Telecel Ghana Mobile Financial Services Policy Standard

Anti-Money Laundering & Counter Terrorist Financing

Owner:	Champion:	Day to day contact:	Version:
Philip Amoateng Director, Mobile Financial Services	Anita Ayivi AML Manager	Mawuena Agbogah AML Specialist	Version 1.0

Objective/Risk:	Scope
Implementation of risk-based controls that deter abuse of Telecel financial services by money launderers and those involved in financing terrorism. The Anti-Money Laundering & Counter Terrorist Financing (AML/CTF) Policy Standard is intended to ensure that Telecel and Telecel Ghana Mobile Financial Services (TGMFS or Telecel Cash) uphold this commitment by complying with both the specific requirements and the spirit of all relevant Ghanaian and international Anti-Money Laundering and Counter Terrorist Funding Laws, Regulations and Standards.[1] This includes compliance with the provisions of the Anti-Money Laundering Act 2020 (Act 1044), the Anti- Money Laundering Amendment Act 2014 (Act 874) the Anti- Money Laundering Regulations, 2011 (L1 1987), the Anti- Terrorism Act, 2008 (Act 762), the Anti-Terrorism (Amendment Act, 2012 (Act 842) and all existing and future directives or guidelines of the Bank of Ghana on AML. This is to avoid reputational damage to Telecel Ghana and Telecel Ghana Mobile Financial Services by ensuring the implementation of risk-based controls that deter abuse of Telecel Cash by money launderers and those involved in financing terrorism. It is also to protect Telecel, its employees, contractors, third party agents and third-party partners from inadvertently committing money laundering and terrorist financing offences.	**This Policy Standard applies to** All Ghana Telecommunications Company Limited (TELECEL GHANA) and Telecel Ghana Mobile Financial Services (TGMFS) employees and contractors. • . • Third party partners and Agents providing Telecel mobile financial services. • Directors, officers, employees, contractors, and third-party agents of these companies. **Services:** All financial services or other products that are mandated to implement AML/CTF controls
Compliance levels are monitored and reviewed by appropriate governance bodies. Any breach will be treated as a serious disciplinary offence and may be subject to disciplinary action in accordance with the provisions of TELECEL GHANA's disciplinary policy.	

Contents

1. Definitions

AML /CTF – Anti-Money Laundering and Counter Terrorist Financing.

AML laws – local or international laws and regulations relating to AML/CTF and local AML laws which are applicable to the relevant Telecel company or third-party partner.

Beneficial Owners - A beneficial owner is an individual who ultimately owns or controls an entity which is a customer or third-party partner or an individual on whose behalf a transaction is being conducted. Under the Global AML/CTF Policy, beneficial owners are defined as individuals owning or controlling more than 25% of a business, corporate or partnership.

Cash Threshold Reporting (CTR)- is the obligation for the automatic reporting of a transaction to a relevant competent authority based on the size and type of transaction or a series of connected transactions. Suspicion in relation to the transaction(s) is not required to obligate the reporting.

Financial Action Task Force (FATF) – an inter-governmental body which sets standards and develops and promotes policies to combat money laundering and terrorist financing.

Mobile money agent – any third party in a temporary or permanent customer-facing role, conducting cash-in and/or cash-out mobile money transactions, and/or registering new customers, and/or providing customer service tasks. It can include agents, aggregators, super agents, freelancers, walkers, or brand ambassadors.

Money laundering – A criminal process to disguise the true ownership and control over proceeds of crime, making such proceeds appear to come from a legitimate source.

Money Laundering Reporting Officer/Nominated Officer (MRLO) – A regulated position held by an individual in a business, required to receive and investigate all internal suspicious activity reports, and make suspicious activity reports to the Financial Intelligence Centre as appropriate.

Politically Exposed Person (PEP) – individuals who are or have been entrusted with prominent public functions in any country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

Regulated Service – a product or service offered by a Telecel Ghana Mobile Financial Services to sell regulated financial products which mandate specific AML/CTF controls. This can include mobile wallets, mobile money, payments, international money transfer, loans, and insurance products.

Relative and Close Associate (RCA) – are a type of politically exposed person deemed as such through a family or friendship connection to a PEP.

Terrorist financing – A criminal process by which terrorist individuals and groups fund their operations, activities, and terrorist acts.

Third Party – any non-Telecel entity that undertakes regulated business on behalf of Telecel. It can include hubs, partners, Agents, or merchants.

