the customer's business relationship with us and record that purpose. In most cases, this will be relatively straightforward, for example "to purchase virtual currency for personal use." The answers that we record should be as specific as possible. It is our practice to collection this information at onboarding.

We also have to conduct a Politically Exposed Person (PEP) or Head of an International Organization (HIO) determination when we enter into a business relationship with a customer. It is our practice to conduct such checks at onboarding and periodically thereafter.

[3] https://www.trulioo.com/

6.3 Customers That Cannot Be Identified

If we are not able to identify a customer, they cannot complete transactions that require identification.

Some customers may be hesitant to provide identification for legitimate reasons. Remember that if you are obtaining identification because you suspect that the customer's transactions or requests are related to terrorist financing or money laundering, you should not tell the customer about your suspicion. Instead, let the customer know that it is our company's policy to ask for identification. Since most objections will be related to privacy and marketing, and not AML or CTF, let the customer know that the information will not be used for marketing purposes if they do not wish to receive marketing messages from PALMEX [4].

6.4 Records Related to "Reasonable Efforts"

In any case where PALMEX is required to take reasonable efforts to obtain or confirm information and/or collect documentation, we must keep a record of those efforts, the date they were taken and whether or not they are successful.

These records are maintained electronically.

7 Reporting

PALMEX must report certain types of transactions.

Reporting to any regulatory, law enforcement, or government agency, should always be completed by the Compliance Officer or a designate (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 (i.e., Unusual Transaction Form) to submit reports to the Compliance Officer.

If you aren't sure whether or not you will need to submit a report, speak with the Compliance Officer for clarification. If it is not possible to speak with the Compliance Officer at that time, err on the side of caution by collecting the information that you need to fill out the form(s) and submit the report(s).

This may include collecting the customer's identification information.

All reports have specific timelines in which they must be submitted. All internal reports should be submitted to the Compliance Officer on the same day that the incident or transaction takes place.

[4] If the customer indicates that they do not wish to receive marketing messages, this should be noted and passed on to the Privacy Officer to be certain that the customer is not added to marketing lists.

These transactions are detected automatically by the IT system and escalated manually by staff members. The Compliance Officer reviews transaction related alerts on a regular basis.

7.1 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 PALMEX or cancelled by the customer.

These reports must be submitted to FINTRAC as soon as practicable (without delay) after completing the measures required to establish reasonable grounds to suspect it may be related to money laundering or terrorist financing.

Employees should report this type of transaction using the Unusual Transaction Form (Internal), included as an appendix in this document. A list of suspicious transaction indicators is also included in this document and should be reviewed regularly by all staff.

It is important not to let the customer know that you are suspicious. It is against the law to deliberately "tip off" a customer about a potential investigation. You are, however, protected under Canadian law from any action when you 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.

In rare instances, where staff suspects that the threshold to report has been reached but the Compliance Officer will not file a STR, an employee can report a suspicious transaction on paper themselves[5]. A reminder that no person or entity will be prosecuted for sending an STR in good faith or for providing FINTRAC with information about suspicions of money laundering or terrorist financing.

It is important to try to identify customers that conduct or attempt suspicious transactions. The customer may ask you why you 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). It is imperative that the customer is not made aware that the transaction is being viewed as suspicious.

STRs and ASTRs must be submitted to FINTRAC as soon as practicable after we have taken measures that enable us to establish that there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission of a money

[5] https://www.fintrac-canafe.gc.ca/reporting-declaration/form/STR-eng.pdf

laundering offence or a terrorist activity financing offence. To meet our obligations, the internal form must be submitted to the Compliance Officer on the same day that the transaction occurs.

7.2 Large Virtual Currency Transactions

Large Virtual Currency Transaction Reports (LVCTR) have to be submitted to FINTRAC when a customer conducts transactions, in virtual currency, valued at CAD 10,000 or more in the same 24-hour period. This may be in a single transaction or several separate transactions.

For such transactions, we are required to verify a customer's identification. We must also conduct a third-party determination as detailed in section 7.4.

LVCTRs must be submitted to FINTRAC within five working days after the day on which the customer transfers or receives the amount.

7.3 Travel Rule

The travel rule refers to specific information that should be included with the information sent or received for virtual currency and EFT transactions. The travel rule information 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.

If we receive such transactions that do not contain the information defined above, we must take reasonable measures to obtain that information. If we are unable to obtain this information, we may reject the transaction.

