KNOW YOUR CUSTOMER (K.Y.C)

A&N Loan Hub. Limited

Version 1.0

Document Classification: Policy

Table of Contents

PURPOSE

This policy outlines the process A&N Loan hub has instituted to prevent the abuse of its financial services and ensure its resources are not being used to support terrorist activities or for money laundering. The policy also seeks to highlight:

a) The company's "know your customer" process;
b) The policies and processes for on-boarding and training of new staff;
c) The disclosure and reporting processes; and
d) The document retention policies and procedures

POLICY SCOPE & APPLICABILITY

This policy is applicable to all employees, advisory bodies, governance members, investors (current and potential) and other decision making bodies.

DISTRIBUTION AND CONTROL OF THIS DOCUMENT

Read Access	–	All
Write Access	–	C.E.O., Audit Committee, Privacy Officer
Revision	–	Within five days from when changes occur
Review	–	At least once every year

DEFINITIONS:

1. Availability- refers to information being accessible and useable upon demand by an authorized entity.
2. Confidentiality- Information is not being made available or disclosed to unauthorized individuals.
3. Customer - refers to a person who establishes a business relationship with A&N Loan Hub (including a natural person, a legal person, an entity other than a legal person, or a trust).
4. Integrity- safeguarding the accuracy and competence of assets (information assets and others).

5. Money laundering - the process and/or methods by which the real identity of illegal or criminally obtained funds and or property are transformed through the use of formal financial and legitimate systems to ostensibly give the appearance of being derived through legal channels.
6. The Proceeds of Crime Act (POCA) - enacted in 2007 by the Government of Jamaica which repealed and replaced the Money Laundering Act (MLA) and the Drug Offences (Forfeiture of Proceeds) Acts.

   Under POCA, the definition of money laundering has been expanded to represent any activity involved with the dealing of criminal property. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct means any conduct constituting an offence in Jamaica, or if outside, conduct that would constitute a crime in Jamaica.
7. Terrorism Prevention Act (TPA) - is intended to substantially limit the ability of individuals, groups or organizations who are directly or indirectly involved in the perpetrating of acts of terror whether locally or in a foreign land from gaining access to and or to move financial assets and resources around the world in support of their terrorist activities.
8. Terrorism Financing - refers to the methods, activities or processes by which financial support and or financing is facilitated or provided to individual groups or organizations that are directly or indirectly involved or linked to acts of terrorism.

POLICY STATEMENT

A&N Loan Hub denounces all forms of terrorism and acts that result in the abuse of financial services. A&N Loan Hub will never knowingly support or tolerate any activity/conduct, individuals or entities associated with terrorism. We are committed to ensuring that we comply with all associated legislation, accountability frameworks, codes of practice, regulations and standards that are applicable to the operations and governance of the company.

MECHANISMS TO FIGHT TERRORISM

A&N's procedures place strong emphasis on "deter, detect, prevent." These procedures respond to and employ the following approaches to maintain this position:

1. Applies a "know your customer" principle and carries out in-depth reference checks on individuals with whom the company has or plans to have contractual arrangements with; to ensure these individuals are not associated with terrorism and do not appear on counter-terrorism lists through the use of an industry-standard auto-screening software.
2. Maintains comprehensive financial records which account for all expenditure and publishes annual financial statements with detailed breakdown of incomes and expenditures.
3. Conducts annual external audits of all expenses as well as external audits of specific projects.
4. Enforces a strict code of conduct among its staff and ensures training of all staff and partners on anti-diversion policies, procedures and practices.
5. Conducts in-depth due diligence integrity checks and monitoring of all staff, board members and advisors.
6. Has instituted transaction limits for all loan disbursement and repayments as follows:
    a. Repayment:
        i. The cash collection limit is JMD $50,000.00 per individual per branch daily. Persons who try to make payments above the limit, multiple payments a day or more than three payments at or close to the transaction limit will be flagged.
        ii. Once limit is reached this will be reported to the Compliance Officer (C.O.) and Hub Operations Manager immediately.
        iii. The company also reserves the right to stipulate that all future payments made by these individuals be done through the formal banking process.