Telecel Ghana Mobile Financial Services (TGMFS) – Telecel Cash

2. Introduction

Harnessing our technology to create new and innovative digital services to improve the lives of our customers is at the heart of Telecel. As a financial service provider, Telecel Cash has an important role to play in furthering the international efforts against money laundering and terrorist financing, this is key to the Telecel Purpose of delivering positive social outcomes and acting with integrity wherever we operate,

It is vital these ambitions and benefits are not compromised by the same services being abused for criminal purposes. We take a robust approach to the prevention, detection and reporting of money laundering and terrorist financing. Failure to implement effective anti-money laundering and counter terrorism financing controls, as set out in this policy, could lead to regulatory and/or criminal action against both TELECEL GHANA, Telecel Cash and/or individual stakeholders. It may also lead the detriment of customers, monetary penalties, diminished commercial performance and a harmful impact on the reputation of Telecel Cash and TELECEL GHANA.

All Telecel employees and contractors are required to report any suspicion of money laundering or terrorist financing to the Money Laundering Reporting Officer.

HR must have appropriate disciplinary policies in place to ensure that overt breaches of the AML/CTF Policy are subject to appropriate disciplinary action.

3. Roles and responsibilities

3.1 CEO & Board of Directors

The CEO of TELECEL GHANA and the Board of Directors of Telecel Ghana Mobile Financial Services have ultimate responsibility for compliance with the AML/CTF Policy and Ghana's AML laws and regulations and any other relevant legislation.

3.2 AML Governance Committee

The AML Governance Committee, under delegation from the Board of Directors, is responsible for coordinating, monitoring the nature and extent of risk exposure against risk appetite and ensuring compliance with AML laws and regulations.

3.3 Director of Telecel Cash

The Director of Telecel Ghana Mobile Financial Services is responsible for implementing AML/CTF policies, controls, and procedures, ensuring all relevant employees and agents receive appropriate AML/CTF training, and must remain vigilant in detecting non-compliance by employees or a failure to follow AML/CTF procedures.

3.4 Policy Owner

A member of ExCo must formally act as the AML/CTF Policy Owner, accountable for policy implementation across TELECEL GHANA.

The Policy Owner must ensure that the Policy Champion has sufficient resources (including analytical staff) to carry out their duties effectively and has access to all information/data required.

3.5 AML/CTF Policy Champion (MLRO)

The AML Manager, who is a subject matter expert is responsible for implementation of the AML/CTF Policy, and day to day management of the AML compliance programme.

The Board of Telecel Ghana Mobile Financial Services, with the assistance of the AML/CTF Policy Owner and AML/CTF Policy Champion, is responsible for ensuring that Telecel Ghana Mobile Financial Services is compliant with the AML/CTF Policy Standard, AML legislation and regulations, The AML/CTF Policy Champion must identify and document national and international AML/CFT legislation and regulations that must be complied with by their entities, and ensure such documentation remains contemporary, with a formal review at a minimum annually. The documented regulatory assessment must clearly outline where legal liability rests including where relevant legal liability on individual role holders, such as Board members, CEO, MLRO etc exists.

.

The AML/CTF Policy Champion must hold seniority and experience to act under their own authority. They must freely report to the AML/CTF Policy Owner and relevant Board committees with sufficient independence from the commercial business. The AML/CTF Policy Champion and any appointed Deputies are required to have completed specialist AML training in the form of an internationally recognised AML/CTF qualification.

3.6 Employees of TELECEL GHANA

All employees must be vigilant in the fight against money laundering and must do their utmost to prevent Telecel Cash from being used for money laundering and terrorist financing activities.

Compliance with the AML/CTF Policy and procedures is mandatory and is a condition of employment. Failure to adhere to the AML/CTF Policy and procedures may result in disciplinary action including termination of employment.

Recognising the importance of knowing our employees just as we know our customers, Telecel Cash acknowledges that insiders can pose the same money laundering risks as external customers. To comply with the AML/CFT regulation 2011 (as amended), The Human Resources (HR) department has implemented adequate policies, procedures, and controls, including thorough screening procedures, to ensure high standards when hiring employees.

TELECEL GHANA's recruitment policy incorporates a detailed screening procedure for new employees. This policy is strictly followed to ensure that recruits not only possess exceptional skills but also demonstrate good character, high ethical standards, honesty, and integrity.

