ANTI-MONEY LAUNDERING POLICY

PURPOSE

This AML/CFT Policy sets out Pappajack Berhad ("PAPPAJACK") or "the Company" general guiding policy in consonance with the policy of the Bank Negara Malaysia ("BNM") to combat money laundering and terrorist financing activities, as embodied in the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 ("AMLATFA") (the "Act").

SCOPE

This Policy is applicable to prevent use of PAPPAJACK's products and services for money laundering (which includes handling of criminal proceeds) or terrorists financing (referred to collectively as "money laundering") purposes.

DEFINITIONS

1.0 Description Of Money Laundering

Money laundering is a process of converting cash or property derived from criminal activities to give it a legitimate appearance. It is a process to clean 'dirty' money in order to disguise its criminal origin.

- **Placement:** The placing of ill-gotten gains into financial or nonfinancial institutions.

- **Layering:** The second stage of the money laundering process where it involves the process of creating multiple layers of complex financial transactions to further distance the illegal funds from their illegal sources. These layers are designed to obscure or to make it difficult to trace the origin of the funds.

- **Integration:** The final stage that completes the money laundering process where laundered proceeds are successfully integrated into the economy as legitimate funds.

2.0 Description Of Terrorism Financing

Terrorism financing is the act of providing financial support, funded from either legitimate or illegitimate source, to terrorists or terrorist organizations to enable them to carry out terrorist acts or will benefit any terrorist organization.

While most of the funds originate from criminal activities, they will also be derived from legitimate sources, for example, through salaries, revenues generated from legitimate business or the use of non-profit organizations to raise funds through donations.

POLICIES AND PROCEDURES

1.0 RISK-BASED APPROACH APPLICATION

1.1 Risk Management Function

1.1.1 In the context of "Risk Based Approach", the intensity and extensiveness of risk management functions will be proportionate to the nature, scale and complexity of the PAPPAJACK's activities and ML/TF risk profile.

1.2 Risk Assessment

1.2.1 PAPPAJACK is required to take appropriate steps to identify, assess and understand their ML/TF risks in relation to their customer, countries or geographical areas and products, services, transactions or delivery.

1.2.2 In assessing ML/TF risks, PAPPAJACK is required to have the following processes in place:-

a. Documenting their risk assessments and findings

b. Considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied.

c. Keeping the assessment up-to-date through a periodic review; and

d. Having appropriate mechanisms to provide risk assessment information to the supervisory authority.

1.2.3 PAPPAJACK is required to conduct additional assessment, as and when required by the supervisory authority.

1.2.4 PAPPAJACK will be guided by the results of the National Risk Assessment issued by Bank Negara Malaysia in conducting their own risk assessments.

1.3 Risk Control and Mitigation

1.3.1 PAPPAJACK will implement among others the following minimum risk mitigation strategies:

a. **Customer Due Diligence (CDD) –** Whenever PAPPAJACK is required to identify a customer, it must establish and verify the identity of the ultimate natural person;

b. **Monitoring of Customers and Transactions** – A permanent monitoring of clients' accounts must be implemented to detect unusual/suspicious transactions. Monitoring must be effected for applicable business areas using adequate processes systems; and

c. **Suspicious Transaction Reporting** – Such circumstances/transactions must be reported to the supervisory authority according to local law. Board of Directors and Senior Management of PAPPAJACK must be informed about all suspicious events, if not explicitly prohibited by local law

d. **Training and Awareness** – All employees (including trainees and temporary personnel) responsible for carrying out transactions and/or for initiating and/or establishing business relationships must undergo anti money laundering training.

1.4 Risk Profiling

1.4.1 PAPPAJACK will consider among others the following factors when measuring money laundering and terrorist financing ("ML/TF") risks on its customers:

a. Customer categories (high, medium and low risk customers) – example residents or non-residents, type of customer, legal person, structure, types of Politically Exposed Persons (PEPs) or types of occupation;

b. Country of origin of customer or geographical location of business risk Factors that will result in a determination that a country poses a higher risk include: Countries subject to sanctions or similar measures issued by the United Nations ("UN") as an example.

c. Any other information suggesting that the customer is of high risks.

