ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM/ANTISOCIAL FORCE(s) POLICY

HAKKI AFRICA LIMITED

&
HAKKI AFRICA INC

KENYA | JAPAN

TABLE OF CONTENTS

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

1. PRELIMINARY

1.1 SCOPE

As a Global Policy, this applies to:

a. HAKKI AFRICA LIMITED, including its headquarters in Japan and all of its country offices, regional offices, liaison offices, and any other offices operating under the name of the HAKKI AFRICA LIMITED.

b. All National Organisations that have signed a Members' Agreement and License Agreement with HAKKI AFRICA LIMITED; and

c. All other entities that agree to be bound by the Global Policies. (together, "HAKKI AFRICA LIMITED International Entities", or may be referred to as "we" or "us" in this document).

All of the HAKKI AFRICA LIMITED International Entities shall enact their own procedures which must be in line with global procedures, regulations, or other regulatory documents that enable compliance by its employees, volunteers, interns, Directors (and/or, when applicable, contractors and other partners) with this Global Policy. Where required by law or local practices, HAKKI AFRICA LIMITED offices and Organisations may enhance the standards and requirements set out in this policy.

1.2 PURPOSE

The purpose of this policy is to strengthen and support HAKKI AFRICA LIMITED International to enable it to realise its full potential in acquiring raising and importantly to ensure the integrity, survival and growth of HAKKI AFRICA LIMITED to achieve HAKKI's vision to help 'Make More Possible' throughout the world. Through this policy HAKKI seeks to address the challenges of a changing global financial environment and meet its obligation to promote transparency and integrity and to recognise that public confidence in the Car Finance's management is paramount. The policy aims to establish best practices in an Anti-Money Laundering (AML) Policy. The policy sets out HAKKI's basic goal and purpose so as to permit examination of funds disbursements accordingly and maintain information on the purpose and objectives of HAKKI's activities.

1.3 MONEY LAUNDERING (DEFINITION)

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism

"Money laundering" shall mean;

- The conversion or transfer of property, knowing that such property is the proceeds of offence, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action;
- The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of offence;
- The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of offence;
- Participation in, and attempts to commit it and aiding and abetting, any of the acts defined in accordance with this article;

"Financing of terrorism" shall mean

"Financing of terrorism" shall mean the wilful provision or collection of funds, directly or indirectly, through 'Whatever means, with the intention that such funds be used or in the knowledge that they are or may be used, in full or in part, for the purpose of supporting terrorism, terrorist acts or terrorist organizations. Money laundering is the term used for a number of offences involving the proceeds of crime or terrorist funds. It includes possessing, or in any way dealing with, or concealing, the proceeds of any crime.

The process of money laundering has three stages:1. placement- through which the funds (often in cash) enter the financial systems;2. layering- by which the funds pass through a complex sequence of transactions designed to make it impossible for investigators to follow a trail of evidence back to the origin of the funds; and3. integration- the point at which the funds emerge from the process back into the legitimate economy in a way that they are unrecognisable as the proceeds of crime.

1.4 ANTI-TERRORISM CONSIDERATIONS

Terrorism/Antisocial force(s), in common with other criminal acts, infringes the fundamental rights of the innocent and the powerless and diverts money and attention from the real needs of the communities we are committed to ‘Making More Possible’ in. We do not engage with terrorist/Antisocial force(s) organisations or give money to partners who carry out, or fund, or advocate terrorist activity. We are fully committed to ensuring all our business processes minimise the risk of funds being diverted for terrorist or any other criminal purposes. We work within the law to ensure that our work and that of our partners is free from interference and that resources are used for the purposes intended.

2. CUSTOMER ACCEPTANCE POLICY AND RISK PROFILING

2.1 Customer Acceptance Policy

HAKKI has customer acceptance policies and procedures as well as some reasonable measures, including risk profiling, in their initial points of contact with potential customers to address different risks posed by each type of customer.

Following the initial acceptance of the customer, HAKKI continuously monitors the customer's account activity pattern to ensure it is in line with the customer profile. Unjustified and unreasonable differences should cause HAKKI to reassess the customer as of higher risk.