b. Loan disbursement:

i. Follows a formal process where all loan disbursements are done through the company's bank account thus ensuring that no loan proceed is disbursed in cash. All persons must have a back account with a commercial bank (refer to KYC process).

ii. The company maintains a loan limit of JMD $1,000,000.00 which is determined by the clients eligibility to repay, collateral, debt to service ratio and other factors. Any loan over the limit has to be approved by the Hub Operations Manager and CEO even if all parameters are cleared for disbursement.

c. The C.O. will also conduct routine audits of the system to ensure 100% compliance with the repayment and disbursement process. All suspected breaches and irregularities will be reported within 8 hours of uncovering same.

EMPLOYEE BACKGROUND CHECKS

The following mandatory documents will be collected from all new hires prior to on-boarding:

a) Application forms
b) Current photograph (passport size)
c) All relevant Academic Certificates
d) Tax Registration Number (TRN)
e) Proof of residence
f) Written references
g) Information on next of kin
h) Sources of additional income and wealth
i) Current photo identification

The following are the acceptable forms of identification:

a. Valid driver's licence (bearing a photograph), issued by the authority in the country in which the person is resident

b. Valid Passport
c. Valid National Identification Card
d. If the person has an expired ID they may use a signed passport size photo from a J.P. which must be a match to the expired ID.

All applicants are subject to stringent due diligence and background checks prior to starting and must submit a police record within the first week of their employment. The background verification process is conducted by a third party and seeks to validate the following:

a) Past employment
b) References
c) Education / Qualification

Additionally, a credit check is required for all employees which is conducted by authorised Credit Bureaus and a copy shared with A&N Loan Hub.

All personnel are required to abide by the company's Employee Handbook Code of Conduct and Acceptable Use policy and other HR policies which may be promulgated, as well as being required to sign to obligations of confidentiality.

TRAINING

All employees are subject to this policy and to the corresponding training requirements which includes (but is not limited to):

a) Information security basics
b) The KYC requirements/ process for persons which interface with the company
c) The applicable legislations (to include POCA, TPA, MLA)
d) The recognition or detection of unusual, irregular or suspicious transactions
e) Incident reporting Process

Training is conducted at the start of employment and annually thereafter with the option to have refresher sessions as deemed necessary by the company. A certificate showcasing satisfactory completion of the employee's training should be issued at the completion of training sessions and a record of the training/signed registers retained.

CUSTOMER DUE DILIGENCE (KNOW YOUR CUSTOMER)

KYC procedures enable the company to know/understand its clients and their financial dealings better, which in turn helps it to manage the associated risks prudently. It also enables the company to comply with all the legal and regulatory obligations in respect of KYC norms / Anti-Money Laundering (AML) standards / combating the Financing of Terrorism (CFT) measures.

The Credit Administration and Credit Sales and Client Services Units must clearly establish the identity of each client. At a minimum, the KYC requirements include:

a) Processes for the identification and verification of the nature and purpose of a client's business, in order to determine whether a transaction is unusual or suspicious, or fits the norm expected of such a business.

b) Procedures for the recording and regular review of client identification and transaction information/records, to ensure that the information is current and comprehensive. S This information is to be retained for a minimum of five years after the transaction was initiated/attempted or had actually taken place, or the business relationship has been terminated.

