AML POLICY

This policy is applicable to all officers, employees, appointed producers, and the products and services of Millance Ltd. Every business unit and location within Millance Ltd must establish risk-based procedures to identify, prevent, and report money laundering activities. These measures should be documented and maintained. The AML Compliance Committee holds the responsibility for initiating Suspicious Activity Reports (SARs) and submitting them to the relevant law enforcement or regulatory authorities.

Any inquiries from these agencies must be directed to the AML Compliance Committee.

Millance Ltd is committed to combating money laundering and any activities that contribute to financing terrorism or other criminal actions. Adhering to applicable laws is obligatory for all officers, employees, and appointed producers to ensure the company's products and services are not misused for money laundering purposes.

For compliance-related matters, please reach out to compliance@millance.com.

Money laundering refers to the process of disguising the origins of illicitly acquired funds to make them appear as though they come from lawful sources.

Money Laundering

Money laundering is the process of transforming illegally acquired money or assets (criminal property) into seemingly legitimate funds or assets, disguising their illicit origins. Criminal property can take various forms, including cash, securities, physical goods, or intangible assets. This also encompasses funds used to finance terrorist activities.

Money Laundering Activities Include:

- Obtaining, utilizing, or holding criminal property.
- Managing funds derived from crimes such as theft, fraud, and tax evasion.
- Knowingly associating with criminal or terrorist property.

- Facilitating the laundering of criminal or terrorist property.
- Using crime proceeds for financial investments.
- Acquiring property or assets using crime proceeds.
- Transferring illicitly obtained property

Money laundering techniques range from buying and selling luxury goods to intricate legal transactions. While it often begins with cash, any asset acquired through illegal means can be laundered. Failing to report known or suspected laundering activities may result in involvement in the crime.

The money laundering process follows three stages:

Placement: Illicit proceeds are first introduced into the financial system, typically through deposits into bank accounts.

Layering: The funds are transferred through multiple transactions to disguise their origins, making them appear lawful.

Integration: After laundering, the money is reintegrated into the economy as seemingly legitimate funds, enabling criminals to use it without suspicion.

No financial industry is exempt from these activities. Companies must evaluate the money laundering risks linked to their products and services to implement effective preventive measures.

Counter Terrorist Financing (CTF):

Terrorist financing occurs when lawful businesses and individuals supply funds to support terrorist groups or activities for ideological, political, or other motives. Companies must verify that their customers are not linked to terrorist organizations and that their services are not used to finance such entities. Unlike money laundering, terrorist financing may not always involve illegally obtained funds but instead focuses on disguising the source or intended use of the money, which will eventually be used for criminal purposes.

Risk-Based Approach

The extent of due diligence required for anti-money laundering measures within a firm should follow a risk-based approach. This involves allocating resources for due diligence based on the risk level of each relationship. Important factors to consider

include:

Customer Risk

Different customer profiles present varying degrees of risk. Conducting thorough Know Your Customer (KYC) checks helps determine this risk. For example, individuals nearing retirement who make small, consistent savings contributions typically pose a lower risk compared to middle-aged individuals making large, irregular payments that do not align with their financial profile. As a result, the latter requires more stringent due diligence. Additionally, corporate structures can present higher risks due to their potential use in concealing fund sources through layering transactions. This enables firms to categorize clients into different risk levels based on their profiles.

Product Risk

Product risk refers to the likelihood of a financial product or service being exploited for money laundering purposes. The Joint Money Laundering Steering Group (JMLSG) categorizes products into three risk levels:

Low Risk – Includes products like pure protection contracts, which are less susceptible to misuse.

Moderate Risk – Applies to products with a medium level of risk.

High Risk – Covers products such as unit trust investments, which are more complex and have a greater potential for misuse.

Additionally, the sales process influences risk levels. Transactions involving advisory services, where KYC procedures are followed, generally present lower risks compared to execution-only transactions, where less customer information is gathered.

Country Risk

A client's geographic location or the origin of their business activities also impacts risk levels, as different countries pose varying degrees of risk. Firms should

consider these four key risk factors to determine the appropriate level of due diligence, both at the initial stage and on an ongoing basis.

Customer Identification Program

Millance Ltd has established a Customer Identification Program (CIP). As part of this program, the company will inform customers that their identification details are required, collect necessary identification information from each individual, and maintain records of the collected data, along with the verification methods and outcomes.

Customer Notification

Millance Ltd will notify customers that their identity verification is mandatory in accordance with applicable legal requirements.