HAKKI should be wary and ensure that they do not fall complacent and completely rely on the customer due diligence conducted by the intermediaries or other third parties they use. The ultimate responsibility of customer due diligence always remains with HAKKI.

2.2 Individual Customer Assessment

In establishing a business relationship with an individual customer, HAKKI should obtain from the individual customer at least the full name, date of birth, identity card/passport number/identity document reference number, occupation/business, address and nationality and Tax Compliance Personal Identification Number.

2.3 HAKKI requires the individual to furnish the original and make copies of one or more of the following documents to finalize the acceptance process:

- National identity card;
- Taxation Personal Identification Number issued by the National Government of the country of operation.

2.4 Customer Due Diligence

HAKKI conducts customer due diligence and obtains satisfactory evidence and properly establishes in its records the identity and legal existence of persons applying to do business with them. Such evidence must be substantiated by verifiable documents in 2.3 above.

Unwillingness of the customer to provide the information requested and to cooperate with HAKKI's customer due diligence process may itself be a cause for suspicion. Such a situation warrants a suspicious transaction report to be submitted to the Financial Intelligence Unit of the Country of Operations.

2.5 The customer due diligence should be conducted, when:

- establishing business relationship with the customer such as opening an account or engaging in any other business dealings;
- carrying out an occasional or one-off transaction, that involves a sum in excess of USD 1,000 (or 100,000 KES or foreign currency equivalent).
- HAKKI has any suspicion of money laundering or financing of terrorism; or
- HAKKI has any doubts about the veracity or adequacy of previously obtained information.

2.6 The customer due diligence undertaken by HAKKI at least comprises the following:

- identify the customer and verify the identity of the customer using reliable, independent source documents, data or information referred to in articles 2.3;
- determine if the customer conducting business is acting on behalf of another person or beneficial owner;

- obtain information on the purpose and intended nature of the business relationship; and
- conduct ongoing due diligence and scrutiny, to ensure the information provided is updated and relevant and ensure that the transactions being conducted are consistent with HAKKI's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

2.7 Enhanced Due Diligence

HAKKI shall conduct enhanced customer due diligence for all categories of higher risk customers as deemed by HAKKI, to ensure that we are not abused by money launderers and financiers of terrorism.

2.8 Enhanced due diligence should include at least:

- more detailed information from the customer, in particular, on the purpose of the business relationship and source of funds;
- independent research and sourcing of additional information about the customer; and
- approval by senior management

3. NON-GOVERNMENT ORGANIZATIONS/FOUNDATIONS

HAKKI requires a Non-Governmental Organization or foundation establishing business relationships to furnish the constitution documents or other similar documents to ensure that it is properly constituted and registered.

The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

HAKKI takes steps to understand who is in control and makes decisions regarding the Non-Governmental Organization/Foundation, and the use of the funds.

4. CLIENT ACCOUNTS

HAKKI will satisfy itself about transactions of accounts passing through lawyers and clients' individual accountants that give cause for concern, and should report those transactions to the Financial Intelligence Unit, once suspicion is aroused.

5. SHELL COMPANIES

HAKKI should not open an account for or conduct business with a shell company, which do not conduct any commercial activities or have any form of commercial presence whichever country but are legal entities through which financial transactions may be conducted.

6. CORRESPONDENT BANKING

HAKKI should take the necessary measure to ensure that they are not exposed to the threat of money laundering and financing of terrorism through correspondent accounts they have with any other Financial Institutions.

6.1 HAKKI entering a correspondent relationship should gather and assess at least the following information on the correspondent;

- board of directors and management;
- business activities and products;
- subjected legislations, regulation and supervision
- AML / CFT measures and controls; and
- annual financial and operational reports.

HAKKI should establish or continue a correspondent banking relationship with the correspondent only if it is satisfied with the assessment of the information gathered.

HAKKI should also document the responsibilities of the respective parties in relation to the correspondent banking relationship.

The decision and approval to establish or continue a correspondent banking relationship should be made at the Senior Management level.

HAKKI should ensure that such correspondent banking relationships do not include correspondent banks and financial institutions that have no physical presence and which are unaffiliated with a regulated financial group.

