AML Policy

Last Updated October 25, 2025

Kraster Pay is committed to maintaining effective crime prevention and detection measures to assist law enforcement agencies in combating financial crime. The site has adopted a strict set of policies and procedures to fulfil the site's legal obligations under international anti-money laundering and anti-terrorism legislation.

1. Main Objectives

- Clients' identities are satisfactorily verified in accordance with the firm's risk based approach before Website does business with them.
- Website knows its clients and understands their reasons for doing business with us both at the client acceptance stage and throughout the business relationship.
- Our staff are trained and made aware of both their personal legal obligations and the legal obligations of Website.
- Our staff is trained to be vigilant for activities where there are reasonable grounds for suspicion that money laundering could be taking place and to make the reports to the Compliance Officer.
- Sufficient records are kept for the required period.
- We establish, maintain and implement appropriate procedures to achieve these objectives.

2. General Principles

Anti-Money Laundering Policy

Kraster Pay has implemented policies, procedures and controls designed to prevent criminals from using Website to launder the proceeds of crime. These policies and procedures are tailored to the risk posed to individual customers.

Customer Due Diligence ('CDD')

Kraster Pay has established customer due diligence procedures to identify the users of its services and, in respect of higher risk customers, the primary beneficial owners and origin of funds. These procedures include knowledge of the nature of our customers' business and vigilance for anomalous transactions.

In general, the CDD policy has been adopted by Website to successfully fulfil the following objectives:

- identification and verification of the applicant for business;
- identification and verification of the beneficial owner, where applicable;
- identification and verification when the applicant for business does not act as principal;
- obtaining information on the purpose and intended nature of the business relationship;
- conducting ongoing monitoring of the business relationship;
- establishing the source of wealth and source of funds;

-
-
  setting up of a customer acceptance policy and ensuring that the applicant for business meets the requirements set out in such policy;
  Website is strictly prohibited from keeping anonymous accounts or accounts in fictitious names.

Suspicious Transactions

Unexplained or anomalous transactions or activities suspected to be related to criminal activity should be reported immediately in writing to the Compliance Officer, who will determine whether the suspicion should be reported to Law Enforcement.

Training

All personnel must be informed of their individual and collective responsibilities and Website's anti- money laundering policies. Personnel are provided with training to enable them to understand the vulnerabilities of Website's business and to recognize and report suspicious activities.

Record-Keeping

The website keeps records of who has been trained and the time and form of the training sessions. We keep all records confirming the identity of our customers for at least 7 years after the end of the business relationship. We also keep records of any internal reports of suspicion made to the Compliance Officer.

3. Our Responsibilities

All money service businesses are required by International Law to:

- Develop a programme to ensure compliance with reporting, record keeping and customer identification requirements;
- Comply with customer identification rules and maintain specific records for specific transactions;
- Report suspicious transactions, large cash transactions and information related to terrorist property.

4. Risk based approach

What is risk? -Risk can be defined as the likelihood of an event and its consequences. In simple terms, risk can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result from such an occurrence. In the context of money laundering/terrorist financing (ML/TF), risk means:

- At the national level: ML/TF threats and vulnerabilities that jeopardise the integrity of the financial system.
- At the Company level: threats and vulnerabilities that put the Company at risk of being used to facilitate ML/TF.

•

All clients default to low risk, UNLESS risk factors are present such as; Automatic high- risk characteristics – if any of the flags below are present the client is high risk.

Politically exposed person.

- A client where a suspicious transaction, terrorist financing report has been filed.
- A client who is an identified terrorist.
- A client for whom we are unable to obtain beneficial ownership information.
- A client from high-risk country.

Client characteristics, product, service, delivery channel:

- Politically exposed person, head of international organization and close associates;
- Unknown source of funds;
- Large transaction (ETF) orders from/to high-risk foreign jurisdictions;
- Third party involvement without reasonable justification;
- Occupation – High-risk occupations (e.g., cash intensive businesses, offshore business, business in high-risk countries, online gambling);
- Client's business structure or transactions seems unusually complex;
- Non face-to-face client identification without justifiable reason.

Geography:

- Client resides outside local or normal client area;
- Client resides in known crime area;
- Client has offshore business activities, client connections to high-risk countries.

Other suspicious transaction indicators:

- Volume/timing/complexity of transactions inconsistent with the client's personal/business activity and/or purpose of the services/account;
- Value of deposits/transfers inconsistent with occupation or source of funds;
- Presence of any suspicious transaction indicators outlined in Part A "Background information" section.