Know Your Customers

When initiating a business relationship, the company must understand the nature of the client's intended business activities to establish what constitutes normal behavior. Once the relationship is formed, ongoing transactions can be monitored against expected activity patterns. Any unusual or unexplained activity should be investigated to determine if there are suspicions of money laundering or terrorist financing. Information such as the client's income, occupation, source of wealth, trading habits, and the economic purpose of transactions is typically gathered during the advisory process. Additionally, personal details like nationality, date of birth, and residential address are collected at the start of the relationship. The financial crime risks, including anti-money laundering (AML) and counter-terrorist financing (CTF), should be assessed. For high-risk transactions, verifying the provided information may be required.

Source of Funds

During a transaction, it is essential to identify and document the source of funds—how the payment is made, its origin, and the individual making it. This is usually done by retaining copies of cheques or direct debit mandates in the client’s file.

Identification

The standard identification requirements for private individuals depend on their circumstances and the type of financial product involved. The risk level of the product—whether reduced, intermediate, or increased—plays a key role in determining identification requirements. For reduced and intermediate-risk products, the following details are typically required:

- Full Name
- Residential Address

Verification

The verification of obtained information must be based on reliable and independent sources, which may include customer-provided documents, electronic records maintained by the firm, or a combination of both. When transactions occur in person, firms should examine the original documents used for verification. To ensure a high level of confidence, documentary evidence is typically issued by a government department, agency, or court, as these entities are more likely to have already verified an individual's identity and details. In cases where such documents are unavailable, other forms of evidence may still be acceptable, provided they offer reasonable assurance of the customer's identity. However, firms should carefully assess these alternatives in relation to the associated risks.

When verifying identity through documents, the following should be used:
A government-issued document that includes:

- The customer's full name
- Their residential address

Photographic Government-Issued Identity Documents:

- Valid passport
- National identity card

Alternatively, verification can be done using a non-photographic government-issued document that includes the customer's full name, accompanied by a secondary document containing:

- The customer’s full name
- Their residential address

Proof of Address

For standard identification verification, the following documents are considered acceptable:

- Recent bank statements or credit/debit card statements from a regulated financial institution (must be original, not printed from the internet, and dated within the last six months).
- Utility bills (excluding mobile phone bills, must be original, not printed from the internet, and not older than six months).

For products classified as higher risk, in addition to standard identification details, the following Know Your Customer (KYC) information should also be collected and documented:

- Employment and income details.
- Source of wealth (i.e., the origin of the funds involved in the transaction).

Monitoring and Reporting

Millance Ltd will conduct transaction-based monitoring within its relevant business units. This process will specifically focus on transactions of $5,000 or more, along with any transactions that appear suspicious or deviate from usual activity. All observations and reports will be properly documented.

Suspicious Activity

Indicators of suspicious activity, commonly known as "red flags," may suggest potential money laundering. If such a red flag is identified, further due diligence will be conducted before proceeding with the transaction. If no reasonable explanation is found, the activity will be reported to the AML Compliance Committee.

Know Your Customer – The Basis for Detecting Suspicious Activity

A transaction may be deemed suspicious if it significantly differs from a customer's established, legitimate business or personal activities or deviates from their typical transaction patterns. A thorough understanding of the customer's business is essential to detect any unusual activities or transaction patterns.

Reporting a Suspicion

- If there is any suspicion that a client or their representative is engaging in a transaction involving criminal proceeds, it must be reported in writing as soon as possible.
- Internal reports must be submitted even if no business has been conducted or is expected to take place.

Investigation

Once the AML Compliance Committee is notified, an investigation will be conducted to determine whether a report should be submitted to the relevant law enforcement or regulatory agencies. This process will involve reviewing all available information, including payment history, birth dates, and addresses. If the findings justify further action, a recommendation will be made to the AML Compliance Committee to file a Suspicious Activity Report (SAR) with the appropriate agency. The AML Compliance Committee is responsible for submitting any necessary reports or notifications.

All investigation results will remain confidential and shared only with those who have a legitimate need to know. Under no circumstances should any officer, employee, or appointed agent disclose or discuss AML concerns, investigations,

notices, or SAR filings with the individuals involved or any unauthorized persons, including their family members.

Freezing of Accounts

If it is determined that the funds in an account are derived from criminal activity or fraudulent transactions, the account must be frozen. Additionally, if there is credible evidence indicating the account holder's involvement in fraudulent activity, their account should also be frozen.