7.4 Third-Party Determinations

A third-party determination must be completed anytime 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.

If there is no third-party, we must still record in the system that a third-party determination was completed.

7.5 PEP & HIO Determinations

FMSBs 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;

PEP determinations are conducted via a third-party service provider.

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).

Foreign PEPs are people who hold or have ever held any of these positions on behalf of a foreign government:

- 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.

Domestic PEPs are people who hold or held in the last five years any of these positions on behalf of the federal government or a provincial/territorial 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.

Domestic PEPs also include 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 five 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).

If a person is a foreign PEP, domestic PEP or HIO is considered high-risk, then certain prescribed family members and close associates (for personal or business reasons,) must also be treated as high-risk.

Prescribed family members include:

- mother or father;
- child;
- spouse or common-law partner;
- spouse's or common-law partner's mother or father;
- 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 a PALMEX employee becomes aware that our customer is a PEFP, PEP, or HIO, they will notify the Compliance Officer immediately so that a risk assessment can be performed, and an adjustment can be made to the customer's risk rating. Foreign PEPs,

their family members and close associates are automatically considered high-risk customer.

If a customer is determined to be a PEP, PEFP, or HIO, the Compliance Officer will ensure that Senior Management is aware of the account and has approved the customer or business relationship within 30 days of the PEP or PEFP determination.

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 we should also record the nature of the relationship between your customer and the PEP or HIO, as applicable

The Compliance Officer must be notified immediately when a customer is a PEP. The Compliance Officer will review the transaction and provide sign-off on behalf of Senior Management. This sign-off must be recorded within 30 calendar days of the date that we determine that our customer is a PEP.

7.6 Terrorist Property

Terrorist Property Reports (TPRs) are completed if you believe that PALMEX may be in possession of funds or property that belong to a terrorist (either an individual or an organization).

These reports should be escalated to the Compliance Officer immediately. In some cases, property or funds must be frozen.

Like STRs and ASTRs, the contents of these reports, or the fact that you are filing a report, should not be disclosed to the customer. These reports are submitted to FINTRAC, as well as directly to law enforcement agencies, and must be submitted immediately.

TPRs must be submitted to FINTRAC, and other agencies, immediately. In order to provide enough time for the Compliance Officer to complete reporting, the internal form must be submitted on the same day that the transaction occurs.

8 Responding to Law Enforcement Requests

If staff are aware that a request has been made by law enforcement, they must immediately notify the Compliance Officer who will handle all related correspondence.

9 Unusual Indicators & Red Flags

There are a wide variety of indicators that can let us know that a transaction or request may be related to money laundering or terrorist financing. These include customer behaviours, as well as transaction patterns. Trust your instincts – if something doesn't feel right (whether or not any of these indicators are present), file an Unusual Transaction Report with the Compliance Officer.

These indicators are a sample provided by FINTRAC and will be augmented regularly by the Compliance Officer based on trends that we have observed in our business transactions and/or industry.

9.1 General

- The individual or entity appears on a government a sanction list.
- Customer admits or makes statements about involvement in criminal activities.
- Customer shows uncommon curiosity about internal systems, controls, and policies.
- Customer has only vague knowledge of the amount of a transaction.
- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer over justifies or explains the transaction.
- Customer is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Customer's home or business telephone number has been disconnected or there is no such number when an attempt is made to contact customer shortly after opening account.
- Normal attempts to verify the background of a new or prospective customer are difficult.
- Customer appears to be acting on behalf of a third-party, but does not tell you.
- Customer is involved in activity out-of-keeping for that individual or business.
- Customer insists that a transaction be done quickly.
- Inconsistencies appear in the customer's presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the customer.
- Customer attempts to develop close rapport with staff.
- Customer spells his or her name differently from one transaction to another.
- Customer provides false information or information that you believe is unreliable.
- Customer offers you money, gratuities, or unusual favours, for the provision of services that may appear unusual or suspicious.

- You are aware that a customer is the subject of a money laundering or terrorist financing investigation.
- You are aware or you become aware, from a reliable source (that can include media or other open sources), that a customer is suspected of being involved in illegal activity.
- You know a new or prospective customer as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist)

9.2 Knowledge of Reporting or Record Keeping Requirements

- Customer attempts to convince employee not to complete any documentation required for the transaction.
- Customer makes inquiries that would indicate a desire to avoid reporting.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer seems very conversant with money laundering or terrorist activity financing issues.
- Customer is quick to volunteer that funds are “clean” or “not being laundered.”
- Customer appears to be structuring amounts to avoid record keeping, customer identification or reporting thresholds.
- Customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds.