1.4.2 While a risk assessment is routinely performed at the inception of a customer relationship, for some customer a comprehensive profile will only become evident once they have begun transacting through an account. Thus, the monitoring of customer / transactions, ongoing reviews and update of the customer's risk profile is a fundamental component of PAPPAJACK's risk based approach. In addition, this type of risk assessment process will also be adjusted for a particular customer based upon information received from a supervisory authority.

2.0 CUSTOMER DUE DILIGENCE

2.1 Customer Acceptance Policy ("CAP")

2.1.1 Customer's Acceptance

2.1.1.1. We will have in place a policy and criteria to identify and assess risk of customers, i.e. AML/CFT risk assessments, risk control and mitigation and risk profiling, especially in identifying the types of customers associated with high risk of money laundering and financing of terrorism.

2.1.1.2. Under PAPPAJACK's Customer Acceptance Policy, PAPPAJACK:

a. Will only accept customers after verifying their identity.

b. Will not proceed with transaction in the name of anonymous / fictitious persons.

c. Will categorise customers into various risk categories and based on the risk perception, decide on criteria for each category.

2.2 When CDD Is Required

2.2.1 PAPPAJACK is required to conduct CDD on the customer and the person conducting transaction, when:

a. establishing business relations, where applicable;

b. when the customer's transaction amount is equivalent to RM3,000 and above;

c. when then customer's redemption amounting to RM3,000 and above;

d. it has any suspicion of ML/TF, regardless of the amount; or

e. it has any doubt about the veracity or adequacy of previously obtained information.

2.3 What Is Required

2.3.1 PAPPAJACK is required to:

a. identify and verify that the customer's identify using reliable, independent source documents, data or information;

b. verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that party;

c. identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that PAPPAJACK is satisfied that it knows who the beneficial owner is; and

d. understand and, where relevant, obtain information on, the purpose and intended nature of the business relationship.

2.4 Timing of Verification

2.4.1 PAPPAJACK is required to verify the identity of the customer and beneficial owner during the registration procedure, before establishing a business relationship with a customer.

2.5 Specified CDD Measures

Individual Customer and Beneficial Owner

2.5.1 In conducting CDD on an individual customer and beneficial owner, PAPPAJACK is required to obtain at least the following information:

a. full name;

b. mobile number (if available);

c. National Registration Identity Card ("NRIC") number or passport number or reference number of any other official documents bearing the photograph / identity of the customer or beneficial owner;

d. residential and mailing address;

e. date of birth;

f. nationality; and

g. purpose of transactions.

2.5.2 PAPPAJACK will verify the documents referred to under Paragraph 6.4.1(b) by requiring the customer or beneficial owner, as the case will be, to furnish the original document and make a copy of the said document. However, where biometric identification method is used, verification is deemed to be satisfied.

2.5.3 Where there is any doubt, PAPPAJACK is required to request the customer or beneficial owner, as the case will be, to produce other supporting official identification documents bearing their photographs / identity, issued by an official authority or an international organization, to enable their identity to be ascertained and verified.

2.6 Enhanced CDD

2.6.1 PAPPAJACK is required to perform enhanced CDD where the ML/TF risks are assessed as higher risk. An enhanced CDD, will include, at least, the following:

a. obtaining CDD information under Paragraph 6.4;

b. obtaining additional information on the customer and beneficial owner (e.g. volume of assets and other information from public database);

c. inquiring on the source of wealth or source of funds. In the case of PEPs, both sources must be obtained; and

d. where applicable, obtaining approval from the Senior Management of PAPPAJACK before establishing (or continuing, for existing customer) such business relationship with the customer. In the case of PEPs, Senior Management refers to Senior Management at the head office.

2.6.2 In addition , PAPPAJACK will implement the following enhanced CDD measures in line with the ML/TF risks identified:

a. obtaining additional information on the intended level and nature of the business relationship;

b. updating more regularly the identification data of customer and beneficial owner;

c. inquiring on the reasons for intended or performed transactions; and

2.6.3 PAPPAJACK are required to conduct enhanced CDD on the following situations which are deemed to be of higher risk:

a. when the customer sends a representative to execute the transactions; and

b. non face-to-face business relationship or transaction through instruction received from telephone, with the customer of whom the business relationship has been established.

