Cloud Nalu Anti Money Laundering (AML) and Know Your Customer Policy (KYC)

Overview

AML laws are part of a broader United States government initiative to tackle criminals that use financial institutions to conceal their activity. The goal of AML is to prevent criminal activity such as terrorism, tax evasion and drug trafficking, where illicit funds are often funnelled through legal channels to obscure illegal activity.

AML regulations were implemented worldwide in 1989 with the creation of a Financial Action Task Force to set international standards for fighting against money laundering. As part of compliance with these regulations, financial institutions are obliged to monitor suspicious activity, and sometimes verify the origin of funds on behalf of the United States government.

KYC laws are a subset of AML. These laws involve verifying the identity of an institution's customers. In recent times these laws have been made significantly stricter as a means of combating terrorist financing.

Cloud Nalu policy is to prohibit and vigorously prevent money laundering and any activity that enables money laundering or the finance of terrorist or criminal activities by observing all applicable requirements under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act), and the Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF Rules) and its implementing regulations.

Money laundering is ordinarily defined as engaging in acts intended to conceal or disguise the real origins of criminally resultant proceeds so that the proceeds appear to have resulted from genuine origins or constitute genuine assets. Usually, money laundering occurs in three stages. Money first comes into the financial structure at the "placement" stage, where the cash created from criminal activities is changed into monetary instruments, such as money orders or traveller's checks, or deposited into accounts at financial establishments. At the "layering" stage, the funds are moved into other accounts or other financial establishments to further separate the money from its criminal origin. At the "integration" stage, the funds are reinstated into the economy and used to obtain legitimate assets or to fund other criminal activities or genuine businesses.

Terrorist bankrolling may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Genuine sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to benevolent donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the incentive differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to

launder funds. Backing for terrorist attacks does not always require large sums of cash and the related dealings may not be intricate.

Our AML strategies, measures and core controls are intended to ensure compliance with all applicable United States regulations and rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

1. Our Measures on Anti-Money Laundering

We conduct a strict verification process for customer identification including the capturing of:

- the name, address, birth date, valid form of Government ID (natural persons),

- the name and the location of the head office or principal office, description of the business and required details of the substantial beneficial owner, as per requirements set out in the legislation (businesses).

  More details of the verification process, they are set out in Clause 6. Furthermore, a risk-based approach is considered and a strict customer due diligence process is implemented to any high- risk transactions. Also, Cloud Nalu conducts transaction screening for unfair transactions such as market manipulation, insider trading, transactions using fictitious names. If a potential unfair transaction is detected through the transaction screening process, we will take appropriate steps to alert the customer, as necessary.

  AML documents such as verification process of customer identification and transaction screening is maintained in line with United States laws, policies and procedures.

  The Cloud Nalu Customer Acceptance Policy (CAP) reflects the international standard, namely to accept only those clients whose identity is established by conducting due diligence appropriate to the risk profile of the client. Where the investor is a new investor, account must be opened only after ensuring that pre account opening KYC documentation and procedures are conducted.

2. KYC & Verification Procedures

One of the standards for preventing illegal activity is customer due diligence (“CDD”). According to CDD, Cloud Nalu establishes its own verification procedures within the standards of anti-money laundering and KYC frameworks.

Cloud Nalu KYC policies incorporate the following four key elements:

- Customer Acceptance Policy;
- Customer Identification Procedures;
- Monitoring of Transactions; and.
- Risk management.

a. Identity Verification

Cloud Nalu's identity verification procedure requires the User to provide Cloud Nalu with reliable, independent source documents, data or information (e.g., state or national ID, passport, bank statement, utility bill). For such purposes Cloud Nalu reserves the right to collect User's identification information for the AML/KYC Policy purposes.

Cloud Nalu will take steps to confirm the authenticity of documents and information provided by the Users. All legal procedures for checking ID information will be used and Cloud Nalu reserves the right to scrutinize certain Users who have been determined to be risky or suspicious.

Cloud Nalu reserves the right to verify User's identity in an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular User). In addition, Cloud Nalu reserves the right to request up-to-date documents from the Users, even though they have passed identity verification in the past. User's identification information will be collected, stored, shared and protected strictly in accordance with the Cloud Nalu's Privacy Policy, applicable laws and regulations. After the User's ID has been substantiated, Cloud Nalu is able to remove itself from possible legal liability in circumstances where its Services are used to conduct illegal activity.

Compliance Officer

The Compliance Officer is the individual, properly authorized by Cloud Nalu, whose duty is to ensure the effective execution and enforcement of the AML/KYC Policy. It is the Compliance Officer's duty to oversee all aspects of Cloud Nalu's anti-money laundering and counter-terrorist financing, including but not limited to everyday

- Collecting Users' identification information
- Creating and updating internal procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations.
- Monitoring transactions and investigating any significant deviations from normal activity.

- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and log.
- Updating risk assessment regularly.
- Providing law enforcement with information as required under the applicable laws and regulations.
- The Compliance Officer is permitted to cooperate with law enforcement involved in stoppage of money laundering, terrorist financing and other illegal activity.
- Monitoring Transactions
  Users are identified not only by authenticating their ID but, more significantly, by scrutinizing their transactional arrangements. Cloud Nalu relies on data analysis as a risk-assessment and suspicion detection tool. Cloud Nalu does a selection of compliance-related responsibilities, comprising capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include
- Checking Users against known “black lists”, aggregating transfers by multiple data points, placing Users on watch and service rejection lists, opening cases for examination where needed, sending company memoranda and completing statutory reports, if applicable;
    - Case and document management. With regard to the AML/KYC Policy, Cloud Nalu will monitor all transactions and it reserves the right to:
        - make sure that transactions of doubtful nature are informed to proper law enforcement via the Compliance Officer;
        - demand the User to provide any extra facts and documents in case of doubtful transactions;
            - suspend or terminate User’s Account when Cloud Nalu has reasonable suspicion that such User engaged in illegal activity.

This list is not comprehensive and the Compliance Officer will monitor Users’ transactions on a day-to-day basis in order to decide whether transactions are to be reported and treated as suspicious or not.

Risk Assessment

Cloud Nalu, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By implementing a risk-based method, Cloud Nalu is able to make sure that procedures to stop or lessen money laundering and terrorist financing are appropriate to the identified risks. This will allow resources to be apportioned in the most effectual ways. The

principle is that resources should be directed in accord with importance so that the greatest risks (if any) receive the main attention.

3. Giving AML Information to Law Enforcement Agencies

Cloud Nalu will respond to any lawful request concerning accounts and transactions by complying with such requests in a timely manner, including searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in any request.

We will not disclose the fact that there has been such a request or whether information has been obtained from us, except to the extent necessary to comply with the law. We will review, maintain and implement procedures to protect the security and confidentiality of requests from such agencies with regard to the protection of customers' non-public information.

4. Customer Identification Program

In addition to the information we need to collect under KYC requirements, Cloud Nalu has established, documented and maintained a written Customer Identification Program (CIP). We will collect certain minimum customer ID information from each customer who opens an account; utilize risk-based procedures to verify the identity of each customer who opens an account; record customer identification information and the authentication methods and results; provide the required adequate CIP notice to customers that we will seek ID information to validate their ID's; and match customer ID information with government-provided lists of suspected terrorists.

5. Required Customer Information

Prior to completing any fiat transaction, Cloud Nalu will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

- The Name;
- date of birth (for an Individual);
- an address, which will be a residential or business street address (for an individual), or residential or business street address of next of kin or another contact individual (for a person without a residential or business street address), or a principal place of business, local office, or other physical location (for a

person other than an individual); and

- an identification number, which will be a taxpayer identification number, or one or more of the following: a taxpayer identification number, passport number and country of issuance, Medicare number, details of other government-issued document verifying nationality or residence and showing a photograph or other similar safeguard.

6. Customers Who Refuse to Provide Information

If a would-be or current customer either declines to provide the material defined above when demanded, or appears to have intentionally delivered deceptive information, we will not process any fiat transactions and, after bearing in mind the risks involved, consider closing any existing account. In either case, our Compliance Person will be informed so that we can decide whether we should report the situation to any government agency.

7. Verifying Information

Founded on the possibility, and to the extent judicious and realistic, we will ensure that we have a sound belief that we know the true identity of our customers by using risk-based processes to verify and document the accuracy of the information we get about our customers. We will analyse the material we obtain to decide whether the information is sufficient to form a realistic belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will validate customer ID through documentary means, non-documentary means or both. We will use documents to validate customer identity when appropriate documents are available. In light of the amplified occurrences of ID fraud, we will complement the use of documentary evidence by using the non-documentary means defined below whenever necessary. We may also use non-documentary methods, if we are still uncertain about whether we know the true ID of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, post code, telephone number, date of birth and Medicare number, allowing us to determine that we have a reasonable belief that we know the true identity of the customer. The information provided needs to be logical and not contain inconsistencies to avoid any adverse outcome.

Proper documents for validating the identity of customers include, but are not limited to, those set out in Clause 6.

We are not obligated to take steps to decide whether the document that the customer has provided to us for ID verification has been validly issued and we may be dependent on a

government-issued identification as verification of a customer's identity. If, however, we note that the document shows some apparent form of fraud, we must consider that factor in determining if we can form a reasonable belief that we know the customer's true identity.