9.3 Identity Documents

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only submits copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details such as a phone number.
- Customer inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Customer presents different identification documents at different times.
- Customer alters the transaction after being asked for identity documents.
- Customer presents different identification documents each time a transaction is conducted.

9.4 Economic Purpose

- Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the customer.
- Activity is inconsistent with what would be expected from declared business.
- A business customer refuses to provide information to qualify for a business discount.
- No business explanation for size of transactions or cash volumes.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

9.5 Indicators Specific to Human Trafficking

The following indicators are specific to human trafficking for sexual exploitation and reflect types and patterns of transactions, contextual factors and those that emphasize the importance of knowing your customer. These indicators and other facts surrounding a financial transaction should be considered as a whole. This is important because a single transaction taken in isolation may lead to a false assumption of normalcy. Considering all indicators may reveal otherwise unknown links that taken together could lead to reasonable grounds to suspect that the transaction consists of proceeds from human trafficking.

9.5.1 Types of Financial Transactions

- Bitcoins or other virtual currencies: frequent purchases in multiples of small amounts (e.g., $3, $12, $24), directly by the customer or through exchanges;

9.5.2 Patterns of Financial Transactions & Account Activity

- Cash deposits/withdrawals between the hours of 10 p.m. and 6 a.m.;
- Multiple cash deposits conducted at different ATMs, possibly across different cities and provinces;
- Frequent transactions (e.g., purchases, payments, account debits/credits, electronic transfers) across different cities and provinces within short timelines;
- Common address provided by different people undertaking domestic/international funds transfers;

9.5.3 Contextual Indicators

- Media or other reliable sources suggest that a customer may be linked to criminal activity which could generate proceeds of crime;
- Media coverage of account holder's activities relating to human trafficking in the sex trade and/or prostitution rings;
- Use of addresses where prostitution is reported to occur by media, law enforcement, or classified ads;
- Phone number provided on online advertising and promotional services is used in different cities and provinces in a short period of time;

- Use of a third-party to execute transactions (for example, under the pretext of requiring an interpreter); and,
- Customer makes deposits accompanied or watched by a third-party who may, on separate occasions, accompany or watch customers who are making deposits. The third-party may be handing over to the customer what is subsequently confirmed to be the customer's identification.

9.5.4 Know Your Customer

- Financial activity is inconsistent with that expected based on one or more of the following: the customer's financial status, stated occupation, type of account or stated business activity;
- Customers give contact/identifying information that is traceable through open sources to advertising related to escort services;
- Use of someone else's identification, or opening an account in the name of an unqualified minor;
- Use of aliases for the purpose of opening multiple accounts in different banks, or in different branches of the same bank; and,
- Addition of an unusual number of individuals as joint account holders, or authorized users to products such as credit cards.

9.6 Indicators Specific to Online Child Sexual Exploitation

Below are money laundering indicators related to online child sexual exploitation. These indicators should not be treated in isolation; on their own, these indicators may not be indicative of money laundering or other suspicious activity. They should be assessed in combination with what is known about the client and other factors surrounding the transactions to determine if there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence. Considering several indicators may reveal otherwise unknown links that taken together could lead to reasonable grounds to suspect that the transaction is related to online child sexual exploitation offences and/or the laundering of proceeds derived from those crimes, it is a constellation of factors that strengthen the determination of suspicion.

9.6.1 Money laundering indicators related to possible perpetrators who are consumers and/or facilitators of online child sexual exploitation

- An individual is the subject of adverse media involving child sexual exploitation-related offences.
- Funds sent to or received from an individual (e.g., a convicted sex offender) charged with child sexual exploitation-related offences (including any luring offences) and/or funds to or from a common counterparty shared with such an individual.
- A male who frequently transfers low-value funds to the same female or multiple females in a/many jurisdiction(s) of concern for child sexual exploitation (e.g.,

Philippines) in a short timeframe and has no apparent familial or other legitimate connection to the country or recipient.