2.7 Ongoing Due Diligence

2.7.1 PAPPAJACK is required to conduct on-going due diligence on the business relationship with its customer. Such measures will include:

a. scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with PAPPAJACK's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

b. ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records particularly for higher risk customers.

2.7.2 In conducting on-going due diligence, PAPPAJACK will take into consideration the economic background and purpose of any transaction or business relationship which:

a. appears unusual;

b. is inconsistent with the expected type of activity and business model when compared to the volume of transaction;

c. does not have any apparent economic purpose; or

d. casts doubt on the legality of such transactions, especially with regard to complex and large transactions or involving higher risk customer.

e. Ongoing due diligence is guided by the parameters set in Appendix 1 *(Please refer to **Appendix 1** for details).*

2.7.3 The frequency of the on-going due diligence, enhanced ongoing due diligence as the case will be, will commensurate with the level of ML/TF risks posed by the customer based on the risk profiles and nature of transactions.

2.7.4 PAPPAJACK is required to increase the number and timing of control applied, and to select patterns of transactions that need further examination, when conducting enhanced on-going due diligence.

2.8 Existing Customer Materiality and Risk

2.8.1 PAPPAJACK is required to apply CDD requirements to existing customer on the basis of materiality and risk.

2.8.2 PAPPAJACK is required to conduct CDD on such existing relationships at least annually taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

2.8.3 In assessing materiality and risk of the existing customer under Paragraph 2.7.1, PAPPAJACK will consider the following circumstances:

a. the nature and circumstances surrounding the transaction including the significance of the transaction;

b. any material change in the way the account or business relationship is operated; or

c. insufficient information held on the customer or change in customer.

3.0 POLITICALLY EXPOSED PERSONS (PEPS)

3.1 The requirements set out under this Paragraph are applicable to family members or close associates of all types of PEPs.

3.2 The definition of PEPs is as follows:

a. Foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials;

b. Domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations and important political party officials; or

c. Persons who are or have been entrusted with a prominent function by an international organization which refers to members of senior management. For example, directors, deputy directors and members of the board or equivalent functions.

3.3 PAPPAJACK is required to take reasonable measures to determine whether a customer or beneficial owner is a foreign PEP or domestic PEP or a person entrusted with a prominent function by an international organization.

3.4 If the customer or beneficial owner is assessed as foreign PEP or domestic PEP or a person entrusted with a prominent function by an international organization, PAPPAJACK is required to assess the level of ML/TF risks posed by the business relationship with the domestic PEP or person entrusted with a prominent function by an international organization.

3.5 The assessment of the ML/TF risks, as specified under Paragraph 3.4, will take into account the profile of the customer under Paragraph 1.4 on Risk Profiling.

3.6 The requirements of enhanced CDD as set out under Paragraph 2.6 must be conducted in respect of foreign PEPs or domestic PEPs or person entrusted with a prominent function by an international organization who are assessed as higher risk.

3.7 PAPPAJACK will apply CDD measures similar to other customer for foreign PEPs or domestic PEPs or persons entrusted with a prominent function by an international organization if PAPPAJACK is satisfied that the domestic PEPs or persons entrusted with a prominent function by an international organization are not assessed as higher risk.

4.0 NEW PRODUCTS AND BUSINESS PRACTICES

4.1 PAPPAJACK is required to identify and assess the ML/TF risks that will arise in relation to the development of new products and business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

4.2 PAPPAJACK is required to:

a. undertake the risk assessment prior to the launch or use of such products, practices; and

b. take appropriate measures to manage and mitigate the risks.

5.0 BANK TRANSFERS

5.1 General

5.1.1 The requirements under this Paragraph are applicable to bank transfers and payments.

5.1.2 PAPPAJACK must comply with the requirements on combating the financing of terrorism under Paragraph 12 in carrying out wire transfer.

5.1.3 PAPPAJACK will not execute the bank transfer if it does not comply with the requirements specified in this Paragraph.

5.1.4 PAPPAJACK is required to maintain all originator and beneficiary information collected in accordance with record keeping requirements under Paragraph 9.

5.2 Non Face-To-Face Business Relationship

5.3.1 PAPPAJACKs will not undertake any transactions without face-to-face contact with the customer unless the business relationship with the customer has been first established and CDD measures have been conducted.

