WELL CHIP GROUP BERHAD

Registration No. 202301014119 (1508041-A)
(Incorporated in Malaysia)

ANTI-MONEY LAUDERING POLICY

---

1. INTRODUCTION

This policy establishes the Anti-Money Laundering and Countering Financing of Terrorism ("AML/CFT") policy for Well Chip Group Berhad and its subsidiaries ("Well Chip"). The aim of this policy is to offer basic direction for preventing money laundering and terrorism financing ("ML/TF"), as stipulated under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ("AMLA") ("Act 613").

Transactions in the pawnbroking and jewellery industries are mainly cash-based. From both ML/TF perspectives, these industries pose two key concerns: (i) Pawners and jewellery buyers may use illicit money to repay debts or purchase jewellery; and (ii) pawners may pawn fraudulently obtained pledges and leave them unredeemed.

The risks of foreign terrorists actually using monies for terrorism financing ("TF") or terrorist activities are moderate to low. Furthermore, a terrorist looking to monetise an asset is more likely to sell it, rather than pawn it.

Well Chip recognizes the importance of the fight against ML/TF, since it impacts fundamental aspects of social life. Well Chip understands that the best way to comply with AMLA is to follow the Bank Negara Malaysia guidelines set out in the AML/CFT and Targeted Financial Sanctions for Designated Non-Financial Businesses and Professions (DNFBPs) & Non-Bank Financial Institutions (NBFIs) policy document that came to effect on 1 January 2020; is to establish effective internal policies, procedures and controls that are conductive to:-

a) Customer Due Diligence Measures (the "CDD");
b) Records keeping;
c) Detection of unusual or suspicious applications or transactions, and the submission of the suspicious transaction report ("STR");
d) Audit of the internal policies, procedures and controls;
e) Compliance management arrangements;
f) The hiring and training of employees; and
g) Identify ML/TF risks that may arise in relation to new technologies.

As a result, Well Chip's management and employees must be vigilant for any suspicious activity and report it immediately to the respective bodies/personal, in

accordance with specified policies and procedure, so that they may in turn notify the relevant authorities.

Only through the commitment of all executives and employees will it be possible to guarantee that the relevant pawn loan being granted cannot be used for money-laundering or terrorism financing purposes.

Adherence to the policy is absolutely fundamental to ensuring that Well Chip, regardless of the different branch location, complies fully with AMLA. All executives and employees of the Group, therefore be actively involved in the policy's implementation and development.

2. THE CONCEPT OF MONEY-LAUNDERING AND TERRORISM FINANCING

Money-laundering ("ML") is a process of converting cash, funds 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. A person commits ML when the person:

<table>
<tr><td colspan="2">Paragraph 4(1) of the AMLA</td></tr>
<tr><td>a. engages directly or indirectly, in a transaction that involves</td><td rowspan="4">Proceeds of an unlawful activity or instrumentalities of an offence.</td></tr>
<tr><td>b. acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes of, or uses</td></tr>
<tr><td>c. removes from, or brings into Malaysia OR</td></tr>
<tr><td>d. conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of</td></tr>
</table>

Commonly, the money laundering process comprises of three stages:-

a) **Placement** - The physical disposal of the benefits of criminal conduct;

b) **Layering** - The separation of the benefits of criminal conduct from their source by creating layers of financial transactions designed to disguise the audit trail; and

c) **Integration** - The provision of apparent legitimacy to the benefits of criminal conduct. If the layering process succeeds, the integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

Terrorism Financing ("TF") is the act of providing financial support to terrorists or terrorist organisations to enable them to carry out terrorist acts or to benefit any terrorist or terrorist organisation.

While funds may come from criminal activities, they may also be derived from legitimate sources, for example, through salaries, revenue from legitimate business or donations including through non-profit organisations.

3. CUSTOMER ACCEPTANCE POLICY

Risk Assessment

Well Chip considers that the threat of becoming involved in any ML/TF activity is directly related to the type of borrowing or jewellery transaction, and such threat can be more effectively and efficiently managed if the potential risk linked to the different types of borrowing or jewellery transaction is known beforehand.

Classifying its borrowers or jewellery buyers by risk level will enable Well Chip to design and implement measures and controls to mitigate such risk. Likewise, it will enable it to focus on those borrowings or jewellery transactions that present greater risk.

Customers will be categorized into risk-assessed groups titled *risk classes:* [low, medium, and high].

Three *risk factors* will be used to determine the *risk class* of each customer. These are:

1) Nationality of customers. Customers holding valid Malaysian IC, PR and all other types of Malaysian employment passes will carry a low-risk classification. Foreign customers from countries that are under economic sanctions by the United Nations will carry a high-risk classification and will not be eligible for any transaction. Customers from other countries will carry a medium-risk classification. Well chip will conduct due diligence on both low-risk and medium-risk before any transaction.