- A male (usually aged over 50) who transfers low-value funds from an in-branch/in-store location usually to a female in a jurisdiction of concern for child sexual exploitation usually between 1 p.m. and 8 p.m., regardless of Canadian time zone.
- A male who transfers low-value funds usually to a female in a jurisdiction of concern for child sexual exploitation through online banking or an online money services business platform in the late evening/early morning hours (usually between 8 p.m. and 1 a.m., regardless of Canadian time zone).
- Travel-related expenses (e.g., passport purchase, flight bookings, airline baggage fees) that occur closely before or after transfers to a jurisdiction of concern for child sexual exploitation.
- Transactions conducted or accounts accessed in a jurisdiction of concern for child sexual exploitation (e.g., ATM cash withdrawals, account logins through IP address in a jurisdiction of concern).
- Purchases at vendors that offer online encryption tools, virtual private network (VPNs) services, software to clear online tracking, or other tools or services for online privacy and anonymity.
- Payments to online file hosting vendors/platforms.
- Transfers to peer-to-peer financing websites or through peer-to-peer funds transfer platforms.
- Payments to or funds received through or from payment processors, including ones that deal in virtual currencies.
- Purchases on webcam/livestreaming platforms, including those for adult entertainment.
- Purchases on dating platforms, particularly Asian dating websites or ones that also offer adult entertainment content (dating websites observed in FINTRAC's analysis were: www.filipinocupid.com, www.asianbeauties.com, www.asiandating.com, www.asiandatingspace.com, www.asiandate.com, www.arabmatching.com, www.amolatina.com, www.lovetoria.com, www.naughtydate.com, www.mingle2.com, Tinder, Grindr).
- Purchases at adult entertainment venues and/or adult entertainment websites.
- Payments to or purchases through a payment processor that specializes in serving high-risk merchants such as those in the adult entertainment industry—some of which appear able to conceal the merchant's name.
- Payments to a self-storage facility and/or for office rentals.
- Purchases at multiple vendors of electronics, computers, and cell phones and/or payments to multiple cell phone service providers.
- Purchases at a vendor that rents or leases computers and/or computer equipment.
- Purchases at online gaming platforms and/or gaming stores.

- Transactions to reload prepaid credit cards (particularly ones that deal with virtual currencies).
- Purchases at online merchants.
- Purchases of gift cards and/or payments made using gift cards.
- Payments to or purchases through social media platforms, including ones that enable payment services through a payment processor.
- Email money transfers that include a partial email address or reference with terms possibly related to child sexual exploitation.
- Use of virtual currencies to fund a virtual currency account, convert funds and/or transfer funds to another virtual currency wallet, obtain a cryptocurrency loan or withdraw funds in cash.

9.6.2 Money laundering indicators related to possible perpetrators who are producers of online child sexual exploitation material

- Purchases at vendors that offer software for peer-to-peer (P2P) sharing platforms for P2P sharing of videos and images, including software to share hard drive content directly over the Internet.
- Purchases at vendors that offer software for capturing video from websites or other online platforms.
- Purchases at vendors that offer Voice-Over-IP communication services.
- Purchases at domain registration/website hosting entities.
- Purchases at vendors specializing in equipment or software for photography or video-making.
- Purchases at creator-content streaming websites (e.g., membership fees or subscriptions to these sites or payment of funds to other streamers on these sites).
- Receiving funds from a payment processor and having a profile on a creator-content streaming website (particularly a creator-content website that includes adult entertainment content with a subscription-based channel model).

9.6.3 Financial indicators possibly related to online child sexual exploitation in the form of luring

- Multiple purchases for accommodations (hotel/motel/peer-to-peer accommodation rentals), particularly at venues in the individual's own city or in a nearby city.
- Purchases made for long-distance travel (e.g., air travel, city-to-city bus).
- Use of separate email accounts to send or receive email money transfers.
- Email money transfers sent to multiple females, including minors.
- Purchases at youth-oriented stores or venues (e.g., toy store, children's clothing store, amusement park, playcentre, candy shop).

- Purchases at vendors for cannabis/cannabis-related products and equipment and/or at pharmacies.
- Payments to an online classified ad website.
- Purchases at youth-oriented live online chat rooms.

9.7 Indicators for Laundering the Proceeds of Fentanyl Trafficking

PALMEX considers the following indicators relevant to their sector in tandem with the low-level drug trafficking indicators that follow to effectively identify potential money laundering activities associated with the trafficking of fentanyl.