5.3 Reliance on Third Parties

5.4.1 PAPPAJACK will, from time to time rely on third parties (i.e. Remittance Agents) to conduct CDD or to introduce business on its behalf. The ultimate responsibility and accountability of CDD measures will however remain with PAPPAJACK.

5.4.2 PAPPAJACK will ensure appropriate internal policies and procedures are in place to mitigate the risks when relying on third parties.

6.0 HIGHER RISK COUNTRIES

6.1 PAPPAJACK is required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having on-going or substantial ML/TF risks.

6.2 Where ML/TF risks are assessed as higher risk, PAPPAJACK is required to conduct enhanced CDD for business relationships and transactions with any person from countries identified by the FATF or the Government of Malaysia as having strategic AML/CFT deficiencies that have not made sufficient progress in addressing those deficiencies.

6.3 In addition to the enhanced CDD requirement under Paragraph 2.6, PAPPAJACK is required to apply appropriate countermeasures, proportionate to the risk, for higher risk countries listed as having on-going or substantial ML/TF risks, as follows:

a. limit business relationship or financial transactions with identified countries or persons located in the country concerned;

b. review and amend, or if necessary terminate, correspondent banking relationships with financial institutions in the country concerned;

c. conduct enhanced external audit, by increasing the intensity and frequency, on branches and subsidiaries of PAPPAJACK located in the country concerned;

d. submit a report with a summary of exposure to customer and beneficial owners from the country concerned to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia on an annual basis; and

e. conduct any other measures as will be specified by Bank Negara Malaysia.

7.0 FAILURE TO SATISFACTORILY COMPLETE CDD

7.1 PAPPAJACK will not commence business relations or perform any transaction in relation to a potential customer, or will terminate business relations in the case of an existing customer, if PAPPAJACK is unable to comply with the CDD requirements.

7.2 In the event of failure to comply with the CDD requirements, PAPPAJACK must consider lodging a suspicious transaction report under Paragraph 16.

8.0 MANAGEMENT INFORMATION SYSTEM

8.1 PAPPAJACK must have in place an adequate management information system (MIS), either electronically or manually, to complement its CDD process. The MIS is required to provide PAPPAJACK with timely information on a regular basis to enable PAPPAJACK to detect irregularity and/or any suspicious activity.

8.2 The MIS will commensurate with the nature, scale and complexity of PAPPAJACK's activities and ML/TF risk profile.

8.3 The MIS will include, at a minimum, information on multiple transactions over a certain period, large transactions, anomaly in transaction patterns, customer's risk profile and transactions exceeding any internally specified threshold.

8.4 The MIS will be able to aggregate customer's transactions from multiple accounts and/or from different systems.

8.5 The MIS will be integrated with PAPPAJACK's information system that contains its customer's normal transaction or business profile, which is accurate, up-to-date and reliable.

9.0 RECORD KEEPING

9.1 PAPPAJACK is required to keep the relevant records including any files, business correspondence and documents relating to transactions, in particular, those obtained during the CDD process. This includes documents used to verify the identity of customer and beneficial

owners, and results of any analysis undertaken. The records maintained must remain up-to-date and relevant.

9.2 PAPPAJACK is required to keep the records for at least six years following the completion of the transaction.

9.3 In situations where the records are subjected to on-going investigation or prosecution in court, they will be retained beyond the stipulated retention period until such time PAPPAJACK is informed by the relevant law enforcement agency that such records are no longer required.

9.4 PAPPAJACK is required to retain the relevant records in a form that is admissible as evidence in court and make such available to the supervisory authorities and law enforcement agencies in a timely manner.

9.5 The following information are required to be recorded in the receipt of transaction with the customer:

i. PAPPAJACK's business address and telephone number;

ii. Date of transaction;

iii. Receipt serial number;

iv. the amount of funds in ringgit be received by the beneficiary;

v. fees and charges to the customer;

vi. name of beneficiary (where applicable); and

vii. customer's NRIC or Company identification number / Passport number (where applicable).

10.0 AML/CFT COMPLIANCE PROGRAMME

10.1 Policies, Procedures and Controls

PAPPAJACK is required to implement programs to mitigate against ML/TF, which correspond to its ML/TF risks and the size of its business.

