



# FICA UPDATE

22 MAY 2025

**Presenter:**

Ferdi Coetzee

Regional Manager

Masthead Eastern Cape



[www.masthead.co.za](http://www.masthead.co.za)

Compliance • Practice Management • Research • Online Learning • Seminars



## AGENDA

1. Welcome
2. FICA updates
3. Inspection findings



[www.masthead.co.za](http://www.masthead.co.za)

Compliance • Practice Management • Research • Online Learning • Seminars



# FICA UPDATES

# FICA UPDATES



- 1) FIC GN 7A
- 2) Directive 3A
- 3) PCC 50A
- 4) Greylisting update
- 5) TF Court order
- 6) CASP SRA
- 7) RCR update
- 8) RMCP submissions
- 9) Travel Rule (CASPs)
- 10) Draft PCC 118A (MVTs)
- 11) IFTR (Banks)
- 12) Draft PCC 23A (CPs)
- 13) Inspections / Sanctions



# GUIDANCE NOTE 7A



## GN 7A

### *Adequacy of Risk Management & Compliance Programme (RMCP)*

- Accountable institutions must **develop, document, maintain, and implement** a **RMCP** addressing money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks.
- The RMCP documentation must adequately address the **full scope of section 42 of the FIC Act**.
- The RMCP must be **adequate, suitable, and effective** for the accountable institution.
- The implementation of the RMCP must be **monitored consistently** and audited periodically to increase the effectiveness of its implementation.



## GN 7A

### *Board and Senior Management*

- The **board of directors or senior management must approve the RMCP** and ensure compliance. The obligation to approve the RMCP **cannot be delegated**.
- The RMCP must be **comprehensive** and include **substantial information** to enable the board to understand and manage ML, TF, and PF risks.
- The board or senior management must ensure a **culture of compliance** within the institution.
- The **board or senior management are responsible** for the adequacy of the RMCP and will be **held accountable if it is found inadequate**.



## GN 7A

### *Compliance function*

- The compliance function must be assigned to a **competent person** with sufficient seniority.
- The RMCP should include a **description of the compliance function's seniority and experience.**



## GN 7A

### *Elements of an effective RMCP*

#### **Risk Identification**

- Conduct an **entity-wide (business) risk assessment** to identify ML, TF, and PF risks.
- It should be **comprehensive** enough to enable an accountable institution to **clearly identify, assess and appreciate** the **inherent and residual** ML, TF and PF risks and threats it faces.
- Consider the **nature, size, products, service offerings, industry, client base, geographic location(s), complexity of business, delivery mechanisms, third party service** providers and any other relevant factors of the accountable institution.
- Before the board approves the RMCP, the **board must consider whether the RMCP adequately mitigates the ML, TF and PF risk**, therefore the board must be satisfied, that an entity wide AML/CFT/CFP risk assessment has been conducted, and all the relevant risk factors have been taken into account.
- Risk assessments should also take into account relevant **published national and sector-specific risk assessments**, and these must be appropriately reflected in the RMCP, as applicable to the operations of the accountable institution."



## GN 7A

### *Elements of an effective RMCP*

#### **Risk Mitigation and Management**

- Implement **appropriate controls** to manage identified risks, including customer due diligence (CDD), reporting and record keeping etc.

#### **Monitoring**

- Continuously monitor the effectiveness of controls.



## GN 7A

### ***Documentation Considerations***

- The RMCP documentation must be **readily accessible** and include references to related documents.
- **RMCP documentation must reference related documentation** that constitutes and enables the full implementation of the RMCP. Documentation that is not referenced in the RMCP is not considered to be part of the RMCP.
- The RMCP should include appropriate documentation of the **institution's risk management policies, risk assessment methodologies and risk profile** in relation to ML, TF and PF, including documentation of the institution's application of those policies.
- It should also cover:
  - **appropriate training** on ML, TF and PF to ensure that **employees are aware** of and understand their legal and regulatory responsibilities and their role in handling possible criminal information or property and ML, TF and/or PF risk management.
  - appropriate descriptions of **decision-making processes** regarding different categories of customer due diligence and other risk management measures, **including escalation of decision-making to higher levels** of seniority in the accountable institution where necessary.
  - **appropriate measures** to ensure that ML, TF and PF risks are escalated and considered in the **day-to-day** operation of the institution.
- The RMCP must be commensurate with the **size, complexity, and the nature** of the institution's business.