9.7.1 Laundering the Proceeds of Low-level Drug Trafficking

- Customer makes transactions that are inconsistent with his or her employment or profile.
- Customer conducts untypical cash transactions given his or her profile.
- Customer makes ATM transactions for larger amounts than would normally be expected.
- Customer lives beyond his or her apparent means, as evidenced by large credit card or other bills, or expenses for real estate or luxury goods.
- Customer incurs significant travel expenses that are inconsistent with his or her profile, such as for car rentals, hotel bills, airline tickets and gasoline.
- Customer has funds deposited into his or her account in amounts below the reporting threshold from what appear to be multiple third-parties located in many parts of the city, a broader geographic area or several provinces.
- Customer is involved in financial transactions that have been the subject of negative media (stories about drugs and weapons offences).
- Customer uses multiple financial institutions; his or her account sees significant cash flow-through; and he or she carries out little typical banking activity (such as paying household bills).
- Customer is a commercial entity that engages in trade transactions for products that do not appear to fit its known business profile.

9.8 Indicators for Laundering the Proceeds of Romance & Mass Marketing Fraud

PALMEX considers the following indicators that follow to effectively identify potential money laundering activities associated with romance and mass marketing fraud.

9.8.1 Indicators relating to romance fraud victims

- Customer met the individual they are transacting with on a social media platform, via email or on a dating website.
- Customer always, or almost always, communicates with the individual they met online by email or text.
- Customer has never met or has never seen the individual they are in the relationship with, and is often older than that individual.

- Customer relays a confusing, conflicting or non-believable story about why the funds are needed or the transaction is taking place.
- Customer is at a potentially more vulnerable stage of life (i.e., a senior or widowed, separated or divorced).
- Customer provides minimal or inconsistent information and/or avoids answering questions about the purpose of the transaction.

9.8.2 Indicators associated with transactions related to romance fraud

- Customer appears to be pooling all financial resources from various sources (e.g., credit cards, loans, retirement savings, insurance policies) and depleting assets (e.g., home, vehicle, investments and retirement savings) to fund transfers to individuals/entities.
- Customer sends funds to another individual, and the amount or frequency of funds sent increases over time.
- Customer is transacting with one or more individuals suspected of being either a victim or perpetrator of romance fraud.
- Customer is identified as a victim and is transacting with one or more individuals who are also identified as victims of romance fraud.
- Customer either cancels transaction for no apparent reason or transaction is refused due to questionable rationale for it.
- Customer makes payments to online dating services or social media websites.
- Customer conducts large volume and/or excessive number of transactions involving foreign jurisdictions over a short period.
- Customer receives funds from numerous individuals in multiple jurisdictions. The funds are then depleted by cash withdrawals conducted in Canada or abroad, or by wires to the benefit of individuals/entities in Canada or abroad.

9.8.3 Indicators of mass marketing fraud

- Customer conducts financial activity or holds accounts at multiple financial entities without adequate rationale.
- Non-account holders or apparently unrelated individuals make deposits or payments to customer's account.
- Customer does not appear to know the sender of a wire transfer from whom the wire transfer was received, or the recipient to whom they are sending a wire transfer.
- Customer conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.
- Account is used for pass-through activities (e.g., to receive and subsequently send funds to beneficiaries).
- Customer becomes defensive when asked about the rationale for a transaction and may take steps to close account or conduct transaction elsewhere.
- Customer orders wire transfers that are frequently returned or cancelled.

- Customer frequently deposits fraudulent cheques or bank drafts that are later returned by the financial institution.
- Customer appears to be directed by a third-party to deposit funds into accounts or to wire funds to individuals domestically or in foreign jurisdictions.
- Customer sends and/or receives an increasing amount of wires/EMTs.
- Customer's wire transfers involve amounts or jurisdictions that are inconsistent with their profile.
- Customer receives multiple incoming wires into a business account in a manner inconsistent with day-to-day business.
- Customer makes numerous third-party cash deposits followed by outgoing draft/wire transfers to or cash withdrawals in high-risk jurisdictions.
- Customer receives payments from payment processors that are inconsistent with the customer's profile.

9.9 Indicators of the Abuse of Virtual Currencies

PALMEX considers the following indicators from #ProjectParticipate to effectively identify potential money laundering, terrorist financing and sanctions evasion activities associated with virtual currencies.

9.9.1 User Information

9.9.2 Documentation

- A user provides falsified, altered, forged or inaccurate identification documents (including selfies), or documents inconsistent with the user's profile.
- A user provides unusual or suspicious identification documents that cannot be readily verified.
- A user provides a Post Office ("P.O.") Box or general delivery or agent's address instead of a street address, inconsistent with the jurisdictional norm.
- A user's telephone is disconnected or cannot otherwise be contacted.
- A user provides contact information (e.g., address, telephone number, email address) that is similar to or the same (in whole or in part) as that of another user.
- A user has a newly registered account.
- A user who is unable to provide strong evidence of sources of wealth/source of funds in respect to the amount of virtual assets.

