AML POLICY

This policy applies to all officers, employees, appointed producers, and Milliva Ltd's products and services. Every business unit and location within Milliva Ltd is required to implement risk based procedures to prevent, detect, and report money laundering activities. These efforts must be documented and retained.

The AML Compliance Committee is responsible for initiating Suspicious Activity Reports (SARs) and reporting to the appropriate law enforcement or regulatory agencies. Any contact from these agencies must be directed to the AML Compliance Committee.

Milliva Ltd is dedicated to preventing money laundering and activities that facilitate funding terrorist or criminal activities. Compliance with applicable laws is mandatory for all officers, employees, and appointed producers to prevent the misuse of the company's products and services for money laundering.

Money laundering involves concealing the origins of criminally obtained proceeds, so they appear to be from legitimate sources.

Money Laundering

Money laundering involves converting illegally obtained money or assets (criminal property) into "clean" money or assets that appear legitimate, hiding their criminal origins. Criminal property can include any form of value, such as money, securities, tangible items, or intangible assets. This also extends to funds used for terrorist activities.

Money laundering activity includes:

- Acquiring, using, or possessing criminal property
- Handling proceeds from crimes like theft, fraud, and tax evasion
- Being knowingly involved with criminal or terrorist property
- Arranging to launder criminal or terrorist property
- Investing crime proceeds in financial products
- Investing crime proceeds through property or asset acquisition
- Transferring criminal property

Money laundering methods vary, from purchasing and reselling luxury items to complex legitimate operations. It typically starts with cash, but any property obtained through criminal activity can be laundered. Knowing or suspecting this and not reporting it implicates you in the process.

The money laundering process follows three stages:

1. **Placement:** Initial proceeds from illegal activities are deposited into financial institutions, such as bank accounts.
2. **Layering:** Funds are moved through various transactions to obscure their origins, making the money appear legitimate.
3. **Integration:** Once laundered, the funds are reintroduced into the economy as seemingly clean money, allowing criminals to use them freely.

No financial sector is immune to these activities. Firms must assess the money laundering risks associated with their products and services to mitigate these threats effectively.

Counter Terrorist Financing (CTF)

Terrorist financing involves legitimate businesses and individuals providing funds to support terrorist activities or organizations for ideological, political, or other reasons. Firms must ensure that their customers are not terrorist organizations and that their services are not used to fund such entities. Unlike money laundering, terrorist financing may not involve proceeds from criminal activities but focuses on concealing the origins or intended uses of the funds, which will ultimately be used for criminal purposes.

Risk Based Approach

The level of due diligence required for anti-money laundering procedures within a firm should be based on a risk-based approach. This means allocating resources for due diligence in proportion to the risk level of each relationship. Key areas to consider include:

Customer Risk

Different customer profiles carry varying levels of risk. An essential Know Your Customer (KYC) check helps establish this risk. For instance, near-retired individuals making small, regular

savings contributions pose a lower risk than middle-aged individuals making irregular, large payments that don't match their financial profile. Thus, due diligence for the latter is more intensive. Corporate structures can pose higher risks due to their potential use to conceal fund sources in layering transactions. This allows for categorizing clients into different risk bands based on their profiles.

Product Risk

Product risk refers to the potential for a financial product or service to be used for money laundering. The Joint Money Laundering Steering Group (JMLSG) classifies these products into three risk levels:

1. **Reduced Risk:** Typically includes products like pure protection contracts, which generally pose a lower risk of misuse.
2. **Intermediate Risk:** Covers products with moderate risk potential.
3. **Increased Risk:** Includes products such as investments in unit trusts, which have a higher risk due to their complexity and potential for misuse.

The risk classification also takes into account the sales process. Transactions conducted on an advisory basis, with Know Your Customer (KYC) procedures, generally carry less risk compared to execution-only transactions, where less customer information is obtained.

Country Risk

The geographic location of a client or the origin of their business activity carries its own risk, as different countries have varying levels of risk associated with them. A firm should use these four risk areas to assess the level of due diligence required initially and continuously.

Customer identification program

Milliva Ltd has implemented a Customer Identification Program (CIP). The company will notify customers that identification information will be requested, collect essential customer identification details from each individual, and document both the information collected and the methods and results of its verification.