## GN 7A

### *Group-wide RMCPs*

- Institutions **operating in groups** may **implement group-wide RMCPs**, tailored to specific entities within the group.
- **Separate entity (business) risk assessments** should be conducted by each accountable institution, which should feed into the group's entity wide AML/CFT/CFP risk assessment.
- Indicate in the RMCP, whether all accountable institutions that form part of a group structure have been covered when conducting the group entity wide risk assessment.
- Group entities can **opt to conduct entity risk assessments** on entities within the group, that are **not accountable institutions**.
- The entity wide risk assessment must **adequately cover all of the accountable institution's businesses, products, service offerings, technologies, delivery mechanisms, enablement processes, business processes and client base etc.**
- The group wide RMCP should indicate **what elements are applicable** to different entities and **what is not applicable** to different entities within the group and the reason for same.



## GN 7A

### *Compliance with Local and International Obligations*

- Institutions must comply with AML, CTF, and CPF obligations in **all jurisdictions** where they operate.
- **If foreign requirements are lower than South African standards, the institution must meet South African requirements** - unless there is a reason that prevents the accountable institution from doing so, then the accountable institution must inform the supervisory bodies, and take into consideration the level of risk in the foreign jurisdiction and apply appropriate additional measures to manage the risk.

### *Review and Updates*

- The RMCP must **be reviewed regularly** to ensure it remains relevant.
- Any **amendments** must be documented and approved.

### *Supervisory Approach*

- The **supervisory body will inspect whether the RMCP has been approved** and whether it adequately addresses ML, TF, and PF risks.
- The **supervisory body will analyse and apply its mind** to determine whether the accountable institution's board of directors, senior management or person(s) with the highest authority, **understand the risks, which is translated into appropriate and adequate controls**, including monitoring and oversight measures as part of the RMCP.



# **DIRECTIVE 3A & PCC50A**



## Directive 3A & PCC 50A

Directive 3A and PCC 50A sets out processes to **mitigate loss of intelligence data** due to a **reporting failure or defective report**. The Directive and PCC applies to all accountable institutions who have an obligation to file reports with the FIC.

### These reports are:

- Section 28 – Cash threshold reporting
- Section 28A – Terrorist property reporting
- Section 29 – Suspicious and unusual transaction **(or activities)** reporting
- Section 31 – International funds transfer reporting

A '**Reporting failure**' refers to where a report ought to be filed with the FIC and the reporter either **failed to submit the report or filed a defective report**.

A '**Defective report**' refers to a report that has been filed with the FIC with the **incorrect or incomplete prescribed information**.



# **GREY LISTING UPDATE**



## Grey listing Updates

The most recent greylisting review for South Africa by the Financial Action Task Force (FATF) occurred during the FATF Plenary on **21 February 2025**.

In this session, the FATF acknowledged South Africa's **significant progress in addressing deficiencies** in its anti-money laundering and counter-terrorist financing (AML/CFT) framework.

Specifically, the FATF noted that South Africa had **successfully addressed 20 out of the 22 action items** outlined in its action plan.

The remaining **two items** pertain to **enhancing the investigation and prosecution of complex money laundering cases and strengthening enforcement against terrorist financing activities**



## Grey listing Updates

“Overall, Designated Non-Financial Businesses and Professions (**DNFBP’s**) **understanding** of ML risks and AML/CFT obligations is **underdeveloped**, and mitigating measures are **not risk-based**, with casinos as a positive outlier. The high-risk **estate agents and attorneys** have a **poor understanding** of risks and obligations.

It is of **concern** that estate agents and attorneys have an underdeveloped understanding of risks and obligations given ML typologies in South Africa.