During the recruitment process, HR department is responsible for confirming new employees subject to positive performance and character reports from their former employers and personal referees. Additionally, verification of credentials is conducted by contacting awarding institutions. All information provided by prospective employees is thoroughly verified during the probation period. Any changes in the provided information, including additional qualifications obtained after confirmation of appointment, are verified against appropriate documents and issuing institutions.

Furthermore, HR conducts background checks to verify the identities of job applicants and also implements ongoing monitoring of employees. These measures are essential to prevent the risk of hiring questionable candidates and uncover negative behaviours that may occur after the recruitment process is concluded as well as ensuring employees continually meet TELECEL GHANA's standards of integrity and competence.

The HR department also has a comprehensive Code of Conduct which embodies all the criteria for 'fit and proper' employees.

Monitoring Employee Conduct

According to the BOG/FIC (AML/CFT&P) Guideline, 2022, every employee's accounts must be monitored for potential signs of money laundering and subjected to the same AML/CFT&P procedures applicable to other customer accounts. This monitoring is supervised by the MLRO.

The AML team is responsible for ensuring that staff accounts receive the same level of due diligence and monitoring as external customers. Any deviations from the normal account patterns must be promptly reported to the MLRO for further investigation. The MLRO's account must be reviewed by the Head of Internal Audit.

Performance Review and AML/CFT Integration

As per the BOG/FIC (AML/CFT&P) Guideline, 2022, the HR department incorporates AML/CFT performance reviews into Telecel Cash's employees' annual performance appraisals. This includes assessing employees' attendance at AML/CFT training sessions and the number of AML/CFT infractions in their Key Performance Indicators (KPIs).

By integrating AML/CFT considerations into performance evaluations, Telecel Cash emphasises the importance of maintaining a strong AML/CFT culture within the organization and reinforces the commitment to ensuring compliance with regulatory requirements.

3.7 Agents & Other Third Parties Who Conduct Activities Material to the AML/CTF Programme

All Agents and their employees must be vigilant in the fight against money laundering and terrorist financing and must do their utmost to prevent Telecel Cash from being used for money laundering and terrorist financing activities.

Compliance with AML/CTF policy and procedures is mandatory and is a condition of working with Telecel; contract clauses must clearly mandate this Failure to adhere to the AML/CTF policy and procedures will result in action including, where appropriate, contract termination.

4. Risk-Based Approach

In line with international best practice as set in the Financial Action Task Force (FATF) Recommendations, Telecel has adopted a risk-based approach (RBA) to its AML programme controls. This is to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate and proportionate with the risks identified, and to ensure resources are allocated in the most effective way.

An entity wide AML/CTF Risk Assessment is conducted at least annually with additional updates in reaction to any clear material risk factor changes (i.e., fundamental changes to customer or product mix, large political or regulatory or security changes,) Results of the Risk Assessment must be shared with relevant governance committees and stakeholders.

As part of the risk-based approach to AML/CTF Telecel Cash must risk assess and attach a proportionate risk rating to all customers (including entities) and third parties undertaking elements of the AML programme. This risk rating process must be conducted at onboarding stage, and again on an ongoing basis taking account of behaviours and transactions observed, with low risk, standard risk and high-risk customers/partners identified. The risk rating assigned must inform the level of due diligence conducted, the due diligence refreshment timelines and ongoing monitoring that is conducted on the customer/third party. The higher the risk rating the more enhanced the due diligence and monitoring must be.

As set out later in this policy, certain factors, such as PEP status, always mandate a high-risk rating and necessitate additional due diligence and ongoing monitoring.

Additional AML/CTF Policy standards may be mandated by the Policy Champion in relation to products that are deemed as high risk for money laundering and/or terrorist financing. This is in order to ensure proportionate additional controls are in place. Example products include gambling and International Money Transfer. Where such standards are issued, they will be clearly communicated to the AML/CTF Policy Owner, AML/CTF Policy Champion and Head of Product & Services.

5. AML/CTF Policy and Procedures

Telecel Ghana Mobile Financial Services is required to have an AML/CTF policy, procedures and controls that enable the management and effective mitigation of risks that have been identified, and to comply with the Global AML/CTF Policy and with local regulatory and legislative requirements. This includes ensuring all required regulatory licenses to operate relevant services are gained and maintained and that all licensing requirements mandated by said licenses are met on an ongoing basis.

The AML Policy and Procedures must be approved by the AML Governance Committee on behalf of Telecel Ghana Mobile Financial Services Board of Directors and also approved by the Policy Owner on behalf of Exco.

