Anti-Money Laundering, Combatting of Terrorist Financing and Countering of Proliferation Financing Policy Statement

Purpose

To formalise Capitec Bank's policy on the control of money laundering, financing of terrorist and related activities and proliferation financing to enable Capitec Bank and its employees to comply with the requirements of anti-money laundering, terrorist financing and proliferation financing laws and regulations. It includes supervisory requirements and measures to prevent that the bank is used for money laundering, terrorist financing and proliferation financing.

Read along with this content

Risk Management and Compliance Programme

Version	V01
Effective Date	31 July 2022
Content Owner	Monique Palmieri
Author	Janine Frittelli
Document Adherence	All employees
Committee to Approve	Financial Crime Risk Management Forum

Disclaimer

Table of Content

1. Introduction 1
2. Policy Statement 1
3. Key Principles 1
4. Risk based approach 1
5. Client Screening 1
6. Payment Screening 2
7. Restricted Relationships 2
8. Correspondent Banking 2
9. CDD, EDD and ODD 2
10. Regulatory Reporting and Transaction Monitoring 3
11. Training and on-going learning 4
12. New products and enhancements to products 4
13. Management information 4
14. Record-keeping 4
15. Resources 4
16. Escalating and reporting of risks 4
17. Glossary of Terms 5
18. Overview of the Risk Management Compliance Programme Documents 9

1. Introduction

As an Accountable Institution, Capitec has the responsibility to comply with the Financial Intelligence Centre Act, as amended, (FICA), and its Regulations, to combat money laundering (AML), terrorist financing (CTF), proliferation financing (CPF) and related activities.

2. Policy Statement

Capitec has a zero tolerance for any willful and intentional breach of any financial crime laws and regulations that apply to its business and transactions it undertakes.

3. Key Principles

3.1 Creation of policies, principles, methodologies, processes, and systems

3.1.1 Capitec have performed risk assessments to identify the financial crime it is exposed to, and subsequently introduced risk-based policies, principles, methodologies, processes, and systems to ensure compliance with the relevant Financial Crime legislations, regulations, and subordinate instruments such as guidance notes and directives.

4. Risk based approach

In compliance with FICA, Capitec applies a risk-based approach to ensure that there are adequate controls in place to combat and mitigate money laundering (ML), terrorist financing (TF) and proliferation financing (PF) activities.

4.1 Financial Crime Risk Assessment

4.1.1 Capitec assesses its financial crime risk across the business by conducting annual Financial Crime Risk Assessments. The outcomes of these Assessments are used to drive the improvements of ML/TF/PF compliance by identifying risks, ensuring control measures are put in place to mitigate these risks and determining any residual risks that remain.

4.2 Client Risk Assessment

4.2.1 Capitec uses the application of a Client Risk Assessment as a key preventative and detective control measure during the complete client life cycle. The identification of high-risk prospective clients allows Capitec to introduce appropriate control measures and apply the appropriate level of client due diligence.

5. Client Screening

In line with regulatory requirements, Capitec has a client screening system in place to screen all prospective and existing clients against approved sanction lists, to determine

whether prospective and existing clients, including their known associates, are Politically Exposes Persons**.**

6. Payment Screening

Screening of transactions conducted by clients under an application to transfer or to receive funds cross border are performed to determine whether current clients, and their counterparties, are subjects of sanctions and/or economic embargoes.

7. Restricted Relationships

Capitec may not establish a business relationship or conclude a single transaction with an anonymous client or a client with an apparent false or fictitious name or any party, Capitec deems restricted as per our Risk Appetite Statement.

8. Correspondent Banking

Correspondent banking is the provision of banking services by one bank to another bank. This may include cash management, international electronic payments, cheque clearing, and foreign exchange services. As correspondent accounts are specifically vulnerable to ML/TF/PF risks, Capitec will ensure that the necessary due diligence is performed.

9. CDD, EDD and ODD

9.1 Client Due Diligence (CDD)

9.1.1 CDD refers to measures, including policies and procedures, which are put in place within Capitec to have knowledge of who our clients are and how they transact, for the bank to detect any suspicious activity.

9.1.2 Before entering a single transaction or establishing a business relationship, Capitec must, while concluding that single transaction or establishing that business relationship, establish and verify the identity of the client based on reliable, independent source documents, and those acting on their behalf in accordance with Capitec's Risk Management and Compliance Programme.

9.1.3 In line with Capitec's approach to develop a client profile linked to a client behaviour risk model the on-boarding requirements for the Remote On-boarding channel differ marginally to that of the business's other on-boarding channels. To mitigate the risk associated with a non-face-to-face channel, the usage of this channel must be limited to South African citizens only. Clients must be 18 years and older with a valid South African Identification document. Client identities are verified using the Department of Home Affairs by providing a valid identification number.

9.1.4 Business Units must have client on-boarding procedures with the requisite level of CDD for face-to-fact and non-face-to-face clients. The relative Business teams may determine

the method of verification for its clients, provided those methods comply with local law and meet the requirements set out in the CDD Standards.