Where casinos are the best DNFBP reporters, **estate agents, attorneys, and Trust Service Providers’s file a very low number of reports**. The larger banks file the best quality reports and the **worst are filed by attorneys and estate agents.**”



# **TERRORIST FINANCING COURT ORDER**



## TF Court Order

**13 February 2025:** South Africa has issued its first court order in terms of section 23 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) (POCDATARA Act), on Tuesday, 11 February 2025.

The South Gauteng **High Court** issued the prohibition upon **two individuals** and **two entities** (the designated persons). In the order, the High Court said, there were **reasonable grounds “to believe** that they have committed, participated in or facilitated the commission of the offence of **terrorism”** which is a specified offence as defined in the POCDATARA Act.



# **CRYPTO ASSETS SERVICE PROVIDER SECTOR RISK ASSESSMENT REPORT (CASP SRA)**



### CASP SRA

**1 April 2025:** The Financial Intelligence Centre (FIC) released a report on the **inherent** and **residual risks** of money laundering and terrorist financing (ML and TF) facing crypto asset service providers (CASPs).

The sector risk assessment report addresses the inherent and residual ML and TF risk factors for CASPs pertaining to their **products, services, clients, transactions, delivery channels and geographical areas**.

Also included in the report are **possible mitigation measures** that can be considered through compliance with the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) (FIC Act).



# **RMCP SUBMISSIONS**



## RMCP Submissions

In terms of section 42(4)(a) of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001) all **non-financial accountable (as found in amended FIC Schedule 1)** institutions listed in the Financial Intelligence Centre Act (FIC Act) were requested to submit a copy of the documentation describing their Risk Management and Compliance Programme (RMCP) to the Financial Intelligence Centre (FIC) on or before close of business on Wednesday, **12 March 2025**.

**The Portal is still open, and submissions must still be done if not done yet.**



# **TRAVEL RULE (DIRECTIVE 9) CRYPTO ASSETS SERVICE PROVIDERS**



## Travel Rule (Casps) Directive 9

### Directive 9 Overview

The purpose of **Directive 9** is to **enhance transparency in crypto asset transactions** to mitigate risks such as money laundering, terrorist financing, and proliferation financing.

The travel rule applies FATF's Recommendation of **16 requirements** to crypto asset transfers, ensuring that information about the **sender and receiver accompanies the transaction**.

CASPs must provide and maintain transaction information and make it available to authorities upon request.

Directive 9 took effect on **30 April 2025**



# **INTERNATION FUND TRANSFER REPORT (BANKS)**



## IFTR (Bank)

### What is an IFTR?

- An IFTR is a **report that must be submitted** to the FIC regarding any **electronic financial transaction or transfer moved** on behalf of, or at the instruction of, another person **across South African borders**.
- These transfers must exceed **R19,999.99**.
- The FIC uses IFTRs to **monitor cross-border** financial activity and identify potential suspicious transactions.

### Why are IFTRs required?

- IFTRs are a **crucial tool** for the FIC in its efforts to **detect money laundering**, terrorism financing, and other financial crimes.
- By requiring financial institutions to report these transfers, the FIC can gain a **better understanding of the flow of funds across borders** and identify any suspicious patterns.



**PCC23A**

## UPDATES



### PCC 23A-Draft

PCC 23A for Credit Providers has been issued for another round of consultation. The issue of incidental credit that was decided on after the 1st round of consultation has been put forward for public comment



# INSPECTIONS



### Trends of non-compliance

1. Business Risk Assessment not conducted / inadequate
2. RMCPs not customized / reviewed
3. RMCPs not implemented
4. RCR non-submission
5. TFS screening and freezing of assets
6. Registration / dual registration (40% of All Sanctions)
7. Customer Due Diligence / Beneficial Ownership identification
8. Remediated non-compliance

#### **FIC Act Appeal Board - Capital Point Properties (Pty) Ltd**

*“The fact that a transgression has been rectified does not mean that it was not a transgression and cannot or should still be the subject of a sanction.”*



**THANK YOU**

**Contact details:**

Ferdi Coetzee

fcoetzee@masthead.co.za

082 940 3759

**[www.masthead.co.za](http://www.masthead.co.za)**

Compliance • Practice Management • Research • Online Learning • Seminars