The AML Policy and Procedures must be reviewed annually (or more frequently in relation to a regulatory change) and where appropriate updated, to consider findings from the last AML Risk Assessment. Any material changes made to the Policy must instigate a renewed policy approval process.

The Procedures must set out the potential corporate consequences (and personal consequences for relevant stakeholders), of failure to adhere to relevant AML/CTF legal and regulatory requirements.

The procedures and controls must be approved by the AML/CTF Policy Champion, and Policy Owner.

6. Policy Principles

Telecel Ghana Mobile Financial Services must have in place the following:

6.1 AML Resource

Telecel Ghana Mobile Financial Services must formally appoint:

- A member of ExCo to act as the AML/CTF Policy Owner
- AML/CTF Policy Champion/ Money Laundering Reporting Officer (MLRO)

The MLRO/AML/CTF Policy Champion must have the necessary time, access, and resource to effectively implement and monitor the AML programme. This includes sufficient staff numbers to implement an effective and

proportionate AML/CTF programme. In line with the Risk Based Approach, resource requirements and allocation must be kept under constant review as AML/CTF risks and product offerings change – a review of resources dedicated to AML/CTF compliance must be completed at least annually as part of MLRO report process.

6.2 Customer due diligence (including Know Your Customer ("KYC") ("SDD") ("CDD") & ("EDD)

A key foundation of all effective AML/CTF programmes is knowing sufficient information on all customers (of all types) to enable appropriate screening, risk assessment and monitoring. Collection and verification of identity and other information provided by customers at on-boarding and throughout the customer relationship is therefore crucial.

The extent of the identity and additional information obtained should be determined on a documented risk-based approach, considering risk factors such as:

- The nature of the product or services that will be available to the customer.
- The size and nature of the types of transactions that may be permitted
- Any relevant external factors relevant to the customer base in question (i.e., geographical factors, external security factors etc)
- The nature and length of any existing or previous relationship with the customer.
- The nature and extent of any assurances from other regulated businesses that can be relied upon.
- Whether the customer is physically present. The identity checks carried out on non-face to face applicants should be designed to mitigate increased risks posed by non-face to face business e.g., identity theft.

The risk-based rationale must be documented, and the activities and transacting levels permitted for each type of customer must be proportionate to the extent of information obtained and verified.

All entities must apply customer identification and verification measures to customers when it does any of the following:

a) establishes a business relationship.
b) carries out an occasional transaction; or
c) doubts the veracity of documents or information previously obtained for the purpose of identification or verification.

Where the entity is unable to apply proportionate customer identification and verification measures in relation to a customer (which for the avoidance of doubt includes natural persons and entities), it must:

a) not establish a business relationship or carry out a transaction with the customer.
b) terminate any existing business relationship with the customer.
c) consider whether it ought to be making a suspicious activity report in accordance with regulatory obligations.

I. Standard AML/CTF Risk Customers - Customer Due Diligence (CDD) Standards -Personal Customers (individuals)

For those customers assessed by the documented risk-based approach to be a standard AML/CTF risk then standard Customer Due Diligence (CDD) requirements must be met.

At a minimum, the following identity information must be obtained for all customers as standard due diligence:

- Full Name
- National ID Card details
- Date of birth
- Address
- Telephone Number
- Nationality

For standard customer due diligence (CDD), at a minimum, customer name and date of birth must always be verified using a credible and independent source, with evidence of verification retained (for example ID copy held or evidence of verification against a third-party database retained).

II. Low AML/CTF Risk Customers and Products – Simplified Due Diligence (SDD) Standards -Personal Customers (individuals)

There may be scenarios where the documented risk-based assessment of customers and products determines that Simplified Due Diligence (SDD) is appropriate and proportionate, considering AML/CTF risk and financial inclusion factors. This will only be by exception, and it must be clearly demonstrable through a documented assessment that:

- the underlying AML/CTF risk from the relevant products and customers is demonstrably low,
- that regulatory standards explicitly allow SDD on relevant customers and products
- that the application of CDD measures would exclude a significant number of potential customers and therefore harm financial inclusion efforts.

Any decision to apply simplified due diligence methods on new and existing customers must be explicitly approved by the CEO or the Director of Telecel Cash and AML Governance Committee following documented consultation with the Policy Champion.