9.1.5 The application of CDD procedures is a key component to combat ML/TF/PF effectively. Capitec clients are risk categorised as low, medium, or high-risk at on-boarding depending on their risk profile.

Risk Category	Impact	Client Due Diligence
Low	Client is a low risk from a financial crime perspective. There is chance that the client may expose the bank to potential financial crime risk, but it is unlikely that this will occur	STDD
Standard	Client is a standard risk from a financial crime perspective There is chance that the client may expose the bank to potential financial crime risk, but it is unlikely that this will occur	STDD
High	It is likely that the client may introduce, risk specifically from a financial crime perspective and more stringent controls must be implemented to mitigate the risk. Client is a high risk from a financial crime perspective and enhanced due diligence is required to mitigate the risk	EDD

9.2 Enhanced Due Diligence (EDD)

9.2.1 Enhanced due diligence measures (including policies and procedures) are taken in addition to the standard client due diligence measures and are conducted on all high-risk clients, including clients identified as Politically Exposed Persons (PEPs) includes Prominent Influential Persons (PIPs) and Foreign Public Influential Persons (FPPO's).

9.2.2 These enhanced due diligence measures include obtaining and verifying additional information as well as periodical review and monitoring of high-risk clients.

9.2.3 Senior Management approval are required for the onboarding of all high-risk clients, including PEPs.

9.3 Ongoing Due Diligence (ODD)

9.3.1 Capitec undertakes to conduct on-going monitoring of client relationships and activity, including the monitoring of accounts to detect potentially unusual or suspicious transactions while using adequate systems and procedures.

10. Regulatory Reporting and Transaction Monitoring

FICA places an obligation on Capitec to report on several types of transactions and activities including Section 28, Section 28A, Section 29 and Section 31. Capitec adheres

to these regulatory and reporting obligations as set out in its Regulatory Reporting and Transaction Monitoring Standard.

11. Training and on-going learning

General awareness employee training and on-going learning is facilitated by the Learning and Development Department, in relation to AML/CFT/CPF. There are also specific training programmes which are rolled out to certain employees who are required to perform certain activities in relation to the prevention of ML/TF/PF.

12. New products and enhancements to products

New and amended products and services are assessed to determine the ML/TF/PF risk posed by the product, and the necessary mitigating controls implemented to help manage the identified risks.

13. Management information

Appropriate management information and reports, which are relevant, reliable, and timely, are provided to senior management regarding Capitec's compliance with Capitec's RMCP to put the Board and senior management in a position to understands the financial crime risk Capitec is facing and how effective Capitec's financial crime risk mitigating controls are.

14. Record-keeping

14.1 Capitec ensures that appropriate customer records and all customer transaction records are retained in accordance with the requirements set out in section 22 of FICA. The minimum record retention period is 5 years after termination of a relationship or after the conclusion of a single transaction.

14.2 Should a transaction or activity have given rise to a report contemplated in section 29, the said records must be retained for at least five years from the date on which the report was submitted to the Financial Intelligence Centre.

15. Resources

Appropriate and adequate resources and systems are maintained to enable Capitec to comply with its AML/CTF/CPF obligations.

16. Escalating and reporting of risks

Capitec does not accept wilful non-compliance with legislation. Employees are therefore encouraged to report any form of non-compliance to the Compliance department, who will assist with the identification and remediation of the compliance risk.

17. Glossary of Terms

Term	Description
AML	Anti-Money Laundering
BU	Business Unit
Business relationship	• A business relationship means an arrangement between Capitec and a client for the purpose of concluding transactions on a regular basis or which entails an on-going relationship in line with the nature of a product or service offering. A business relationship therefore entails an element of duration to the engagement with the client • A business relationship is created at the point at which the client is enabled by Capitec to transact, deposit, receive funds or accept products or services offered
Capitec	"Capitec " means Capitec Bank Limited (incorporated with limited liability in South Africa under registration number 1980/003695/06) which includes: • Capitec retail banking • Capitec shared services • Capitec business banking
CFT	Combating the Financing of Terrorism / Terrorist Financing Control
Client	A client is a person or entity with whom Capitec has established a business relationship to provide products and services, or for whom an occasional transaction is carried out. In this document “client” and “customer” are used interchangeably, and for the purposes of this document, have the same meaning. A relationship will only be established if all Capitec’s client due diligence measures have been met both in respect of the client and the related persons, i.e., persons acting on behalf of the client or exercising control over the client or owing the client as set out in Capitec’s *Client Due Diligence (CDD) Standards*. The related person/s do not become a client and an entity do not become a client unless all related persons are included in the process to establish a business relationship or concluding an occasional transaction
Client Due Diligence (CDD)	Client Due Diligence (CDD) information comprises the facts about a client that should enable an organisation to assess the extent to which the client exposes it to a range of risks. These risks include money laundering (ML)/terrorist financing (TF). CDD consists of the following 4 main obligations: • To identify and verify the client’s identity using reliable, independent source documents, data or information • Identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner • Understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship • Conduct on-going due diligence on the business relationship and scrutinise transactions undertaken throughout the course of that relationship to ensure that the transactions being