10.2 Board of Directors

10.2.1 General

a. Members of Board of Directors (Board members) are required to understand their roles and responsibilities in managing ML/TF risks faced by PAPPAJACK.

b. Board members must be aware of the ML/TF risks associated with business strategies, delivery channel and geographical coverage of its business products and services.

c. Board members must understand the AML/CFT measures required by the laws including the AMLATFA, subsidiary legislation and instruments issued under the AMLATFA, and the industry's standards and best practices as well as the

importance of implementing AML/CFT measures to prevent PAPPAJACK from being abused by money launderers and financiers of terrorism.

10.2.2 The Board of Directors has the following roles and responsibilities:

a. maintain accountability and oversight for establishing AML/CFT policies and minimum standards;

b. approve policies regarding AML/CFT measures within PAPPAJACK, including those required for risk assessment, mitigation and profiling, CDD, record keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism;

c. establish appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in PAPPAJACK's products and services, technology as well as trends in ML/TF;

d. establish an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by PAPPAJACK;

e. define the lines of authority and responsibility for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls;

f. ensure effective internal audit function in assessing and evaluating the robustness and adequacy of controls implemented to prevent ML/TF;

g. assess the implementation of the approved AML/CFT policies through regular reporting and updates by the Senior Management and Risk Management Committee; and

h. establish MIS that is reflective of the nature of PAPPAJACK's operations, size of business,

i. complexity of business operations and structure, risk profiles of products and services offered and geographical coverage.

10.3 Senior Management

10.3.1 Senior Management is accountable for the implementation and management of AML/CFT compliance programs in accordance with policies and procedures established by the Board, requirements of the law, regulations, guidelines and the industry's standards and best practices.

10.3.2 The Senior Management has the following roles and responsibilities:

a. be aware of and understand the ML/TE risks associated with business strategies, delivery channels and geographical coverage of its business products and services offered and to be offered including new products, new delivery channels and new geographical coverage;

b. formulate AML/CFT policies to ensure that they are in line with the risks profiles, nature of business, complexity, volume of the transactions undertaken by PAPPAJACK and its geographical coverage;

c. establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT policies.

d. and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;

e. undertake review and propose to the Board the necessary enhancements to the AML/CFT policies to reflect changes in PAPPAJACK's risk profiles, institutional and group business structure, delivery channels and geographical coverage;

f. provide timely periodic reporting to the Board on the level of ML/TF risks facing PAPPAJACK, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which will have an impact on PAPPAJACK;

g. allocate adequate resources to effectively implement and administer AML/CFT compliance programs that are reflective of the size and complexity of PAPPAJACK's operations and risk profiles;

h. appoint a compliance officer at management level at Head Office and designate a compliance officer at management level at each branch or subsidiary;

i. provide appropriate level of AML/CFT training for its employees at all levels throughout the organization;

j. ensure that there is a proper channel of communication in place to effectively communicate the AML/CFT policies and procedures to all levels of employees;

k. ensure that AML/CFT issues raised are addressed in a timely manner; and

l. ensure the integrity of its employees by establishing appropriate employee assessment system.

10.4 Compliance Management Arrangements at the Head Office

10.4.1 The Compliance Officer acts as the reference point for AML/CFT matters within PAPPAJACK.

10.4.2 The Compliance Officer is required to be "fit and proper" to carry out his AML/CFT responsibilities effectively.

10.4.3 For the purposes of Paragraph 10.4.2, "fit and proper" will include minimum criteria relating to:

a. probity, personal integrity and reputation; or

b. competency and capability.

10.4.4 The Compliance Officer must have the necessary knowledge and expertise to effectively discharge his roles and responsibilities, including being informed of the latest developments in ML/TF techniques and the AML/CFT measures undertaken by the industry.

10.4.5 PAPPAJACK will encourage the Compliance Officer to pursue professional qualifications in AML/CFT so that they are able to carry out their obligations effectively.