2) Transaction amount. The transaction amount is another risk factor that needs to be considered. For example, a transaction amount below RM25,000 will carry a low-risk classification. And any amount that reaches RM25,000 and above will carry a high-risk classification and requires enhanced due diligence.

3) PEP. Well Chip determines that a particular risk factor, if present, will automatically result in a high-risk classification, regardless of the other risk factors. Any customer with a PEP designation will automatically carry a high-risk classification.

Refer to Annex A for risk assessment table.

Enhanced CDD Measures

Well Chip must perform enhanced customer due diligence measures by completing the Enhanced CDD form if any of the risk factors in the risk assessment carry a high-risk classification, and not limited to the below points:

a) The relevant loan or purchase of jewelry is complex or unusually large.
b) The pawner has taken up 2 or more relevant loans that have no apparent or visible economic or lawful purpose.
c) The relevant loan is granted to a person or transaction with jewellery buyer who is from or in a higher-risk foreign country.
d) Well Chip has reason to believe that the pawner or jewelry buyer, or the relevant loan or purchase of jewellery may present a high risk of ML/TF.

UN Sanctions List

Well Chip shall ensure compliance with the United Nations (Anti-terrorism Measures) Regulations. Well Chip will take appropriate risk-management systems by uploading the UN Sanctions List into our blacklist database and classified it under Terrorist. In particular, Well Chip shall, before conducting any business or entering into any transaction with any person, verify the identity of the person against the lists of terrorists, persons associated with terrorist organisations and entities, other groups and undertakings associated with terrorist organisations as updated from time to time and made available on the Internet through the official United Nations website, at the following links:

https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list

In addition to the above list (which are issued under the Terrorism (Suppression of Financing) Act and UN Sanction Regulations), Well Chip shall not transact with entities or individuals listed under other UN Sanction Regulations which seek to address proliferation risks of weapons of mass destruction (as listed below). Well Chip shall also “freeze” without delay assets and funds collected from these persons or entities and seek further instructions from the authorities.

These Regulations include, but are not limited to:

a) United Nations (Freezing of Assets – Cote d’Ivoire) Regulations 2006;
b) United Nations (Sanctions – Democratic People’s Republic of Korea) Regulations 2010;
c) United Nations (Freezing of Assets of Persons – Democratic Republic of Congo) Regulations 2006;
d) United Nations (Sanctions – Iran) Regulations 2014;
e) United Nations (Freezing of Assets of Former President of Liberia and Connected Persons) Regulations 2004; and

f) United Nations (Freezing of Assets of Persons – Sudan) Regulations 2006 (collectively referred to as the "UN Regulations").

Well Chip shall maintain a database of names and particulars of listed persons in the UN Consolidated List and the list that is made by the Minister of Home Affairs under the section 66B (1) of the AMLA.

If Well Chip has reason to suspect that a relevant person is a terrorist or terrorist entity, Well Chip must —

a) Decline to enter into any transaction with the relevant person;
b) Terminate any transaction entered into with the relevant person, as well as request the settlement of the outstanding balance; and make a report to the relevant authorities.

Politically Exposed Persons (PEP)

Well Chip will take appropriate risk-management systems by uploading the PEP list into our blacklist database and classified it under PEP, and take reasonable measures, to assess whether a relevant person is a PEP or a family member or close associate of a PEP.

Where Well Chip determines that a relevant person is PEP or a close associate of a PEP, Well Chip will not establish or continue any business relationship with that person.

4. KNOW YOUR CUSTOMER (CUSTOMER DUE DILIGENCE MEASURES)

Well Chip must perform customer due diligence measures for all customers.

The most effective means of preventing the use of the financial system for ML/TF is to identify and know your customers, regardless of whether they are established customers or otherwise.

Along these lines, Well Chip has developed and implemented an internal policies procedures and controls aimed at obtaining effective and complete knowledge of their customers and their activities, in order to:

- Confirm and document the true identity of customers who maintain any type of business relationship.
- Confirm and document any additional customer information commensurate with the assessment of the ML/TF risk.
- Ensure that Well Chip do not do business with any individuals or entities whose identities cannot be confirmed, who do not provide all required information, or who have provided information that is false or that contains significant inconsistencies that cannot be clarified.

For customer identification, Well Chip shall consider the following criteria:

- In the case of individuals, an official identification document shall be required to confirm the individual's identity.
- A scanned copy or photocopy of the official document must be saved.
- Neither anonymous borrowers nor entities using fictitious names may be maintained.
- The documents evidencing the authority of any person authorizing financial transactions on behalf of the customer shall be required. Well Chip shall have procedures for determining that person's identity and relationship to the customer.
- All necessary measures shall be taken to obtain information about the true identity of the person on whose behalf a relationship is established, an account opened, or a significant transaction conducted (that is, the beneficial owners) whenever the customer is acting on behalf of third parties or in cases where doubts exist as to whether the customer is acting on its own behalf.