At a minimum, the following identity information must be obtained for all SDD customers. However, where SDD is approved evidence of verification of the information collected is not strictly required:

- Full Name
- National ID Card details
- Date of birth
- Address
- Nationality

Identifying non-personal customers (e.g., businesses, merchants, Ecommerce businesses, mobile money agents, customers seeking PayBill, bulk disbursement, and/or "buy goods" accounts).

When entering into a business relationship or performing an occasional transaction with a non-personal customer, tailored customer due diligence is required to prevent unlawful use of Telecel Cash services. This is in order to gain sufficient understanding of the customer to be able to properly assess the money laundering and terrorist financing risks associated with the business relationship, and to take appropriate steps to mitigate the risk.

All entities applying this policy are required to:

- Identify and verify the customer appropriately, including:
    - Name, legal form, and proof of existence – verification could be obtained, through a certificate of incorporation, corporate registration documents including business regulations, Form A and Form 3 where applicable, other documentation from a reliable independent source proving the name, form, and current existence of the customer.
    - How long the business has been in operation.
    - The ownership and control structure, and the names of the relevant persons having a senior management position in the legal person or arrangement (e.g., directors in a company. Take copies of the IDs of the directors.
    - Shareholders and their nationalities.
    - The address of the registered office, and, if different, a principal place of business.
    - TIN and Tax Certificate.
    - The nature and purpose of the business.
    - Existing size and sales turnover.
    - Expected value and volume of transactions through the service
    - *If a regulated entity*; name of regulator and up-to-date licence (this should be kept up to date)
    - *If the regulated entity is subject to anti-money laundering obligations:* Evidence that it has taken steps to meet its AML obligations (e.g., name of MLRO, AML/CTF Policy etc).

- Identify the beneficial owners of the customer (all-natural persons holding an ownership or control interest of 25% equity more) and take reasonable measures to verify the identity of such persons (e.g., make use of records of beneficial ownership information in the public domain, request business registration documents where ownership information is typically stated) and obtain and verify the same information about that beneficial owner as it would for an individual customer. Take copies of the IDs of the beneficial owners.
- *For merchants*: A merchant category code must also be determined and assigned.

III. Higher risk customers (Individuals, business customers and 3rd parties such as agents) and Enhanced Due Diligence

Telecel Ghana Mobile Financial Services must identify higher risk customers as part of an AML risk assessment, both at onboarding and on an ongoing basis (e.g., through on-going monitoring)

As standard, Political Exposed Persons (PEPs), Relatives and Close Associates (RCA's) of PEPs and customers confirmed as appearing on other relevant watchlists (as defined proportionally locally) must be treated as high-risk customers and be subject to:

- enhanced due diligence,
- MLRO customer acceptance processes and
- enhanced on-going monitoring.

Where higher risk services (as identified in risk assessment by the AML team) or higher-level transaction limits are being made available to customers, or customers demonstrate higher risk customer behaviours (could include high cumulative values being transacted or unusual transaction patterns compared to what is known about the customer) then enhanced customer due diligence measures beyond standard due diligence must take place.

These enhanced measures must include collection of copies of identity documents in addition to the KYC requirements for a standard due diligence. These documents include:

- Tenancy Agreement
- Utility Bill
- Income Tax Certificate
- Bank statements
- Reference letter from another Tier 2 customer (who has been on VFCASH for 6months or more) or Employer's reference letter.

.

In addition, proportionate additional measures such as the below should be applied:

- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining the approval of senior management to continue or end the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination

IV. CDD for beneficiaries of life insurance policies

Life insurance businesses should, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measures on the beneficiary(ies) of life insurance policies, as soon as the beneficiary(ies) are identified/designated:

a) For beneficiary(ies) that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person.

b) For beneficiary(ies) that are designated by characteristics or by class (e.g., spouse or children at the time that the insured event occurs) or by other means (e.g., under a will) – obtaining sufficient information concerning the beneficiary to be satisfied that it will be possible to establish the identity of the beneficiary at the time of the pay-out.

The verification of the identity of the beneficiary(ies) should occur at the time of the pay-out.

V. Unregistered customers

Unregistered Customers pose a higher risk to Telecel and require tailored controls. If unregistered customers have been authorised to receive money, they must be required to provide identification in order to cash the funds and be subject to transaction limits more stringent than a registered customer. No other services should be provided to unregistered customers without the prior written approval of the Policy Owner.