10.4.6 PAPPAJACK is required to ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented.

10.4.7 The Compliance Officer has a duty to ensure the following:

a. PAPPAJACK's compliance with the AML/CFT requirements;

b. proper implementation of the AML/CFT policies;

c. the appropriate AML/CFT procedures, including CDD, record-keeping, on-going due diligence, reporting of suspicious transactions and combating the financing of terrorism, are implemented effectively;

d. the AML/CFT mechanism is regularly assessed to ensure that it is effective and sufficient to address any change in ML/TF trends;

e. the channel of communication from the respective employees to the branch or subsidiary compliance officer and subsequently to the Compliance Officer is secured and that information is kept confidential;

f. all employees are aware of PAPPAJACK's AML/CFT measures, including policies, control mechanism and the channel of reporting;

g. internal generated suspicious transaction reports by the branch or subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia; and

h. the identification of ML/TF risks associated with new products or services or arising from the reporting

i. institution's operational changes, including the introduction of new technology and processes.

10.4.8 PAPPAJACK is required to inform, in writing, the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, within ten working days, on the appointment or change in the appointment of the Compliance Officer, including such details as the name, designation, office address, office telephone number, fax number, e-mail address and such other information as will be required.

10.5 Employee Screening Procedures

10.5.1 The screening procedures will be applied upon hiring the employee and throughout the course of employment.

10.5.2 PAPPAJACK is required to establish an employee assessment system that is commensurate with the size of operations and risk exposure of PAPPAJACK to ML/TF.

10.5.3 The employee assessment system will include an evaluation of an employee's personal information, including employment and financial history.

10.6 Employee Training and Awareness Programs

10.6.1 For the purpose of this Paragraph, reference to employees includes agents.

10.6.2 PAPPAJACK is required to conduct awareness and training programmes on AML/CFT practices and measures for their employees. Such training must be conducted regularly and supplemented with refresher courses.

10.6.3 The employees must be made aware that they will be held personally liable for any failure to observe the AML/CFT requirements.

10.6.4 PAPPAJACK must make available its AML/CFT policies and procedures for all employees and its documented AML/CFT measures must contain at least the following:

a. the relevant documents on AML/CFT issued by Bank Negara Malaysia or relevant supervisory authorities; and

b. PAPPAJACK's internal AML/CFT policies and procedures.

10.6.5 The training conducted for employees must be appropriate to their level of responsibilities in detecting ML/TF activities and the risks of ML/TF faced by PAPPAJACK.

10.6.6 Employees who deal directly with the customer will be trained on AML/CFT prior to dealing with them.

10.6.7 Training for all employees will provide a general background on ML/TF, the requirements and obligations to

10.6.8 Monitor and report suspicious transactions to the Compliance Officer and the importance of CDD.

10.6.9 In addition, training will be provided to specific categories of employees:

a. Front-Line Employees

Front-line employees will be trained to conduct effective on-going CDD, detect suspicious transactions and on the measures that need to be taken upon determining a transaction as suspicious. Training will also be provided on factors that will give rise to suspicion, such as dealing with occasional customers / collecting agent / remittance agent transacting in large cash volumes, PEPs, higher risk customer and the circumstances where enhanced CDD is required.

b. Employees that Establish Business Relationships

The training for employees who establish business relationships will focus on identification, verification and CDD procedures of customer, including when to conduct enhanced CDD and circumstances where there is a need to defer establishing business relationship with a new customer until CDD is completed satisfactorily.

c. Supervisors and Managers

The training on supervisors and managers will include overall aspects of AML/CFT procedures, in particular, the risk-based approach to CDD, risk profiling of customers, enforcement actions that can be taken for non-compliance with the relevant requirements pursuant to the relevant laws and procedures related to the financing of terrorism.

10.7 Independent Audit Functions

10.7.1 The Board is responsible to ensure regular independent audits of the internal AML/CFT measures to determine their effectiveness and compliance with the AMLATFA, its regulations, subsidiary legislations, the relevant documents on AML/CFT issued by Bank Negara Malaysia as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.

10.7.2 The Board is required to ensure that the roles and responsibilities of the auditor are clearly defined and documented. The roles and responsibilities of the auditor include, at a minimum:

a. checking and testing the compliance with, and effectiveness of the AML/CFT policies, procedures and controls; and

b. assessing whether current measures are in line with the latest developments and changes to the relevant AML/CFT requirements.