9.9.3 User Behavior

- A user is over-providing information or details when not necessary.
- A user fails to provide additional information upon request, is reluctant to provide such information, or provides inconsistent information.
- A user takes an inordinate amount of time to provide what should be easily accessible documents.
- Frequent changes in the user's identification information, such as home address, IP address or linked bank accounts. It should be noted that IP addresses on mobile

phones may change frequently, and sudden changes in IP address changes may be explained by mobile phone access to VASPs.

- A user operates more than one account without first seeking approval from the platform.
- A user operates an account on behalf of a third-party without first obtaining consent from the platform and/or makes a false third-party declaration.
- A user attempts to form an unreasonably close relationship with employees, including customer support and compliance staff.
- A user shows uncommon curiosity about internal systems, controls and policies.
- A user requests exemption from ID requirements or reporting activities.
- A user offers inducements or bribes to employees.
- A user provides misleading or inaccurate information regarding source of funds and destination of funds, purpose of transaction, relationship to counterparty and/or transaction details.
- A user requests to delete any information/documentation that he or she previously submitted without providing a plausible explanation for the request.

9.9.4 Product & Channel

- A user's portfolio only consists of or has a high value of privacy coins (e.g., Monero, Dash, Zcash).
- A user has a long period of dormancy followed by a large volume/velocity of transactions.
- Paying and/or willingness to pay high commission fees for converting (selling) virtual assets in exchange for fiat, compared to commission fees typically charged by virtual assets exchanges.
- A user receives frequent and/or large value transactions from Bitcoin ATMs.
- A user is involved in conducting, or involved with organizations conducting, virtual assets mining operations.

9.9.5 Organizational Structure

- A user is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries (beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner's identity).
- Use of corporate vehicles (legal entities and legal arrangements) to obscure ownership, involved industries and jurisdictions.
- The organizational structure is unusually complex and/or includes subsidiaries in multiple jurisdictions.

9.9.6 Money Transmitter Documentation

- A user is unable to provide confirmation that it is registered with a financial authority.

- A user advises that the regulations for its jurisdiction are obscure or do not require registration with a financial authority.
- A user's AML/KYC policy and procedures have been copied and pasted from a publicly available source with minimal or no customization for the user's inherent risk.
- A user is unable to provide contact information for its Compliance Officer.
- A user takes an inordinate amount of time to produce AML/KYC policy and procedures and Compliance Officer information.

9.9.7 Other

- Use of Virtual Private Network ("VPN") and/or The Onion Router ("TOR").
- A user is registered with encrypted, anonymous email or a temporary email service (e.g., protonmail.com and tutanota.com).
- Requests from law enforcement or government authorities where a user's information has been requested as part of an investigation, or requests/legal orders to freeze a user's funds.
- Negative media or open source research reveals that the user is believed to be involved in illicit activity.
- A user admits or makes statements about involvement in illicit activities.

9.10 Exchange/Trading Platform

9.10.1 Movement & Velocity of Funds

- Funds deposited soon after account registration and withdrawn again shortly thereafter in the same virtual asset without using platform features (e.g., trading/margin funding) – may be indicative of a platform being used as a mixer/tumbler.
- Funds are primarily sent to or received from P2P exchanges without using the platform's features, particularly fiat-based services.
- Outgoing funds to newly created and heretofore never used virtual asset addresses.
- Funds deposited from or withdrawn to a virtual asset address with direct and indirect (e.g., few hops removed) links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, wallets known to be involved in illegal activities (e.g., ransomware) and/or theft reports.
- Funds in a user account have been reported stolen or otherwise reported to have been obtained illegally.
- Funds move from an illicit source through numerous intermediary addresses over a short period of time before being deposited with a VASP.
- A user submits comments for transactions (e.g., withdrawals) which may refer to illicit activity.
- Depositing virtual assets and withdrawing funds in fiat currency and vice-versa, without utilizing any platform services.