VI. Refreshment of Due Diligence

Telecel Ghana Mobile Financial Services must have documented, and risk based, due diligence refreshment processes for all customer relationship types. Due diligence should be refreshed more frequently the higher the risk profile of the customer. These processes must reflect the overall AML/CTF risk of the customer/entity type (including agents). Ongoing risk profiling of customers must inform the nature and timing of refreshment of due diligence, with any high-risk customers (either identified through screening, external information, or the nature of their transactions) subject to a EDD process once identified. If permitted by regulation, and justifiable through a documented risk rationale, it may be that lower risk customers are only asked to refresh due diligence based on defined trigger events.

6.3 Third Party management

Robust and effective controls must be in place for all Third Parties that are engaged in connection with Regulated Services. This is of particular importance where the Third Party is to undertake regulated AML/CTF activities on behalf of Telecel (for example, mobile money agents who register customers and conduct transactions, international money transfer hub partners and/or other service providers who play a part in customer registrations or monitoring customer activity).

Appropriate due diligence on such third parties must be conducted prior to business commencing. The due diligence requirements outlined above for non-personal customers should also be met for all third parties conducting regulated activities on behalf of Telecel Ghana Mobile Financial Services, subject to this policy. This includes, but is not limited to, verification of the nature and purpose of the business, risk-based identity checks and Watchlist screening of owners (including beneficial owners) and directors. Due diligence should be refreshed periodically using a risk-based approach, with higher risk third parties required to provide refreshed due diligence information more frequently.

Third Parties are also formally required to adhere to Telecel AML/CTF Policy standards, be monitored to ensure adherence, and face sanctions for breaches. Appropriate contractual obligations must be put in place to mandate these requirements. For clarity, the ultimate responsibility for the Telecel entity's compliance with the AML/CTF Policy and all AML/CTF laws and regulations remains with the Telecel regulated entity.

6.4 Systemic transaction, balance, and account limits

Telecel Ghana Mobile Financial Services shall have appropriate, system-enforced, transaction, account, and balance limits in place across wallets and customer types. This must be a documented risk-based approach, proportionate with the level of AML/CTF risk from the product and the level of customer due diligence information held on the customer.
There must be a maximum number of accounts per customer, which must be based on a clear business case designed for normal usage by the service's target customers. Where more than one account is permitted per customer, the combined transaction and balance limits for the maximum number of accounts permitted must be the aggregated balances and transactions across all the accounts and shall not exceed the limits stipulated for

the respective level of account as provided under the provisions of the Bank of Ghana Guidelines for E-Money Issuers in Ghana and its relevant amendments from time to time.

6.5 Record Retention

Telecel Ghana Mobile Financial Services is required to maintain, for a **minimum of five (5) years** (post the end of a customer relationship), all necessary records, to enable compliance with information requests from the competent authorities, and to conduct effective internal monitoring and investigations. Such records include but are not limited to staff and agent training, customer due diligence documents, all transactions, all watchlist screening or transaction monitoring alerts, details of all customer investigations and investigation decision rationales.

Records of Agent KYC information (ID records and transaction history) must be kept for a **minimum of 5 years** after the relationship with Telecel (or partner) has ended. This includes any copies taken of documentary evidence of identification.

Records of suspicious activity reports made internally to the MLRO and externally to the authorities must be kept for a **minimum of 5 years** after the report is made. This should include details of the investigation carried out and the logic behind the MLRO's decision.

All of the above-mentioned records must be stored securely and be easily accessible to the MLRO/AML/CTF Policy Champion.

At the end of the five (5) year period, the records shall be sent to the Public Records and Archives Administration Department in accordance with Act 1044 of Ghana.

6.6 Employee and Agent training

Telecel Ghana Mobile Financial Services must employ people with the skills, knowledge, and expertise necessary to perform the responsibilities allocated to them.

All employees involved with Telecel Cash must receive AML training as part of their induction training within 30 days of commencing employment. Auditable records of such training, and its content must be maintained.

Mobile money agents must receive AML training prior to commencing activity. These training requirements apply equally in the case of other Third Parties that AML regulated activity is outsourced to, where applicable.
All AML training must be provided by a competent trainer, and refresher training must take place at least every two years.

The business's approach to training should be built around ensuring that the content and frequency of training reflects the risks associated with the Services offered, the AML/CTF Policy requirements, legislation and regulation, and the specific role of the individual.

Training attendees are required to demonstrate awareness by passing a knowledge test in order to be considered to have completed training and be ready to begin work. Auditable records of such training, and its content must be maintained.