10.7.3 The scope of independent audit will include, at a minimum:

a. compliance with AMLATFA, its subsidiary legislation and instruments issued under the AMLATFA;

b. compliance with PAPPAJACK's internal AML/CFT policies and procedures;

c. adequacy and effectiveness of the AML/CFT compliance programme; and reliability, integrity and timeliness of the internal and regulatory reporting and management of information systems.

10.7.4 The auditor must submit a written audit report to the Board to highlight the assessment on the effectiveness of AML/CFT measures and any inadequacy in internal controls and procedures.

10.7.5 PAPPAJACK is required to ensure that independent audits are carried out at the institution level at least on an annual basis.

10.7.6 PAPPAJACK must ensure that such audit findings and the necessary corrective measures undertaken are submitted to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and its relevant supervisory authorities within ten working days of their submission to its Board.

11.0 SUSPICIOUS TRANSACTION REPORT

11.1 General

11.1.1 PAPPAJACK is required to promptly submit a suspicious transaction report to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia whenever PAPPAJACK suspects or have reasons to suspect that the transaction (including attempted or proposed), regardless of the amount:

a. appears unusual;

b. has no clear economic purpose;

c. appears illegal;

d. involves proceeds from an unlawful activity; or

e. indicates that the customer is involved in ML/TF.

11.1.2 PAPPAJACK must provide the required and relevant information that gave rise to doubt in the suspicious transaction report form, which includes but is not limited to the nature or circumstances surrounding the transaction and business background of the person conducting the transaction that is connected to the unlawful activity.

11.1.3 PAPPAJACK must establish a reporting system for the submission of suspicious transaction reports.

11.1.4 Triggers / red flags for the purposes of reporting suspicious transactions are shown in the **Appendix 1** – List of Parameters to be established in the Fraud Detection System.

11.2 Reporting Mechanisms

11.2.1 PAPPAJACK is required to ensure that the designated branch or subsidiary Compliance Officer is responsible for channeling all internal suspicious transaction reports received from the employees of the respective branch or subsidiary to the Compliance Officer at the Head Office. In the case of employees at the Head Office, such internal suspicious transaction reports will be channeled directly to the Compliance Officer.

11.2.2 In the event of discovery suspicious transaction, Internal Suspicious Transaction Report ("ISTR") must be raised and submitted to the Compliance Officer within 1 working day.

11.2.3 Upon receiving any internal suspicious transaction report whether from the head office, branch or subsidiary, the Compliance Officer must evaluate the grounds for suspicion within 5 working days upon submission. Once the suspicion is confirmed, the Compliance Officer must promptly submit the suspicious transaction report. In the case where the Compliance Officer decides that there are no reasonable grounds for suspicion, the Compliance Officer must document and file the decision, supported by the relevant documents.

11.2.4 The Compliance Officer must maintain a complete file on all internally generated reports and any supporting documentary evidence regardless of whether such reports have been submitted. If there is no suspicious transaction reports submitted to Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the internally generated reports and the relevant supporting documentary evidence must be made available to the relevant supervisory authorities upon request.

11.2.5 The Compliance Officer must ensure that the Suspicious Transaction Report is submitted within the next working day, from the date the Compliance Officer establishes the suspicion.

11.2.6 PAPPAJACK must ensure that in the course of submitting the suspicious transaction report, utmost care must be undertaken to ensure that such reports are treated with the highest level of confidentiality. The Compliance Officer has the sole discretion and independence to report suspicious transactions.

11.2.7 The Compliance Officer must submit the suspicious transaction report in the specified suspicious transaction report from through any following modes:

Mail: Director
Financial Intelligence and Enforcement Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur
(To be opened by addressee only)

Fax: +603-2693 3625

E-mail: st@bnm.gov.my

11.2.8 Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the compliance officer of PAPPAJACK must submit its suspicious transaction reports on-line:

Website: https://bnmapp.bnmlov.my/fins2

11.2.9 PAPPAJACK must provide additional information and documentation as will be requested by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia and to respond promptly to any further enquiries with regard to any report received under Section 14 of the AMLATFA.

11.2.10 PAPPAJACK must ensure that the suspicious transaction reporting mechanism is operated in a secured environment to maintain confidentiality and preserve secrecy.