5. REPORTING SUSPICIOUS ACTIVITIES TO THE AUTHORITIES

Well Chip will make or file a STR disclosure under Part B, section 19.1 of the Bank Negara Malaysia AML/CFT Policies, and document the basis for its determination, in the following circumstances:

a) Well Chip is unable to complete performing the customer due diligence for any reason;
b) A pawner or jewellery buyer is unable or unwilling to provide any information requested, or decides to withdraw the pawn loan application or cancel the jewellery purchase deal when requested to provide information;
c) the relevant loan is part of an unusual pattern of loans with no apparent economic or lawful purpose;

General red flags indicators

1) Pawner taking multiple loans and repaying them before due date
2) Personal documents appear to be forged
3) Borrower does not resemble photograph in personal document
4) Borrower possesses large amount of jewellery without accountable origin (e.g. not in gold trading business)
5) Borrower appears nervous and evasive when subject to CDD

When Executive or employees report suspicious transactions or activities to Bank Negara Malaysia, in accordance with the procedures established by internal policies and procedures, they are strictly prohibited from providing any information internally or externally regarding the customers or transactions to which the information pertains.

All employee and executive of Well Chip should be constantly alert so as not to unwittingly assist in the criminal schemes of ML/TF. These efforts can help to maintain Well Chip's reputation. Well Chip will lodge a STR if there is a reasonable suspicion of ML/TF activity during the course of the Well Chip's administration or operations. Failure to do so may constitute a criminal offence.

A STR should be made when a person knows or has reason to suspect that any borrowing is directly or indirectly connected to a criminal conduct and the knowledge or suspicious arose during the course of the administration or operations.

Once the suspicion is confirmed, the Compliance Officer must submit the STR within the next working day, from the date the compliance officer establishes the suspicion, through any of the 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 : +603-2691 6108
E-mail : str@bnm.gov.my

Well Chip must provide the required and relevant information that gave rise to doubt in the STR, 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.

Where applicable and upon the advice of the Financial Intelligence and Enforcement Department, Bank Negara Malaysia, the Compliance Officer that has been granted access to the FINS administered by the Financial Intelligence and Enforcement Department, Bank Negara Malaysia must submit the STR through the following website:

https://bnmapp.bnm.gov.my/fins2

6. RECORD-KEEPING AND REPORTING REQUIREMENTS

Well Chip required to keep all relavant documents and information (including any analysis performed) relating to a person that the pawnbroker obtained during the CDD process for a period of 6 years after the latest of the following dates (so far as they are applicable):

a) The date on which the person offered to pawn goods to the pawnbroker;
b) The date on which the person redeemed a pledge from the pawnbroker;

c) The date on which the pawnbroker forfeited a pledge made by the person;
d) The date on which the pawnbroker ended any transaction or relationship with the person;

Well Chip shall maintain the following documents for at least 6 years, unless other legislation specifies a longer period:

- Documentation containing information on the identification and knowledge of the customer.
- Reports made to Financial Intelligence and Enforcement Department, Bank Negara Malaysia, concerning suspicious customer activity relating to possible ML/TF, together with supporting documents.
- Records of all courses given on the prevention of money-laundering and terrorism financing.
- Risk assessments and any other documents or registers required to be retained under applicable AML/CFT.

Well Chip shall make the documents and information required to be kept above available upon request to the supervisory authorities and law enforcement agencies in a timely manner.

Ongoing Monitoring

Well Chip shall perform ongoing monitoring of all existing customers relationships.

7. TRAINING OF PAWNBROKING PERSONNEL

A priority objective for Well Chip is the adoption of necessary measures to enable its personnel to be familiar with the requirements established by AML/CFT laws and regulations.

Thus, the Compliance Officer organise training programmes and special courses for management and employees, and specifically for personnel whose positions are suitable for detecting activity or transactions that may be related to ML/TF, and train these employees to detect suspicious activity and to understand the procedure in such cases.

The training programs should bear in mind international standards and local legislation to prevent ML/TF, the latest trends in criminal activity, and Well Chip policies and procedures designed to combat ML/TF, including how to recognize and report suspicious activities.

The Compliance Officer, in adapting corporate training plans and programs, should develop similar training programs and determine which personnel require specialized training in view of the risk of ML/TF inherent in their responsibilities or positions.

Apart from general training programmes, Compliance Officer shall be informed of and should provide on-going updates to the employees regarding changes in the policies and laws and regulations on this subject, as well as any new methods, techniques, or procedures found to be susceptible to ML/TF.