IDENTIFICATION OF NATURAL PERSONS

The following information should be obtained from all prospective clients:

a) True name and names used;

b) Current permanent address, including postal address; (verified through utility bill or letter from JP or postal stamp)

c) Date of birth; (verified through drivers licence, TRN or passport)

d) Nationality;

e) Source of funds, and source of wealth, where considered appropriate;

f) Proof of employment through submission of staff ID, Job letter, contract and payslips;

g) Contact numbers (work; home; cellular);

h) 2 References;

i) Taxpayer Registration Number (TRN);

j) One of the following as an acceptable form of identification:

- Valid Driver's licence (bearing a photograph), issued by the authority in the country in which the person is resident
- Valid Passport
- Valid National Identification Card
- If the person has an expired ID they may use a signed passport size photo from a J.P. which must be a match to the expired ID.

k) Use of funds details

The requirements as outlined in bullets "a – j" are applicable for all guarantor/s and will be processed/ validated in the same manner as that which is used for the primary applicant. Also, it should be noted that all reoccurring loans require updated payslips, bank statements, proof of address and updated ID (if expired) for the applicant and guarantor/s.

CREDIT CHECKS

a) Credit checks are done for all loans above JMD $100,000.00, and is used as a guide to understand the better serve the client.

b) This is also required for clients who apply for business loans and are registered Sole Proprietors.

IDENTIFICATION OF CORPORATE BODIES

As it regards bodies corporate transacting business, the following are required:

a) Certificate of Incorporation or Certificate of Registration;

b) Articles of Incorporation or Partnership Deed;

c) The most recent Financial Statement of the business :

a. All yearly statements should be audited. Exceptions are only made for Financial Statements done in the last quarter.

d) A description of the principal line of business and major suppliers (if applicable);

e) A copy of the licence/approval to operate where the principal line of business is one that falls under a regulatory/supervisory body;

f) List of names, addresses and nationalities of principal owners and directors, including evidence of the identity of the natural persons,;

g) Group/Corporate structure, where applicable;

h) Tax Compliance Certificate to Tax compliance letter; and

i) Use of funds details.

HIGH RISK TRANSACTIONS/BUSINESS RELATIONSHIPS

a) Loan are not issued to persons who are deemed as politically exposed or high risk (regarding possible criminal conduct or association with person/groups known to have criminal conduct).

b) Loans are not given to non-nationals

DUE DILIGENCE REQUIREMENT FOR INVESTORS

All new investors should be referred to the company and should clear a reference/ background check. This will be conducted by a third party agency. They are also required to submit a police record and provide a credit report from an authorized local Credit Bureau.

The following will also be collected and verified as part of the due diligence process:

a) True name and names used;

b) Correct permanent address, including postal address; (verified through utility bill or letter from JP or postal stamp);

c) Date of birth (verified through drivers licence, TRN or passport);

d) Nationality;

e) Source of funds, and source of wealth, where considered appropriate/ declaration of income;

f) Contact numbers (work; home; cellular);

g) Taxpayer Registration Number (TRN);

h) Employment type;

i) 2 References;

j) Identification in any of the following forms:

- Valid Driver's licence (bearing a photograph), issued by the authority in the country in which the person is resident
- Valid Passport
- Valid National Identification Card
- If the person has an expired ID they may use a signed passport size photo from a J.P. which must be a match to the expired ID.

INFORMATION DISCLOSURE AND REPORTING

The C.E.O. is the nominated officer through whom A&N will fulfill and observe its responsibility to report and make disclosures regarding suspicious transactions. A&N's Nominated Officer holds the responsibility to report and make disclosures regarding suspicious transactions within fifteen (15) days of being notified of same.

This function will be supported by the Compliance Officer, the Board of Directors and the Audit Committee working together to:

1. Ensure the full implementation, maintenance and adherence to the company's ML/TFA policy, compliance management framework and information security policies.
2. Routine internal and external audits to determine adherence to internal policies, relevant legislature and Industry guidelines
3. Ensure there is adequate compliance monitoring and training to support employees;
4. Drive a compliance aware culture, including where employees feel comfortable to identify/ report incidents in a timely fashion and understand their obligations as well as their exposure to risk for prosecution in failing to execute their duties as prescribed; and

5. Enforce disciplinary and corrective actions where the policies and processes are not adhered to.

(Refer to the Compliance Management Framework - Governing Policy for further details on the overarching compliance framework)

All members of staff are encouraged to report breaches, potential risk, allegations of fraud and other incidents of non-compliance.