HAKKI should exercise enhanced due diligence with respect to correspondent banks and financial institutions which allow direct use of the correspondent accounts by their customers to transact business on their own behalf such as payable-through accounts. HAKKI should implement customer due diligence for such customers as required for intermediaries introducing business.

HAKKI should pay special attention to correspondent relationships with correspondent banks and financial institutions from countries which have insufficiently implemented the internationally accepted AML / CFT measures. Enhanced due diligence is needed to assess the money laundering and financing of terrorism risks.

7. REMITTANCE/WIRE TRANSFER

HAKKI conducting or participating in an outgoing remittance/wire transfer transaction should include with it the necessary originator's name, address, account number, identification number or customer reference number and the details of the transaction.

HAKKI facilitating or acting as intermediary to a remittance/wire transfer transaction should ensure such originators' information is still retained with the remittance/wire transfer message.

HAKKI receiving a remittance/wire transfer message with incomplete originators information should conduct enhanced due diligence and may consider it as a factor of suspicion.

It would be deemed unnecessary to include all the above information in the message accompanying a remittance / wire transfer transaction of less than USD 1,000 (100,000KES or its equivalent in any other currencies).

HAKKI should pay attention to wire transfers by higher risk customers and consider such factors as the name of the beneficiary, the destination and amount of the remittance/wire transfer. The customer should be asked to provide further explanation of the nature of any remittance/wire transfer which is inconsistent with the customers usual business/activity.

8. MONEY CHANGERS

HAKKI must pay special attention to and ensure that the moneychangers who maintain accounts with them are licensed and only conduct legitimate currency exchange transactions. HAKKI should ensure that the nature and volume of transactions in the moneychangers account reflect the nature of their business.

If HAKKI identifies any discrepancies in the activities of the moneychangers account, they should submit a suspicious transaction report to the Financial Intelligence Unit.

9. RECORD KEEPING

9.1 Records

HAKKI should keep all records, documents and copies of documents involved in all forms of transactions for at least 5 years after the date of the transaction. All identification data, files, records, documents, business
Correspondence and copies of documents obtained on a customer must be maintained for at least 5 years after the accounts have been closed or the business relations with the customer have ended.

Where the records are subjected to an on-going investigation or suspicious transaction report submitted, they shall be retained beyond the stipulated retention period until it is confirmed by the relevant authority that such records are no longer needed.

HAKKI should retain the relevant document as originals or copies, on microfilm or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner

HAKKI should conduct on-going due diligence for all customer relationships, using a risk-based approach. The risk-based approach to on-going customer due diligence should ensure that the risk profile of the customer is up-to-date.

HAKKI shall pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, to determine whether the transactions have an apparent or visible or lawful purpose.

9.2 Existing Accounts

HAKKI should take necessary measures to ensure that the records of existing customers remain up-to-date and relevant. Further evidence of the identity of existing customers should, where necessary, be obtained to ensure compliance with customer due diligence standards set by the present document. HAKKI should conduct regular reviews on existing records of customers. These reviews should at least, be conducted when:

- a significant transaction is to take place;
- there is a material change in the way the account is operated;
- the customer's particulars change substantially; or
- information held on the customer is insufficient.

In the event that the circumstances above do not arise, HAKKI should, based on risk assessment, obtain additional information in line with their current standards from those existing customers that are of higher risk.

9.3 Audit Trail

HAKKI must ensure that the retained documents and records are able to create an audit trail on individual transactions that would enable the supervisory and enforcement agencies to trace funds.

The records kept must enable HAKKI to establish the history and nature of and reconstruct each transaction. The records shall include at least:

- the origin of funds, such as method of receipt and or name of originator of wire and transfer;
- the identity of the person undertaking the transaction if not an account holder;
- the type of transaction; and
- the instruction and the destination of fund transfers.

9.4 Management Information System and Special Attention

HAKKI should put in place an adequate management information system for identifying and detecting transactions that we suspect or have reasonable grounds to suspect related to proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism. The management information systems should provide HAKKI timely information on a regular basis to enable them to detect suspicious activity.

