MultiChoice Group Limited (MCG)

Anti-Money Laundering (AML) Policy

TABLE OF CONTENTS

1. Purpose

MultiChoice Group ("MCG" or "Group") is committed to conducting its business in accordance with applicable laws, regulations and standards. MCG recognizes that inadvertent association with customers involved in the laundering of money derived from criminal activities can cause severe reputational and other damage.

The purpose of this Anti-Money Laundering (AML) Policy ("Policy") is to outline the overarching principles with regards to detecting and deterring any attempts made by customers to use MCG's products and services for any money laundering purposes.

2. Application

This Policy applies to all MCG Group employees (whether temporary or permanent) and directors (including non-executive directors). Third parties (including consultants, contractors, agents and suppliers) are also expected to be aware of and adhere to the policy.

3. Definitions, Acronyms and Abbreviations

Term	Definition
"Anti-Money Laundering" or "AML"	Refers to a set of policies and practices to ensure that financial institutions and other regulated entities prevent, detect, and report financial crime and especially money laundering activities.
"business unit" or "BU"	MultiChoice South Africa, DStv Media Sales, SuperSport, M-Net, Showmax, General Entertainment, MultiChoice Nigeria, Northern Region, Southern Region, MAH BV, Irdeto.
"employee"	All permanent employees, fixed term contractors and learners on a learnership programme.
"Initiator"	The initiator is the owner of the SOP. The initiator must be the head of the relevant function for which this SOP is being developed.
"MCG"	MultiChoice Group Limited.
"MCSA"	MultiChoice South Africa Holdings (Pty) Ltd and its subsidiaries.
"Money laundering"	The process of illegally concealing the origin of money, obtained from illicit activities such as drug trafficking, corruption, embezzlement or gambling, by converting it into a legitimate source. It is a crime in many jurisdictions worldwide and it is usually a key operation of organised crime.
"MultiChoice Group" or "the group"	MCG and its subsidiaries.
"PIP"	A prominent influential person is a person entrusted with public functions within a specific country, his or her close associates or immediate member of the family or an international organisation. Each business

	should keep or have access to detailed lists of relevant PIPs.
"Segments"	MCSA, RoA, Showmax and Technology (Irdeto), and "Segments" shall mean any one of them.
"SOP"	Standard operating procedure.

4. Policy details

4.1 Applicability of AML obligations

Each Group segment, business unit and/or function ("business" or "businesses") needs to assess at least annually, or earlier in the case of changes to AML laws, whether:

- Requirements exists to register with relevant AML regulator/s and
- If so, to comply with the relevant AML laws and its requirements.

There are businesses ("applicable business" or "applicable businesses") within the Group that are required to comply with specific AML obligations, mainly due to the nature of their activities and/or the relevant in-country AML laws where the businesses operate. These applicable businesses should ensure they comply with the high-level AML principles set out in this Policy, as well as following its specific AML policy and/or AML Standard Operating Procedures (SOPs).

4.2 Designated AML Compliance Officer

Only business units who are required to register with the relevant AML regulator/s and have to comply with relevant AML laws and it's requirements, must appoint a designated AML compliance officer. The designated AML compliance officer can be the person within the business unit that looks after risk and compliance and is responsible for ensuring that the business complies with the specific AML laws and its requirements, and to report specific transactions to the relevant Regulator, if required.

Key requirements for the designated AML compliance officers include:

- Having a good understanding of the requirements of the relevant AML laws and its requirements
- Being objective in carrying out his/her duties
- Receiving adequate training on AML laws and its requirements
- Reporting specific transactions to the Regulator promptly and efficiently once internal clearance has been given, where applicable
- Ensuring the business keeps accurate records of clients' identities, transactions and other relevant information
- Implementing an effective AML compliance programme that includes policies, procedures and controls

- Communicating effectively with senior management and staff about the business' AML compliance programme
- Staying up-to-date with any amendments to the relevant AML laws and its requirements.

4.3 Risk-based approach

Each applicable business must follow a risk-based approach with regards to complying with its specific AML requirements. Risk management starts with identifying the inherent risk, which is the money laundering risk that the applicable business is exposed to before applying any AML mitigating controls. It is important to note that the Group follows a pragmatic approach when it comes to the application of the risk-based approach. The risk of an individual customer laundering money on a normal basis ie. residence plus holiday home is very low, and hence very little further analysis should be considered going forward on these customers. Higher risk customers, such as customers with multiple accounts or business accounts, however, may create a higher risk, and further analysis should be considered for these customers. As part of its risk management approach, the business should consider the following characteristics which impact the money laundering risk, and how it increases and/or decreases such risk.

- **Customers** - Factors include whether the customers are natural persons, trusts, partnerships, legal entities, influential persons, have beneficial ownership, are locally or foreign based, citizens of the relevant country, etc.
- **Products and services –** Factors include the nature of the product or services rendered to customers, sanctions imposed, trade embargoes, payment terms, country of origin, etc.
- **Distribution channels –** Factors include the nature of the sales channel, use of third-party intermediaries, sales agreements, customers not providing their full details, application not in writing, telephonically or digitally, etc.
- **Geographic locations –** Factors include locally based customers, cross-border based customers, customers based in sanctioned countries, etc.