11.2.11 Where a suspicious transaction report has been lodged, PAPPAJACK is not precluded from making a fresh suspicious transaction report as and when a new suspicion arises.

11.3 Tipping Off

11.3.1 In cases where PAPPAJACK forms a suspicion of ML/TF and reasonably believes that performing the CDD process would tip off the customer, PAPPAJACK is permitted not to pursue the CDD process. In such circumstances, PAPPAJACK will proceed with the transaction and immediately file a suspicious transaction report.

11.3.2 Tipping off in relation to suspicious transaction report is not applicable if:

a. the purpose of the disclosure is made to inform the ML/TF risks involved in dealing with the customer, within the group; or

b. such disclosure is made to a supervisory authority of PAPPAJACK.

11.3.3 Provisions under Paragraph 11.3.2 will not come into effect until such date as will be specified by Bank Negara Malaysia.

12.0 COMBATING THE FINANCING OF TERRORISM

12.1 Where relevant, references to a customer in this Paragraph include a beneficial owner and beneficiary.

12.2 PAPPAJACK is required to keep updated with the various resolutions passed by the United Nations Security Council (UNSC) on counter terrorism measures in particular the UNSC Resolutions 1267 (1999), 1373 (2001), 1988 (2011) and 1989 (2011) which require sanctions against individuals and entities belonging or related to the Taliban and the Al-qaeda organization.

12.3 PAPPAJACK is required to maintain a list of individuals and entities (the Consolidated List) for this purpose. The updated UN List can be obtained at: http://www.un.org/sc/committees/1267/aq sanctions_list.shtml

12.4 PAPPAJACK is required to maintain a database of names and particulars of listed persons in the UN Consolidated List and such orders as will be issued under sections 66B and 66C of the AMLATFA by the Minister of Home Affairs.

12.5 PAPPAJACK will ensure that the information contained in the database is updated and relevant, and made easily accessible to its employees at the head office, branch or subsidiary.

12.6 PAPPAJACK is required to conduct checks on the names of new customer, as well as regular checks on the names of existing customer, and potential customers, against the names in the database. If there is any name match, PAPPAJACK is required to take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, PAPPAJACK must immediately:

a. block the transaction (where applicable), if it is an existing customer,;

b. reject the potential customer, if the transaction has not commenced;

c. submit a suspicious transaction report; and

d. inform the relevant supervisory authorities.

12.7 PAPPAJACK is required to submit a suspicious transaction report when there is an attempted transaction by any of the persons listed in the Consolidated List or orders made by the Minister of Home Affairs under sections 66B or 66C of the AMLATFA.

12.8 PAPPAJACK is required to ascertain potential matches with the Consolidated List to confirm whether they are true matches to eliminate "false positives". PAPPAJACK is required to make further inquiries from the customer or counter-party (where relevant) to assist in determining whether the match is a true match.

12.9 PAPPAJACK will also consolidate their database with the other recognized lists of designated persons or entities issued by other jurisdictions.

13.0 NON-COMPLIANCE

13.1 Non-compliance with this policy and its operating procedures will result in disciplinary actions. Before a decision with regard to disciplinary action is taken, the seriousness and merits of each case will be appraised by the Management.

14.0 APPENDICES

APPENDIX 1

List of Parameters to be established in the Fraud Detection System

No	Description	Type	Parameter / Threshold
1	Match with UN Consolidated List	Sanction Screening	>RM 3,000
2	Match with Malaysia's Listing Related to Terrorism and Terrorism Financing	Sanction Screening	>RM 3,000
3	Match with Higher Risk Countries	Sanction Screening	>RM 3,000
4	Unable to provide the proof of identity	Suspicious ML/TF Screening	>RM 3,000
5	Huge quantity but unable to provide the proof of ownership	Suspicious ML/TF Screening	>3 items
6	Huge amount but unable to provide the proof of ownership	Suspicious ML/TF Screening	>RM 3,000
7.	Number of different outlets visited by customer	Suspicious ML/TF Screening	>RM 3,000
8.	Frequent defaulters	Suspicious ML/TF Screening	>5 times per month

****

This version:	Version No. 2
File Name:	Anti-Money Laundering Policy (2023)
Prepared by:	Shawn Lim
Approved by:	Board of Directors