HAKKI should conduct on-going due diligence with regards to business relationships and transactions with individuals, business, company and financial institutions from countries which have insufficiently implemented the internationally accepted AML / CFT measures. Such business relationships and transactions should require HAKKI to make further detailed inquiries, about their background and purpose, to establish the findings in writing, and to make them available to the competent authorities.

9.5 Suspicious Transaction Reporting

HAKKI are required to establish a reporting system and to promptly submit suspicious transaction reports to the Financial Intelligence Unit when any of its employees suspects or has reasonable grounds to suspect that the transaction involves proceeds of an offence or are related to money laundering or financing of terrorism or they have any other grounds of suspicion about a customer transaction.

Some examples of suspicious transactions are listed in Clause 1.3. These examples are not exhaustive and only provide examples of basic ways in which money may be laundered or used for the financing of terrorism. HAKKI should establish their own internal guidelines on suspicious transaction reporting incorporating the relevant provisions in the Law on Anti-Money Laundering and Combating the Financing of Terrorism and the relevant provisions in the present Document including a list of suspicious transactions indicators.

Other suspicious activities that HAKKI considers are:

- Entering partnership arrangements with organisations that may be fronts for criminal activities.
- Use of an alternative banking system to move funds to areas of operation.
- Use of conduits for funding (money held for the organisation in a conduits name).
- Use of couriers to transport cash or valuables (gold or commodities) into areas of operation.
- Payment of facilitation charges in an area of operation where these amount to a private benefit rather than a lawful tax or duty.
- Suppliers may be set up to provide such money laundering facilities, so we must ensure that due tender and procurement process is followed and suppliers are confirmed as bone fide.
- Operating trading outlets with donated goods with insufficient internal controls. (No purchase invoices to match any sudden increase in cash income.)
- Operation of trading subsidiaries with insufficient internal controls (can be used to receive loans and repay loans to confuse the audit trail).

- Interest-free loans
- Requests to use HAKKI as a conduit and pass money through it.

HAKKI should also submit a Suspicious transaction report when a new or existing customer fails to complete the customer due diligence without reasonable excuse, regardless of whether HAKKI accepts, rejects, continues or terminates the business relationship with such customer.

10. REPORTING MECHANISMS

HAKKI shall appoint an officer at the senior management level to be the compliance officer to appoint as a Money Laundering Reporting Officer (‘MLRO’) to be responsible by law for receiving suspicion reports in an organisation and for passing these on to the Financial Intelligence Unit.

The employees of HAKKI should report suspicious transactions to the compliance officer even if they do not know precisely what the underlying unlawful activity is or whether such activities have occurred.

Once the suspicious transaction report reaches the compliance officer, the compliance officer should promptly evaluate and establish whether there are reasonable grounds for suspicion and promptly, within 24 hours, submit the suspicious transaction report to the Financial Intelligence Unit the compliance officer considers, and records his/her opinion, that such reasonable grounds do not exist.

The Suspicious transaction report submitted by the compliance officer shall be in writing and using the approved form as attached in Clause 1.3 and delivered by safe hand, secure mail or secure electronic transmission to the Financial Intelligence Unit.

HAKKI should ensure that when preparing and submitting a suspicious transaction report, information about the suspicious transaction, the customer and the reporting of the matter remains confidential and is available only to staff, on a strict 'need to know’ basis.

HAKKI should authorize their compliance officer to cooperate with the Financial Intelligence Unit in providing additional information and documentation requested and to address further enquiries with regard to the submitted suspicious transaction report.

11. PROHIBITION OF TIPPING OFF

HAKKI must ensure that the reporting system put in place for the submission of suspicious transaction reports is operated in a confidential and systematic manner.

HAKKI must ensure that the customer reported on, is not informed of the existence of the suspicious transaction report or does not become aware of the suspicious transaction report. Staff should be made aware that article 15 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism prohibits any individual having knowledge of a suspicious transaction report from communicating such information or reports to any natural or legal persons other than the Financial Intelligence Unit, except where so authorized by the Financial Intelligence Unit.

11.1 Remedial Measures

HAKKI should maintain a complete file on all suspicious transaction reports submitted by their employees to its compliance officer and such reports that have been further submitted to the Financial Intelligence Unit.