- A user has a high frequency of deposits or withdrawals with unknown third parties.
- A user requests a withdrawal to be processed unreasonably quickly or outside of a company's terms of service ("ToS").
- A user conducts transactions at specific times/amounts not in line with normal industry practices and/or transactions that are unnecessarily complex.
- Multiple third-party transactions being transferred and accumulated into one user account.
- A user conducts transactions of similar amounts to multiple third-parties.
- A user receives a large proportion of funds directly from a mixer/tumbler without pre-advising the receiving VASP.
- A user sends a large proportion of funds to a mixer/tumbler without pre-advising the sending VASP.
- A single ATM processes inexplicably high values of transactions in a short time period.
- Funds flow through a large number of intermediate addresses in a very short period of time prior to being deposited in a customer's wallet, or just after being withdrawn, and where the ultimate source or destination is an illicit entity.

9.10.2 Darknet Connections

- A user frequently receives funds from, or sends funds to, darknet wallet addresses that accumulate to large values.
- A significant percentage of a user's deposits to an exchange originate from darknet marketplaces.
- A significant percentage of a user's withdrawals from an exchange ultimately result in transactions with darknet marketplaces.
- Indirect exposure to darknet marketplaces is identified (i.e., the funds moved from a darknet wallet through two or more hops to the user's wallet in a short time frame in similar amounts).
- A user is found on open source forums or other sites that connect the user directly or indirectly to darknet markets.
- Direct exposure to the darknet marketplace is identified.
- A user is found to have been connected to TOR through the user's IP address or Internet Service Provider ("ISP").

9.10.3 Geography

- Transactions with jurisdictions known to be used to circumvent sanctions or used in trade-based money laundering schemes.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.

- Funds transfer activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the customer's operations or rated high-risk for ML, TF or sanctions avoidance.
- Bitcoin ATM withdrawals are made from high-risk geographies or areas with high crime rates.

9.10.4 Other

- A user exploits technological glitches/failures in an effort to intentionally take advantage of a platform or obtain funds.
- A user conducts trades in such a way that creates a negative balance or reduces equity in one account, in order to increase equity or create a positive balance in another account operated by the same user.
- A user conducts transactions that appear to be inconsistent with the user's KYC, transaction history/patterns and/or market trends.
- Transactions conducted appear to have no economic benefit or purpose.
- A platform receives unusual/demanding requests from other exchanges/vendors/ service providers in respect to a user's funds deposited on a platform.

9.10.5 Fiat Funding/Withdrawals

- Amount of funding is not consistent with the user's net worth or declared income.
- Funding is structured below the user's jurisdictional reporting thresholds (typically $10,000).
- Withdrawals are otherwise structured.
- A user receives and/or sends wires or provides information to a financial institution from prohibited or high-risk jurisdictions or areas run by an unstable government.
- Funding or withdrawals match to recognized watch lists.
- Transactions with jurisdictions known to be used to circumvent sanctions or used in trade-based ML schemes.

9.11 Politically Exposed Persons ("PEPs")

- A user utilizes third-parties to shield identity as a PEP or beneficial owner.
- Information volunteered by PEP user is inconsistent with other information, such as publicly available asset declarations, published official salaries and open source research.
- A PEP user seeks to make use of the services of a financial institution or a designated non-financial business or profession ("DNFBP") that would normally not cater to foreign or high value customers.
- A PEP user repeatedly moves funds to and from countries with which the user does not appear to have any ties.
- A PEP user has a substantial authority over or access to state assets and funds, policies, and operations.
- A PEP user provides documentation that reveals government contracts that are directed to companies that operate in an unrelated line of business (e.g.,

payments for construction projects directed to textile merchants and/or shell corporations or other unrelated activities).
- Information obtained that a PEP user is or has been denied entry to a country.
- A PEP user is from a country that prohibits or restricts its/certain citizens to hold accounts or own certain property in a foreign country.
- A PEP user (actively) downplays importance of the user's public function, or the public function with which the user is associated.

A PEP user from a country with a "mono" economy (i.e., economic dependency on one or a few export products), especially if export control or licensing measures have been recently put in place for such products.

9.11.1 Darknet Marketplaces

- A customer conducts transactions with virtual currency addresses that have been linked to darknet marketplaces or other illicit activity.
- A customer's virtual currency address appears on public forums associated with illegal activity.
- A customer's transactions are initiated from IP addresses associated with Tor.
- Blockchain analytics indicate that the wallet transferring virtual currency to the exchange has a suspicious source or sources of funds, such as a darknet marketplace.
- A transaction makes use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.