5. Indicators of suspicious transactions or potential high-risk clients

The following are examples of some general and industry-specific indicators that may give you reasonable grounds to suspect that a transaction involves money laundering or terrorist financing. The presence of one or more of these factors does not mean that the transaction is suspicious and should be reported to a regulator, but it does indicate that a more in-depth examination is required.

General indicators. The following are a few examples of general indicators that might lead us to suspect that a transaction is related to a money laundering or terrorist activity financing offence. It will not be just one of these factors alone, but a combination of several factors in conjunction with what is normal and reasonable in the circumstances of the transaction or attempted transaction.

- Client admits to or makes statements about involvement in criminal activities;

-
-
- Client refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify;
- Client produces seemingly false documentation that appears to be counterfeited, altered or inaccurate;
  Client appears to have accounts with several financial institutions in one area for no apparent reason;
  Client repeatedly uses an address but frequently changes the name involved;
- Client shows uncommon curiosity about internal controls and systems;
- Client presents confusing details about the transaction;
- Client makes inquiries that would indicate a desire to avoid reporting;
- Client is involved in unusual activity for that individual or business;
- Client presents confusing details about the transaction or knows few details about its purpose;
- Client seems very familiar with money laundering or terrorist activity financing issues; • Client refuses to produce personal identification documents;
- Client frequently travels to a high-risk country.

Industry specific examples

- Client requests a transaction at a foreign exchange rate that exceeds the posted rate.
- Client wants to pay transaction fees that exceed the posted fees.
- Client exchanges currency and requests the largest possible denomination bills in a foreign currency.
- Client knows little about address and contact details for payee, is reluctant to disclose this information, or requests a bearer instrument.
- Client wants a cheque issued in the same currency to replace the one being cashed.
- Client wants cash converted to a cheque and you are not normally involved in issuing cheques.
- Client wants to exchange cash for numerous postal money orders in small amounts for numerous other parties.
- Client enters into transactions with counter parties in locations that are unusual for the client.
- Client instructs that funds are to be picked up by a third party on behalf of the payee.
- Client makes large purchases of traveler’s cheques not consistent with known travel plans.
- Client makes purchases of money orders in large volumes.

6. Data request

To mitigate the risks associated with money laundering and terrorist financing, we strictly do not accept or send payments to third parties (unidentified). Each customer may only send and receive payments through their own accounts, including electronic payment system accounts, bank accounts, and credit and debit cards.

In accordance with KYC ("Know Your Customer") policy, our employees are authorised to carry out customer verification. In this case, the customer is required to provide the following information.

-

- Information about the services for which the funds were received;
- A screenshot confirming the receipt and withdrawal of funds;
- Additional information that may be requested;

We reserve the right to refuse to process a transaction at any stage if it is suspected to involve money laundering or other criminal activity.

•

7. Restricted Activities and Clients

To mitigate and control ML risk related to client, Website does not provide services and refuse account opening for the following clients with unacceptable risk level:

Private individuals with the following personal and/or business activity

- information of the negative nature is available about the client, which indicates their possible relation to the proceeds of crime or laundering or terrorism if the information is received from trusted sources, such as World Check and public authorities websites;
- client funds have previously been frozen or arrested in connection with suspected criminal activity;
- reinsurance services, when the service provider is not properly licensed and there is a lack of supervision of the service provider;
- the client is trying to avoid the provision of information or is trying to hide their economic activity;
- trafficking in arms and ammunition;
- economic activity, that has to be registered in the legal entity form;
- unlicensed foreign currency exchange intermediary services (such as forex dealers, Binary options), as well as other unlicensed investment services;
- client's transactions or payments are complex, unusually large for the customer's economic or personal activity or are unclear in terms of their legal and economic objective;
- Escort services organisation / activities and / or distribution of erotic / pornographic videos and pictures and other related services;
- Cash collection services;
- Debt recovery services provider;
- Drugs, vitamins and nutritional supplements distribution;
- Detective services provider;
- Direct marketing services provider;
- Pyramid schemes;
- Telemarketing;
- Pawnshop services provider;
- Auctions and related services provider;
- Tobacco and alcohol products distribution.