HAKKI must take reasonable measures to ensure that all their officers and employees involved in conducting or facilitating customer transactions are aware of these reporting procedures.

12. DETECTION AND REPORTING OF THE FINANCING OF TERRORISM

HAKKI should take the necessary measures to ensure compliance with the United Nations Security Council (UNSC) Resolutions and relevant regulations and legislation on financing of terrorism.

HAKKI should extend the suspicious transaction report system and mechanism to cover suspicion of financing of terrorism.

HAKKI should maintain a database of names and particulars of terrorists in the United Nations list and they should consolidate their database with the other recognized lists of designated persons. Information contained in the database should be updated and relevant and made easily accessible to employees for the purpose of identifying suspicious transactions and freezing accounts' funds.

HAKKI should conduct checks of the names of new and existing customers against the names in the database. If there is a name match, HAKKI should take reasonable measures to verify and confirm the identity of its customer. If the customer and the person listed in the database are the same person HAKKI should immediately freeze the customer's accounts and inform the Financial Intelligence Unit. Where HAKKI suspects that a transaction is terrorist-related, it should make suspicious transaction reports to the Financial Intelligence Unit within 24 hours.

13. RISK MANAGEMENT OPERATIONAL MEASURES

The Directors of HAKKI should establish an effective internal control system for AML/CFT compliant with legal and regulatory requirements. It is the responsibility of the senior management to ensure such internal controls are implemented effectively.

The Directors and senior management should be aware of and understand the AML/CFT measures required by law, the regulators, the industry's standards and best practices as well as the importance of putting in place AML/CFT measures to prevent HAKKI from being abused by money launderers and financiers of terrorism. The Directors should oversee the overall AML/CFT measures undertaken by HAKKI.

The Directors and senior management should be aware of the money laundering and financing of terrorism risks associated with all its business products and services.

The Directors should ensure that HAKKI has, at the minimum, policies on AML/CFT procedures and controls. The senior management should assist the Directors in formulating the policies and ensure that the policies are in line with the risks associated with the nature of business, and complexity and volume of the transactions undertaken by HAKKI.

The Directors should ensure that the procedures for AML/CFT measures including those required for customer acceptance policy, customer due diligence, record keeping, on going monitoring, reporting of suspicious transactions and combating the financing of terrorism are in place.

The Directors should assess the implementation of approved AML/CFT policies by the senior management via periodic reports.

The Directors should define the lines of authority/chain of command and responsibilities 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. The Directors should ensure the:

- appointment of a compliance officer to ensure that the policies, procedures and controls are in place; and
- effectiveness of internal audit in assessing and evaluating the controls in place to counter money laundering and financing of terrorism.

The Directors should review and assess the policies and procedures on the AML/CFT measures in line with changes and developments in its products, services and technology systems, as well as trends in money laundering and financing of terrorism techniques. The senior management should implement the necessary changes to the

policies and procedures with the approval of the Directors to ensure that the current policies are sound and appropriate.

The Directors and senior management should ensure that there are adequate ongoing AML/CFT training programs for their staff in place.

14. HAKKI STAFF OBLIGATIONS

14.1 Staff Integrity

Senior management should ensure that HAKKI establishes an employee assessment system, approved by the Directors, to adequately screen its employees, both existing and new, to ensure that the integrity of its employees is not compromised. The employee assessment system should at least examine personal information including criminal records, employment and financial history of its new employees as part of the recruitment process.

Obligations of HAKKI staff include:

- not to assist in the money laundering process through acquiring, concealing, disguising, retaining or using the proceeds of crime;
- not to prejudice an investigation; and
- not to contact any person who has been suspected of, and reported for, possible money laundering in such a way as to make them aware of the suspicion or report (“tipping off”) It is important to note that the law requires all cases of suspicion to be reported, regardless of size.

14.2 The Compliance Officer

Senior management is responsible to appoint the compliance officer at Senior Management level with the approval of the Directors. Senior management should ensure that the Compliance Officer effectively discharges his/her AML/CFT responsibilities. The compliance officer should act as the reference point for the AML/CFT measures HAKKI has established, including employee training and reporting of suspicious transactions.