Notice to customers

Milliva Ltd will inform customers that it is requesting information to verify their identities, in compliance with applicable laws.

Know Your customers

When establishing a business relationship, the company needs to understand the nature of the business a client intends to conduct to define what constitutes normal activity for that client. Once the business relationship is established, ongoing transactions can be compared against the expected activity pattern. Unusual or unexplained activity can then be investigated to assess whether there may be a suspicion 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 collected as part of providing advice. Personal details such as nationality, date of birth, and residential address are also gathered at the outset of the relationship. This information regarding financial crime risks should be evaluated, including anti-money laundering (AML) and counter-terrorist financing (CTF). For high-risk transactions, it may be necessary to verify the information provided by the client.

Source of Funds

When a transaction occurs, it is crucial to determine and document the source of funds—how the payment is being made, from where it originates, and by whom. This is typically accomplished by retaining a copy of the cheque or direct debit mandate in the client file.

Identification

The standard identification requirements for private individuals are generally based on the customer's circumstances and the type of product involved, with the risk associated with the product—whether it is reduced, intermediate, or increased—playing a pivotal role. For reduced risk and intermediate-risk products, the following information is typically required for identification purposes:

- Full Name
- Residential Address

Verification

Verification of the information obtained must rely on reliable and independent sources, which can include documents provided by the customer, electronic records from the firm, or a combination of both. When business is conducted in person, firms should review the original documents used for verification.

For documentary evidence to provide a high level of confidence, it is typically issued by a government department, agency, or court, as these authorities are more likely to have verified the identity and characteristics of the individuals. In cases where such documents are not available, other forms of evidence may still provide reasonable confidence in the customer's identity. However, firms should carefully consider these alternative forms of evidence in relation to the associated risks.

If the identity is to be verified from documents, this should be based on:

Either a government issued document which incorporates:

- The customer's full name, and
- Their residential address

Photographic Government Issued Identity Documents

- Valid passport
- National Identity card

Alternatively, this can be done by a non-photographic government issued document which incorporates the customer's full name, supported by a second document, which incorporates:

- The customer's full name, and
- Their residential address

Evidence of Address

For standard identification purposes, the following documents are acceptable:

- Current bank statements or credit/debit card statements from a regulated financial institution (not printed from the internet and not older than six months).
- Utility bills (excluding mobile phone bills, not printed from the internet, and not older than six months).

For products with an increased risk level, in addition to the standard information, the following Know Your Customer (KYC) details should also be obtained and recorded:

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

Monitoring and reporting

Transaction-based monitoring will be conducted within the relevant business units of Milliva Ltd. This monitoring will focus on transactions of $5,000 or more, as well as any transactions that raise suspicion of unusual activity. All findings and reports will be documented accordingly.

Suspicious activity

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

Know Your Customer – The Foundation for Identifying Suspicious Activity

A transaction is often considered suspicious if it deviates from a customer's known, legitimate business or personal activities or from the typical transactions expected for that customer. Therefore, the key to recognizing such transactions is thoroughly understanding the customer's business to identify any unusual transactions or patterns.

Reporting a Suspicion

- If there is any suspicion that a client, or anyone on their behalf, is involved in a transaction related to the proceeds of crime, it must be reported in writing as soon as practicable.
- Internal reports must be submitted regardless of whether any business was conducted or is planned to be conducted.

Investigation

Upon notification to the AML Compliance Committee an investigation will be commenced to determine if a report should be made to the appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file the SAR with the appropriate law enforcement or Upon notification to the AML Compliance Committee, an investigation will be initiated to determine whether a report should be made to the relevant law enforcement or regulatory agencies. This investigation will involve reviewing all available information, including payment history, birth dates, and addresses. If the investigation's findings justify it, 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 any notifications or filings with law enforcement or regulatory agencies.

Results of the investigation will be kept confidential and discussed only with individuals who have a legitimate need to know. Under no circumstances should any officer, employee, or appointed agent disclose or discuss any AML concerns, investigations, notices, or SAR filings with the individuals involved or any other person, including their family members.

Freezing of Accounts

If it is confirmed that the funds in an account originate from criminal activity or fraudulent instructions, the account must be frozen. Moreover, if there is evidence suggesting that the account holder is involved in the fraudulent activity, the account should also be frozen.