Legal persons with the following personal and/or business activity:

- the client is trying to avoid the provision of information or is trying to hide their economic activity;
- information of the negative nature is available about the client, which indicates their possible relation to the proceeds of crime or laundering or terrorism if the information is received from trusted sources, such as World Check and public authorities websites;
- client funds have previously been frozen or arrested in connection with suspected criminal activity;
- reinsurance services, when the service provider is not properly licensed and there is a lack of supervision of the service provider;
- trafficking in arms and ammunition;

- investment services and investment ancillary services, when the service provider is not properly licensed in the European Economic Area or in another country, where the legislative requirements of anti-money laundering and terrorism financing are equivalent to the European Union legislation;
  legal entities, which are recognized as shell companies;
- unlicensed gambling services organization;
- the reason for the client's legal entity's establishment is unclear and the client 6 of the legal and the information about the client's economic objectives are vague and ambiguous;
- unlicensed foreign currency exchange intermediary services (such as forex dealers, Binary options);
- client's transactions or payments are complex, unusually large for the customer's economic or personal activity or are unclear in terms of their legal and economic objective;
- Escort services organisation / activities and / or distribution of erotic / pornographic videos and pictures and other related services;
- Cash collection services;
- Debt recovery services provider;
- Drugs, vitamins and nutritional supplements distribution;
- Detective services provider;
- Direct marketing services provider;
- Pyramid schemes;
- Telemarketing;
- Pawnshop services provider;
- Auctions and related services provider; • Tobacco and alcohol products distribution.

In accordance with the internal AML/CFT procedure, Website has customers in two risk categories - low-risk and high-risk customers. For high-risk customers, EDD should be carried out.

A high-risk client is someone:

- who is politically exposed person, his/her family member or a close associate;
- with whom financial claims and either arising out of or related obligations exceed 10 000 $ CAD;

8. Sanctions

Website is prohibited from transacting with individuals, companies and countries that are on prescribed Sanctions lists. Website will therefore screen against the relevant sanctions lists in the jurisdictions in which we operate.

Website has no AML Risk Appetite for establishing or maintaining a customer or a counterparty relationship with a natural person or legal entity designated on any of the below lists or where otherwise prohibited by applicable law or regulation:

- sanction lists administered by the United States Office of Foreign Assets Control (OFAC),
- the United Nations Security Council Sanctions List (UN);

-
- the Consolidated List of European Union Financial Sanctions (EU); • including the List of Specially Designated Nationals and Blocked Persons;
- any other sanctions list.

In addition, Website pays particular attention to entities from countries which are on the list of noncooperative countries and territories drawn up by the Financial Action Task Force (FATF) and to monetary operations or transactions performed by or on behalf of them.

---

9. List of Non-serviced Countries

Website does not open accounts and does not provide services to clients from the following countries:

- Islamic Republic of Afghanistan (AF)
- Republic of Angola (AO)
- Belarus (BY)
- Bosnia and Herzegovina (BA)
- Republic of Botswana (BG)
- Commonwealth of The Bahamas (BS)
- Kingdom of Cambodia (CM)
- Republic of Burundi (BI)
- Democratic Republic of the Congo (CD)
- Central African Republic (CF)
- Republic of the Congo (CG)
- People's Democratic Republic of Algeria (DZ)
- Republic of Ecuador (EC)
- State of Eritrea (ER)
- Federal Democratic Republic of Ethiopia (ET)
- Republic of Ghana (GH)
- Republic of Guinea (GN)
- Republic of Guinea-Bissau (GW)
- Co-operative Republic of Guyana (GY)
- Republic of Haiti (HT)
- Republic of Iraq (IQ)
- Islamic Republic of Iran (IR)
- Japan (JP)
- Republic of Kenya (KE)
- Democratic People's Republic of Korea (KP)
- Lebanese Republic (LB)
- Republic of Liberia (LR)
- Libya (LY)
- Republic of the Union of Myanmar (MM)
- Federal Republic of Nigeria (NG)
- Islamic Republic of Pakistan (PK)
- Republic of Serbia (RS)
- Russian Federation (RU)
- Republic of the Sudan (SD)
- Democratic Socialist Republic of Sri Lanka (SL)

- Federal Republic of Somalia (SO)
- Republic of South Sudan (SS)
- Syrian Arab Republic (SY)
- Republic of Tunisia (TN)
- Republic of Trinidad and Tobago (TT)
- Ukraine (UKR)
- Republic of Uganda (UG)

- United States of America (US)
- Republic of Vanuatu (VU)
- Bolivarian Republic of Venezuela (VE)
- Republic of Yemen (YE)
- Republic of Zimbabwe (ZW)

10. Monitoring for suspicious activity

Website AML policy includes customer's and beneficial owner's due diligence and ongoing AML monitoring and AML reporting policies. At various points in time, Website may request information regarding the transactions carried out through the customer's account opened at Website and the parties of the respective payment. If the customer may not respond sufficiently or within a timely manner Website also reserves the right to reject any respective payments subject to the requirements of the applicable AML laws and regulations.