HAKKI should upon the appointment or change in the appointment of the Compliance Officer inform the Financial Intelligence Unit of the details of the Compliance Officer including the name, address, telephone number; facsimile number, e-mail address and other relevant background information.

HAKKI should ensure that the roles and responsibilities of the Compliance Officer are clearly defined and documented. The roles and responsibilities of the AML/CFT compliance officer should include at least ensuring:

- implementation of the policies for AML/CFT measures;

- the appropriate AML/CFT procedures including customer acceptance policy, customer due diligence, record keeping, ongoing monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- regular assessment of the AML/CFT mechanisms to ensure that the mechanisms are sufficient to address the changing trends;
- the channel of communication from the respective employees to the Compliance Officer is secured and that any information is kept confidential;
- compliance with the AML/CFT legal and regulatory requirements;
- all employees are aware of AML/CFT measure including policies, control mechanisms and channel of reporting to ensure the effectiveness of such measures;
- the identification of money laundering and financing of terrorism risks associated with new products or services or arising from HAKKI's operational changes, including the introduction of new technology and processes.

Compliance Officer(s) should have the necessary knowledge and expertise to effectively discharge his/her responsibilities, including knowledge on AML/CFT obligations required under the relevant laws and regulations and an understanding of Developments in money laundering and financing of terrorism techniques.

15. STAFF TRAINING AND AWARENESS PROGRAMME

HAKKI should have an awareness and training programme on AML/CFT practices and measures for its employees. The training and awareness programme must be extended to all new and existing employees.

Senior Management should ensure that proper channels of communication are in place to inform all levels of employees at HAKKI of their AML/CFT policies and procedures.

Employees should be aware of AML/CFT policies and controls in place and the requirements as specified in the present Document and at HAKKI AML/CFT internal manual.

HAKKI should at least adapt to their needs the following training packages for the various sectors of employees within their institutions:

- New Employees

A general background to money laundering and financing of terrorism, the requirement and obligation to identify and report suspicious transactions to the appropriate designated point within HAKKI, and the importance of not tipping off the customer.

- Front-Line Employees

Employees who deal directly with the customers as the first point of contact with potential money launderers and financiers of terrorism should be trained in identifying suspicious transactions, the measures to be taken once a transaction is deemed to be suspicious, factors that may give rise to suspicions, large cash reporting and enhanced customer due diligence.

- Employees - Account Opening/New Customers

Employees, who are responsible for account opening or the acceptance of new customers, should at least receive the equivalent training given to front-line employees. In addition, they should be trained in customer identification and verification, opening of accounts and establishing business relationships with customers.

- Supervisors and Managers

Supervisors and managers should receive a higher level of instruction covering all aspects of AML/CFT procedures including the penalties for non-compliance to the AML/CFT requirements, and procedures in addressing combating the financing of terrorism issues.

These training and awareness programmes should be conducted regularly with refresher courses provided for employees. New employees should be trained within three months of commencement of employment and front-line employees, supervisors and managers should have refresher training annually.

16. INTERNAL AUDIT

The Directors should ensure that internal auditors undertake an audit of the effectiveness and compliance with AML/CFT requirements of the relevant laws and regulation as well as the present Document.

The Director should ensure that the roles and responsibilities of the internal auditor are clearly defined and documented and at least include:

- testing the effectiveness of the policies, procedures and control for AML/CFT measures; ensuring effectiveness of AML/CFT control mechanisms including the appointment of compliance officers, staff training and awareness programmes, employee screening mechanisms and AML/CFT internal manual; and
- ensuring that measures put in place are in line with current developments and changes of the relevant AML / CFT requirements.

HAKKI should inform the Financial Intelligence Unit upon the appointment or change in the appointment of the internal auditor and on the approach and procedures adopted by the internal auditors.

The internal auditor should submit a written report on the audit findings to the Directors on a regular basis. The annual audit report should highlight inadequacies of any AML/CFT measures and control systems within HAKKI, and the Directors should ensure that necessary steps are taken to rectify the situation. Audit findings and reports on AML/CFT should be submitted to the Central Bank of the country of operations after consideration by the Directors.

PREPARED BY: AMY NJAMBI