4.4 Customer identification

- **At onboarding** – Each applicable business should, in line with the pragmatic approach applied by the Group when it comes to the application of the risk-based approach, establish higher risk customer's identity before onboarding the customer. The business should not enter into a business relationship or execute transactions with such higher risk customers before establishing a customer identity. Based on the risk assessment conducted on the customer, the business should take appropriate measure to manage and mitigate the identified risks relating to higher risk customers, where applicable.
- **Customer information –** With respect to the specific customer information that needs to be obtained, each business should follow the processes set out in the applicable AML laws and/or the requirements included in the business' AML policy and/or AML SOPs.
- **Periodic reviews –** The business should undertake periodic reviews of existing customer information as soon as there is any doubt regarding the identity information held by the business, not later as stated in the business' AML policies and/or AML SOPs.

- **Prohibitions to deal with certain person/s -** It is prohibited to deal with persons / entering into transactions with persons who are included in the published United Nations Security Council (UNSC) list. Each business should check customers at onboarding against this sanctions list, which can be accessed at the below link: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

4.5 Verification of customer information

Each applicable business should verify the higher risk customer information obtained by comparing it with the applicable and corresponding independent and reliable supporting documentation, as stated in the relevant AML laws. Verification of the information shall be done prior to onboarding a customer and before any transaction is completed.

Verification of the customer identity after establishment of the business relationship, is only allowed subject to the business' AML policy and/or AML SOPs. In case the business enters into a business relationship with the customer and is unable to complete the verification procedures, it shall terminate this relationship and consider notifying the relevant Regulator, if required.

4.6 Enhanced due diligence.

Each applicable business should conduct enhanced due diligence on a customer at the onboarding stage if the customer is classified as follows:

- High risk and/or
- Prominent influential persons ("PIP").

Before establishing the relationship, the business should follow the requirements set out in its AML policy and/or AML SOPs and obtain the necessary approval from the designated AML Compliance Officer and segment CFO.

It is the responsibility of the Group's management and those charged with governance, to ensure that our business activities are conducted in accordance with laws and regulations and to identify any form of non-compliance by any of its stakeholders. Non-compliance may result in fines, litigation, or other consequences for the Group that may have a material effect on its financial statement and may also affect negatively investors, creditors, employees or general public.

The Group has a responsibility to respond appropriately when identifying possible instances of non-compliance with laws and regulations (NOCLAR). The NOCLAR review process is performed twice a year, at the interim phase and at year end. Responses to matters of NOCLAR may include obtaining a better understanding of the matter, addressing the matter with management and those charged with governance, inform next higher level of authority, determining whether further action is needed, determining whether to disclose the matter to an appropriate authority, etc.

4.7 Training

Each applicable business should conduct ongoing risk-based staff training and awareness activities relating to the specific AML laws and any other topics that may be relevant to its business. The designated AML compliance officer should ensure that staff complete and attend all scheduled training and awareness activities within the prescribed deadline.

The designated AML compliance officer should collate and report on progress with training and awareness activities at relevant management and/or board meetings. Each applicable business should implement escalation measures to ensure that any outstanding training and awareness are followed up timeously.

4.8 Reporting

Each applicable business should develop procedures for the reporting of 'suspicious transactions' and/or 'transactions above prescribed limits', and the details should be included in the applicable business' AML policy and/or AML SOPs.

- **Suspicious transactions –** The business should, within such a period as may be prescribed or as soon as possible after the suspicion arises, report a suspicious transaction to the relevant Regulator, if required. The suspicious transactions should be reported by the applicable business throughout the dealings with the customer.
- **Transactions above prescribed limits –** The applicable business should, within such a period as may be prescribed or as soon as possible after identifying the transaction, report the particulars concerning a transaction above the prescribed limited to the relevant Regulator, if required. The prescribed limits for reporting are contained in the relevant AML laws.

The applicable business' designated AML compliance officer should ensure that all reportable occasions are documented and are reported appropriately to the businesses' senior management and/or board of directors through the existing reporting processes.

The business' designated AML compliance officer should also quarterly report all significant AML related matters to the Group Legal Compliance and Ethics Officer, who should include the relevant information in his/her quarterly report to the Group Audit and Risk sub-committee of the MCG board.

4.9 Record keeping

Each applicable business should develop procedures for keeping the following:

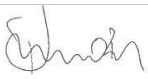
- Records related to customer due diligence
- Records related to transactions
- Records related to risk rating of clients, including the reason for the risk rating and any risk rating adjustments
- Records of reports filed with Regulators in terms of relevant laws
- Records that relate to training provided / conducted

- Records of decisions explaining why a transaction / activity was not reported to Regulators.

5. Non-compliance

Any group, organisation or business area, including individuals who are subject to this Policy found not to comply with the provisions as set out in this Policy or any amendment thereto, shall be subjected to appropriate disciplinary and legal action.

6. Document Properties

MultiChoice Group		Document Number	
		MCG-GRP-BOARD-011	
		1 April 2024	
Initiated By:		**Reviewed By:**	**Approved By:**
Johann Stander		Tim Jacobs	MCG
Group Legal Compliance and Ethics Officer		Group Chief Financial Officer (CFO)	Board of directors
			Minutes of meeting held on 28 March 2024
Re. No.	**Rev. Date**	**Section/s**	**Description of Change**
1	31 March 2024	All	New policy