9.11.2 Illicitly Operating Dealers in Virtual Currency

- A customer receives multiple wire deposits from disparate jurisdictions, branches of a financial institution, or persons and shortly thereafter uses such funds to acquire virtual currency.
- A customer receives a series of deposits from disparate sources that, in aggregate, amount to nearly identical aggregate funds transfers to a known virtual currency exchange platform within a short period of time.
- Customer's phone number or email address is connected to a known peer-to-peer virtual currency exchange platform advertising exchange services.

9.11.3 Unregistered Foreign-Located MSBs

- A customer transfers or receives funds, including through traditional banking systems, to or from an unregistered foreign virtual currency exchange or other MSB with no relation to where the customer lives or conducts business.
- A customer utilizes a virtual currency exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate AML/CTF regulations for virtual currency entities, including inadequate KYC or customer due diligence measures.
- A customer directs large numbers of virtual currency transactions to virtual currency entities in jurisdictions with reputations for being tax havens.

- A customer that has not identified itself to the exchange, or registered with FINTRAC, as a money services business appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions, which may indicate that the customer is acting as an unregistered MSB.

9.11.4 Illicitly Operating Bitcoin ATMs

- A customer operates multiple Bitcoin ATMs in locations that have a relatively high incidence of criminal activity.
- Large numbers of transactions from different customers sent to and from the same virtual currency wallet address but not operating as a known virtual currency exchange.

9.11.5 Illicit Activity Leveraging Bitcoin ATMs

- Structuring of transactions just beneath the identification threshold or the Bitcoin ATM's daily limit to the same wallet address either by using multiple machines (i.e., smurfing) or multiple identities tied to the same phone number.

9.11.6 Other Potential Indicators

- A customer conducts transactions with virtual currency addresses that have been linked to extortion, ransomware, sanctioned virtual currency addresses, or other illicit activity.
- A customer's transactions are initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
- Use of virtual private network (VPN) services or Tor to access virtual currency exchange accounts.
- A customer initiates multiple rapid trades between multiple virtual currencies with no related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.
- A customer provides identification or account credentials (e.g., non-standard password, IP address, or flash cookies) shared by another account.
- A customer conducts transactions or rapidly executes multiple conversions between various types of different virtual currencies below relevant due diligence, recordkeeping, or reporting thresholds and then transfers the value off of the exchange.
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a virtual currency money mule or a victim of elder financial exploitation.
- A customer shows limited knowledge of virtual currency despite engagement in virtual currency transactions or activity, which may indicate a victim of a scam.
- A customer declines requests for "know your customer" documents or inquiries regarding sources of funds.

- A customer purchases large amounts of virtual currency not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a victim of a scam.
- A common wallet address is shared between accounts identified as belonging to two different customers.
- Deposits into an account or virtual currency address significantly higher than ordinary with an unknown source of funds, followed by conversion to currency of legal tender, which may indicate theft of funds.
- Multiple changes to email address and other contact information for an account or customer which may indicate an account takeover against a customer.
- Use of language in virtual currency message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.

10 Appendix: Unusual Transaction Form (Internal)

This form should be completed if you have reasonable grounds to suspect that a customer's activities are related to money laundering or terrorist financing activities. This form should be submitted to the Compliance Officer on the same day that it is completed.

Do not let the customer know that you are filling out this form or discuss its contents with anyone other than the Compliance Officer or a designate.

Your Name & Location (PALMEX Office Location):

_____

Customer's Name:

_____

Were you able to identify the customer?

If yes, please include the customer's identification information in the section below. If not, please explain why this was not possible (please use additional pages as needed):

_____

_____

_____

_____

Describe the customer's request or transaction, including whether the transaction was completed or not (please use additional pages as needed):

_____

_____

Describe in your own words what happened, and what made you suspicious. Please be as detailed as possible, and include facts about the customer's behavior, and any specific words or phrases that they used. Describe what you did and said, as well as how the customer responded. Please use additional pages as needed:

_____

_____

_____

_____

_____

_____

_____

Date:

_____

Time:

_____

Your Signature:

_____

10.1 Compliance Use Only

Date reviewed: _____

Reviewed By: _____

This transaction has been deemed suspicious: _____ Yes _____ No

Describe the rationale for the decision above (whether or not the transaction is deemed to be suspicious). Please use additional pages if required.

_____

_____

_____

_____

Describe any follow up actions (if applicable). For example, adjustments to the customer's risk rating, enhanced due diligence activities, etc.

_____

_____

_____