All compliance failures, breaches and suspicious activity should be reported to the Compliance Officer or the C.E.O, particularly those that are systemic and/or reoccurring issues. The company will continuously reinforce the need to report all breaches irrespective of the perceived potential impact as even a small failure, if not reported, can lead to the view that the failure does not matter or is not taken seriously and this may result in non-compliance becoming a systemic problem

REPORTING/DESIGNATED AUTHORITY

Designated Authority to whom suspicious transaction are to be reported, the Chief Technical Director (CTD) of the Financial Investigative Division of the Ministry of Finance and the Public Service for the purpose of carrying out the institutions obligations under law

SUSPICIOUS TRANSACTION REPORTS

The following conditions are considered triggers for making internal reports on suspicious transactions:

a) Payment attempts that would be above daily/ weekly limits for cash transactions.
b) Transactions flagged by the C.O. during weekly audits of repayment records or loan disbursement.
c) Any transaction with a client that is unusual and inconsistent with their known circumstance and or is uncommon for the nature and type of business the client is in.

d) There is information and or belief that the client has or is engaged in a transaction that could amount to or be related to money laundering and the information was obtained in the course of regular business transaction with a client.

Where a transaction or potential transaction with a client falls within the realm of being classified as a suspicious transaction, the matter must be brought to the attention of the Compliance Officer or Hub Operations Manager immediately.

This report will be passed on to the CEO, acting in the capacity of the nominated officer who will work with the Compliance Officer and Hub Operations Manager to review and assess whether the transaction or potential transaction falls within the realm of being a justifiable suspicion.

A&N will ensure that all suspicious reports are made, details of its internal investigation / associated documents are provided within the shortest possible timeframe and within the fifteen (15) day deadline. Additionally, all the investigation and all elements of the company's communication will be held in the strictest confidence and documented throughout the entire process.

RECORD KEEPING AND RETENTION

Scanned copies of all files will be created once a loan is being processed/ application made. This will be maintained regardless of the loan processing outcome. The Underwriter will conduct a secondary check to ensure that scanned copies are available for all loans. A loan will not be disbursed unless all requisite documents are available.

Once a loan is closed the Collections Officer will collect all closing documents and place on the client's record. All closing documents will also be scanned and saved in the records management system

.

FOR INDIVIDUAL CLIENTS

The following information will be retained:

a. Full Bank account number(s) and detail of all transactions;

b) Full names on the account to include aliases;

c) Proof of Nationality;

d) Clear and complete copies of the identifications presented (i.e. Driver's License, Passport and National Identification);

e) Tax Registration Number (TRN);

f) Correct permanent address to include post offices (proof provided). NB. Postal Agencies (P.A.) and Post Office (P.O.) addresses are not acceptable;

g) Source of funds/wealth/income (proof provided);

h) At least two (2) written references;

i) All contact numbers;

j) Account opening forms (i.e. Loan Applications, credit authorization forms, loan agreement etc.);

k) Business correspondences presented in support of the application; and

l) Loan repayment detail to include dates, types of currency used and all other details forming part of the transactions.

FOR CORPORATE CLIENTS

The minimum information required to be retained are:

a) Full account numbers of all transactions;

b) Full legal name of the corporate entity;

c) Country of incorporation;

d) Description of business carried out by the corporate entity;

e) Tax Registration Number (TRN);

f) The registered office location;

g) Full and complete transaction details of all dealings with the entity;

h) Full personal detail of the signatory for the corporate entity on the account; and

i) Full knowledge and identity of the beneficial owner

The Compliance Officer will conduct random file reviews on a monthly basis to evaluate the adherence to the requirements above and to ensure that scanned copies are available for each client file. Once an account is closed the Collections Officer will present the closing file to the Compliance Officer who will verify that all the required documents are present. These files will be stored and records for individual and corporate clients maintained for a minimum of five (5) years.