8. The following non-documentary methods may be used to verify ID:

- Verifying the customer's ID through the appraisal of material provided by the customer with information obtained from a consumer reporting agency, public databank or other source;
- Checking references with other financial institutions; or
- Obtaining a financial statement.
- Non-documentary methods of verification will be used when:
- the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- Cloud Nalu is unfamiliar with the documents the customer presents for identification verification;
- the customer and Cloud Nalu do not have direct personal contact; and
- there are other circumstances that increase the risk that Cloud Nalu will be unable to verify
  the true identity of the customer through documentary means.
- The information will be verified within a realistic time before or after the account is opened. Contingent on the type of the account and requested transactions, we will refuse to complete a transaction before we have verified the information, or in some instances when we require more time, we may, pending authentication, limit the types of transactions or dollar amount of transactions. If we find suspicious information that points to possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with Cloud Nalu's AML Compliance Person, file a report with the appropriate government agency in accordance with applicable laws and regulations.

9. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we may do one or more of the following: (1) not approve an account; (2) close an account after attempts to verify a customer's identity fail; and (3) determine whether it is necessary to file a report in accordance with applicable laws and regulations.

10. Record Keeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will retain records having a depiction of any document that we relied on to verify a customer's ID, observing the type of document, any ID number contained in the document, the place of issue, and if any, the date of issue and expiry date. With regard to non- documentary authentication, we will keep documents that describe the procedures and the outcomes of any actions we took to validate the ID of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when validating the identifying information acquired. We will keep records of all identification information for five years after the account has been closed; we will keep records made about verification of the customer's identity for five years after the record is made.

11. Notice to Customers

We will provide notice to customers that Cloud Nalu is requesting information from them to verify their identities, as required by United States law. Notices will be by email unless a preferred contact address is indicated.

12. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business monitoring. This will be conducted through automated as well as manual methods. The customer risk profile will serve as a baseline for assessing potentially suspicious activity. The AML Compliance Person or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

13. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate government agency. If a customer appears on the Consolidated List, we will do likewise.

14. Red Flags

Indicators for likely money laundering or terrorist financing include, but are not limited to:

- Offers uncommon or doubtful identification documents that cannot be readily verified.
- Unwilling to provide comprehensive material about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Declines to identify a legitimate source for funds or information is false, misleading or substantially incorrect.
- Background is dubious or differs from business undertakings.
- Customer with no obvious motive for using Cloud Nalu's service.
- Efforts to Avoid Reporting and Recordkeeping.
- Unwilling to offer information needed to file reports or fails to continue with a transaction.
- Attempts to influence an employee not to file required reports or not to keep required records.
- "Configures" deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.
- Uncommon anxiety with Cloud Nalu's compliance with government reporting requirements and Cloud Nalu's AML policies.
- Activity Inconsistent with Business
- Transaction arrangements show an abrupt change inconsistent with typical activities.
- Uncommon transfers of funds without any obvious business purpose.
- Maintains multiple accounts.
- Seems to be acting as an agent for an undisclosed principal.
- Other Suspicious Customer Activity
- Unexplained high level of account activity.

- Law enforcement subpoenas.

- Payments to third-party without obvious association to customer.

15. Tax Policy

Cloud Nalu is committed to being a responsible tax payer in Australia as well as any other country in which we operate. We are committed to maintaining a tax compliance framework in order to file tax returns and pay our applicable taxes. In doing so we aim for conformity with tax laws, rules and regulations in each country and tax treaties. We do not arrange transactions and structures for tax avoidance or tax base erosion. There always must be reasonable business rationale or economic substance.

16. Commitment to Corporate Ethics

The management and employees of the Cloud Nalu pledge to abide by all United States and International laws as well as the rules stated in the *Code of Ethics* of Cloud Nalu. *(Click link for Code of Ethics)*

17. AML Recordkeeping

Cloud Nalu's AML Compliance Person and designee will be in control for ensuring that AML records are maintained properly and that required reports are filed as required. We will maintain documentation for at least six years.

18. Training Programs

We will advance constant employee training under the management of the AML Compliance Person and senior management. Cloud Nalu's training will occur as frequently as may be determined by management. It will be based on our size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law with the underpinning motive to remain compliant with applicable laws.

Our training will include, at a minimum: (1) methods to recognize red flags and indications of money laundering that arise during the course of the employees' duties; (2) action to be taken when the risk is recognized; (3) employees' roles in Cloud Nalu's compliance determinations and how to perform them; (4) Cloud Nalu's record retention policy; and (5) the corrective consequences (including civil and criminal penalties) for non-compliance.