Well Chip shall establish in writing and apply the appropriate policies and procedures to ensure high ethical standards in the hiring of employees.

8. INTERNAL AUDIT

The internal audit function is necessary to ensure continued compliance with this policy, and its responsibilities include independently supervising the effectiveness of Well Chip's ML/TF prevention system (which comprises compulsory policies, standards and procedures) to ensure that all employees know their customers and that transactions are performed in conformity with professional ethics and current AML/CFT laws. The internal audit will be conducted at least once a year.

Well Chip shall appoint Compliance Officers to conduct the necessary audits and reviews for this purpose.

The Compliance Officer must:

- Have full responsibility for overseeing, developing, updating and enforcing the AMLCFT program
- Have sufficient authority to oversee, develop, update and enforce AMLCFT policies and procedures throughout the company
- Be competent and knowledgeable regarding:
  - Money laundering issues and risks
  - The AML/CFT legal framework

The Compliance Officer has a duty to ensure the following:

a) Well Chip'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 the Well Chip's AML/CFT measures, including policies, control mechanism and the channel of reporting;
g) Internally generated STR by the branch or subsidiary compliance officers are appropriately evaluated before submission to the Financial Intelligence and Enforcement Department, Bank Negara Malaysia;

h) Internal criteria such like red-flags must be established to enable identification and examination of suspicious transactions; and
i) The identification of ML/TF risks associated with new products or services or arising from Well Chip's operational changes, including the introduction of new technology and processes.

Well Chip shall also have an independent audit function to determine the effectiveness and compliance with the AMLA, its regulations, subsidiary legislations, the relevant documents on AML/CFT issued by the Bank as well as the requirements of the relevant laws and regulations of other supervisory authorities, where applicable.

9. ROLES AND RESPONSIBILITIES FOR TOP MANAGEMENT IN ORGANIZATION

- Board
  - i. General

Board members must understand their roles and responsibilities in managing ML/TF risks identified in organization.

Board members must have knowledge and awareness of the ML/TF risks associated with business strategies, delivery channels and geographical coverage of its business products and services.

Board members must understand the AML/CFT measures required by the relevant laws, instruments issued under the AMLA, as well as the industry's standards and best practices in implementing AML/CFT measures.

  - ii. Roles and Responsibilities

The Board 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 the reporting institution, including those required for risk assessment, mitigation and profiling, customer due diligence (CDD), record keeping, on-going due diligence, STR and combating the financing of terrorism;
c) Approve appropriate mechanisms to ensure the AML/CFT policies are periodically reviewed and assessed in line with changes and developments in the reporting institution's products and services, technology as well as trends in ML/TF;
d) Approve an effective internal control system for AML/CFT and maintain adequate oversight of the overall AML/CFT measures undertaken by the reporting institution;

e) Define the lines of authority and responsibility for implementing 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 Audit Committee; and
h) Establish a Management Information System (MIS) that is reflective of the nature of the reporting institution's operations, size of business, and complexity of business.

❖ Senior Management

i. General

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

ii. Roles and Responsibilities

The Senior Management has the following roles and responsibilities:

a) Be aware of and understand the ML/TF 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 the reporting institution and its geographical coverage;
c) Establish appropriate mechanisms and formulate procedures to effectively implement AML/CFT policies and internal controls approved by the Board, including the mechanism and procedures to monitor and detect complex and unusual transactions;
d) Undertake review and propose to the Board the necessary enhancements to the AML/CFT policies to reflect changes in the reporting institution's risk profiles, institutional and group business structure, delivery channels and geographical coverage;
e) Provide timely periodic reporting to the Board on the level of ML/TF risks facing the reporting institution, strength and adequacy of risk management and internal controls implemented to manage the risks and the latest development on AML/CFT which may have an impact on the reporting institution;
f) Allocate adequate resources to effectively implement and administer AML/CFT compliance programmes that are reflective of the size, nature and complexity of the reporting institution's operations and risk profiles;

g) Appoint a Compliance Officer at management level at the Head Office and designate a Compliance Officer at management level at each branch or subsidiary;
h) Ensure appropriate levels of AML/CFT training for its employees at all levels within the organisation, where relevant;
i) 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;
j) Ensure that AML/CFT issues raised are addressed in a timely manner; and
k) Ensure integrity of its employees by establishing appropriate employee assessment procedures.

10. POLICY OWNER

The owner of this policy is Board of Directors of Well Chip.

ANNEX A

Risk Assessment Table

Risk Factors	Risk Classes>	Low	Medium	High
Nationality		MY, PR, WP	Others	Countries under economic sanctions by UN ****Not eligible for transaction**
Amount		< RM25000	-	≥ RM25000 ****To Do Enhance CDD**
PEP		No	-	Yes ****Not eligible for transaction**

This Anti-Money Laundering Policy is dated 07 November 2023