Term	Description
	conducted are consistent with the institution's knowledge of the client, their business and risk profile, and where necessary, the client's source of funds. (FATF Recommendation 12)
Client Type	Client type refers to the legal form of the client, this may be natural or juristic persons
Client Risk	Client risk refers to the inherent financial crime risk of Capitec associated with its client base and in line with its risk-based approach
Enhanced Due Diligence (EDD)	The level of due diligence applied to high-risk clients, which is more than standard CDD
Existing client	An existing client is a natural person or entity with whom Capitec has already established a business relationship
FIC Act or FICA	Financial Intelligence Centre Act 38 of 2001, including all amendments
Financial Crime	Any kind of criminal conduct relating to money or to financial services or markets, including but not limited to any offence involving: • Fraud or dishonesty • Misconduct in, or misuse of information relating to, a financial market (market abuse and insider trading) • Money laundering • Bribery and corruption • Financing of terrorism • Electronic crime • Information security For the purposes of this policy, collectively used specifically for money laundering and terrorist financing (sanctions)
Inherent Risk (IR)	IR represents the exposure to ML/TF risk in the absence of any control environment being applied. After the design and implementation of AML/CFT controls, in combination with other business controls, inherent risk is reduced to residual risk
Lines of defence	In the 3 lines of defence risk management model, management control is the first line of defence (1LOD), the various risk control and compliance oversight functions established by management are the second line of defence (2LOD), and independent internal assurance is the third line of defence (3LOD)
Money Laundering (ML) or Money Laundering Activity	Means an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition, or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of the FIC Act or section 4, 5 or 6 of the Prevention of Organised Crime Act
On-going Due Diligence	Means to conduct on-going due diligence on a business relationship

Term	Description
(ODD)	and scrutinise transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the client, their business and risk profile, and where necessary, the client's source of funds. (FATF Recommendation 12)
Payable Through Account	A "payable through account" (PTA) (also known as Pass-Through or Pass-by) occurs when a financial institution funnels the deposits and cheques of its clients (usually individuals or businesses located outside the country) into a single account that the financial institution holds at the other bank and provides its clients (sometimes referred to as sub-account holders) with direct access to the other bank, by virtue of the client's independent ability to conduct transactions with the another bank through the PTA. PTAs therefore pose a challenge to "know your client" policies and requirements, and suspicious activity reporting
POCDATARA	Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004
Politically Exposed Person (PEP)	Refers collectively to all Politically Exposed Persons, including PIPs and FPPOs
Prominent Influential Persons (PIPs)	Refers only to those PEPs that hold a prominent public position within South Africa
Foreign Prominent Public Official (FPPO)	Refers only to those PEPs that hold a position outside of South Africa
Proliferation financing	The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations
Prospective client	A prospective client refers to a client who has indicated an intention to take up products/services with Capitec, and has embarked on establishing a relationship, but has not yet formally taken on any product or service. A prospective client will have provided Capitec with certain minimum information to allow the client acceptance to occur, after which the successful conclusion thereof will allow product/s or services to be taken up
Residual Risk	Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management controls. The residual risk rating is used to assess whether the ML/TF risks within Capitec are being adequately managed
Risk-Based Approach	Taking a risk-based approach towards client due diligence entails the application of due diligence measures commensurate with the

Term	Description
	ML/TF risk posed to Capitec. For instance: • Where Capitec identifies instances of higher ML/TF risk (clients, products etc.), Capitec should ensure that its AML/CFT regime adequately addresses such risk • Where Capitec identifies instances of lower ML/TF risk, Capitec can consider the application of simplified due diligence under certain conditions
Sanctioned persons	Natural persons and entities listed on the consolidated United Nations Security Council Sanctions List (UNSCS), Her Majesty's Treasury (HMT) consolidated list of targets, Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons List and Targeted Financial Sanctions list (TFS)
Single Transaction	A transaction other than a transaction concluded during a business relationship and where the value of the transaction is not less than R5 000.00 (the amount is determined by the Minister of Finance in the Regulations). This can be described as occasional or once-off business where there is no expectation on the part of Capitec or the client that the engagements would recur over a period
Terrorist Financing (TF)	Terrorist financing or the financing of terrorism involves the solicitation, collection and the providing of funds and other assets with the intention that it may be used to support terrorist acts, terrorist organisations or individual terrorists
RMCP	Refers to the Risk Management and Compliance Programme which describes how Capitec identify, assess, monitor, mitigate and manage its Financial Crime risk
STDD	Refers to Standard Due Diligence
EDD	Refers to Enhanced Due Diligence

18. Overview of the Risk Management Compliance Programme Documents