The MLRO is required to complete specialist AML training in the form of a recognized qualification. All other members of AML Teams, such as analysts, must also be provided proportionate and structured AML/CTF training, both at the start of their roles and on an ongoing basis.

On-going records of all AML training must be securely maintained and kept for 5 years after an individual has left employment.

6.7 Watchlist/Sanctions screening

Accounts must not be opened, and Services must not be provided to sanctioned individuals or entities, and any existing accounts or services identified in the name of sanctioned individuals or entities must be immediately

closed and the relevant authorities notified. This includes sanctioned individuals that are Ultimate Beneficial Owners (UBOs) of any entity provided a regulated service or any third party associated with providing Services (including mobile money agents).

If identifying a positive sanction hit, then the MLRO must immediately notify the Sanctions Policy Champion and the Sanctions escalation policy must be adhered to as mandated by the Sanctions Policy.

As part of onboarding processes all potential customers and third-party suppliers (individuals, entities and UBOs) must be screened against the sanction lists set out below:

- United Nations
- European Union
- Office of Foreign Asset Control (OFAC), US
- HM Treasury, UK
- US Sanctions List
- Any other list as required under the Anti-Money Laundering Act, 2020 of Ghana (Act 1044).

Ongoing screening must also take place to ensure that hits against any changes to either, customer or third-party details (including entity ownership) or changes on the lists screened against, are identified in a timely manner. Records of all screening must be maintained as per the record retention requirements set out above.

Customer and agent accounts applied for by individuals (including those who are an UBO of an entity which is a customer or third-party supplier) meeting the definition of a Politically Exposed Person (PEP) or Relative or Close Associate of such a person must be subject to approval from the MLRO and such customers shared with the Governance Committee. Approved accounts held by PEPs require enhanced KYC and due diligence checks and enhanced transaction monitoring which must be logged on a central database.

Screening must also take place against relevant crime lists, (which should be defined locally based on a proportionate risk-based approach). Any customer (including entities and UBO's of any business customer), agent or third party, identified on any crime list as a non-Sanctioned Special Interest Person (SIP) must be treated as high risk and subject to enhanced due diligence checks and where an existing customer, enhanced transaction analysis. To maintain a relationship with any Non-Sanctioned SIP customers identified, approval must be gained from the MLRO, who understands the AML/CTF Policy, the customer and product risk profile. Any Non-Sanctioned SIP customers accepted must be subject to ongoing enhanced transaction monitoring which must be logged on a central database.

The AML programme must contain methods to identify and block any customer or entity that has previously had their relationship with Telecel terminated due to factors relating to AML/CTF risk. Implementation of local screening lists should be maintained for this purpose.

An up-to-date record of all sanction and Watchlist screening alert parameters and list configurations must be maintained, and documented investigation procedures must be in place. A formal review of configurations must be conducted by the MLRO at least every 6 months, or sooner than this in response to material market changes.

6.8 Transaction monitoring

Telecel Ghana Mobile Financial Services is required to undertake systematic monitoring of transactions and behaviour to ensure that they are consistent with our knowledge of our customers, distribution channels, products, services, and risk profile. Monitoring and alerting must be in place to identify activity that could potentially be money laundering or linked to the financing of terrorism.

In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume, and size of transactions with customers, and the nature of those transactions, in the context of the assessed customer and product risk. The scope and complexity of the transaction monitoring processes will be influenced by the Service activities and size and also specific risks identified in our jurisdiction, for example corruption risks, prevalence of certain predicate offences, terrorism financing risks etc.

Typologies and parameters must be documented and maintained, taking account of risk assessment analysis for services, any behaviours/transactions which have resulted in SAR submissions previously and any emerging risks within the jurisdiction, including terrorism risks. This must be informed by a regular review of risk factors and threat profiles, including the AML/CTF Risk Assessment mandated by this Policy.

Telecel Ghana Mobile Financial Services must have documented investigation procedures followed by AML Analysts and the MLRO when investigating transaction monitoring alerts and other potentially suspicious activity.

A formal review of transaction monitoring typologies, parameters and effectiveness must be conducted by the MLRO at least every 6 months, or sooner than this in response to material market changes. All such reviews must be documented and must ensure that transaction monitoring is calibrated against contemporary standard customer behaviours and any emerging risk factors.

6.9 Reporting – Suspicious Activity Reports & Cash Threshold Reporting

All members of staff, contactors and those acting on behalf of Telecel's in relation to Telecel Cash, including mobile money agents, are required to report any suspicion of money laundering or terrorist financing to the Money Laundering Reporting Officer (MLRO).

Telecel Ghana Mobile Financial Services must maintain easily accessible channels for employees and relevant third parties to report suspicions of money laundering to the MLRO for further investigation. These channels must be communicated regularly.

Upon receiving a report, the MLRO must then conduct a full investigation into the suspect's activity including a review of any connected accounts, businesses, or agents. If the suspicion is validated, a report must be submitted to the Financial Intelligence Centre (FIC) as required under Act 1044 and any other relevant legislation of Ghana.

When a person makes a suspicious activity report internally to the MLRO, or the MLRO discloses externally to the authorities, the report or circumstances must not be disclosed to customers in any circumstances and must only be disclosed internally on a strict need to know basis. Sharing information risks "tipping off" customers engaged in illegal activity and doing is a breach of anti-money laundering laws.

When a customer/agent/Third Party has been subject to a suspicious activity report validated by the MLRO, a decision must be made as to whether the account(s) should be closed. Processes to enable these decisions must be documented and explain legal requirements. Such processes must follow the governance process set out in the document**: Telecel Ghana Mobile Financial Services – AML Procedure Manual.** Regard should also be had to any risk of tipping off the customer that a report has been made in the process of closing the account.

Cash Threshold Reports (CTR) are not mandated in legislation or regulation for Telecel Ghana Mobile Financial Services. The Bank of Ghana has set limits for the various tiers and these limits are automated on our platform in such a way that does not allow for limit breaches.

6.10 Compliance monitoring

The MLRO, under delegation from senior management, is required to regularly assess compliance with this AML/CTF Policy and the adequacy of AML systems and controls to ensure the management of risks effectively. The MLRO/AML/CTF Policy Champion must document an AML Compliance monitoring plan.

The findings and analysis of monitoring (including breaches and areas requiring improvement) will be reported to the local senior management. This must include documented reporting to the ExCo AML/CTF Policy Owner, Director of Telecel Cash, and the AML Governance Committee.

As part of Compliance monitoring the MLRO must annually compile an MLRO report and shared with the senior management of Telecel Cash and the Governance Committee.

The Policy Champion will conduct risk-based compliance monitoring to ensure standards are maintained.

In addition, independent assurance review of the AML/CTF programme will be undertaken by Internal and External Audit teams at proportionate intervals.

7. Off-Network Transaction

Off-network transactions are any which leave the internal financial ecosystem. This includes International Money Transfers and Interoperable Transfers. These types of transactions are higher risk than internal transfers as control and visibility moves to a Third Party. To ensure that these risks are effectively mitigated, robust and tailored controls must be implemented prior to the commencement of off-network transactions.

Eligibility to use these services must be restricted to customers who have been able to complete the Standard KYC process at a minimum.

Appropriate controls including targeted systematic transaction monitoring, partner due diligence and documentation of processes between internal and third-party AML teams are also required. System capabilities must also be in place to comply with FATF Recommendation 16 on wire transfers and provide information on the payer and payee accompanying the transfer of funds.

The MLRO must discuss AML requirements with the Policy Owner prior to any off-network service being offered, to ensure that all requirements are implemented.

8. Markets launching or considering New or Amended Services

It is imperative that when any product/service is launched, or where an additional service is offered the necessary controls are in place for it to be a long-term success and ensure that AML risks are effectively managed.

In order to ensure that this is the case the MLRO/AML/CTF Policy Champion must oversee and approve an AML Risk Assessment of all new products and services and/or assessments of existing products where material changes are being made to them.

As part of this risk assessment appropriate and proportionate AML controls must be mandated and product launches must not take place without implementation of said controls. Appropriate governance must be implemented in relation to new product and services launches,

All new products and services launches must be outlined in the annual MLRO Report.

9. Document history

Version	Date	Changes	Other standards affected	Approved by	Signed by
1.0	29 February 2024	Original document	TGMFS – AML Procedure Manual	AML Governance Committee on behalf of the Board of Directors	**Philip Amoateng** – Director, TGMFS/Policy Owner/Board Member/Committee Member..... **Samuel Owusu-Mensah** – CFO/Board Member/Committee Member..... **Judith Adumua-Bossman** – Committee Member..... **Vera Amaning-Kwarteng** – Committee Member..... **Anita Ayivi** – Policy Champion/MLRO .....