Financial
Intelligence Centre

THE ROLE OF THE FIC (RSA) MIDDLE EAST NORTH AFRICA (MENA)

Ahzur Mohamed CA(SA)
Mohammed Jahed

3 October 2022

The role of the FIC

Financial Intelligence Centre

Assist in identifying proceeds of unlawful activities

Assist in combating money laundering

Assist in combating terrorist financing

SHARE INFORMATION WITH
- NPA
- LEAs
- Supervisory bodies
- Intelligence services
- SARS and
- Other international agencies

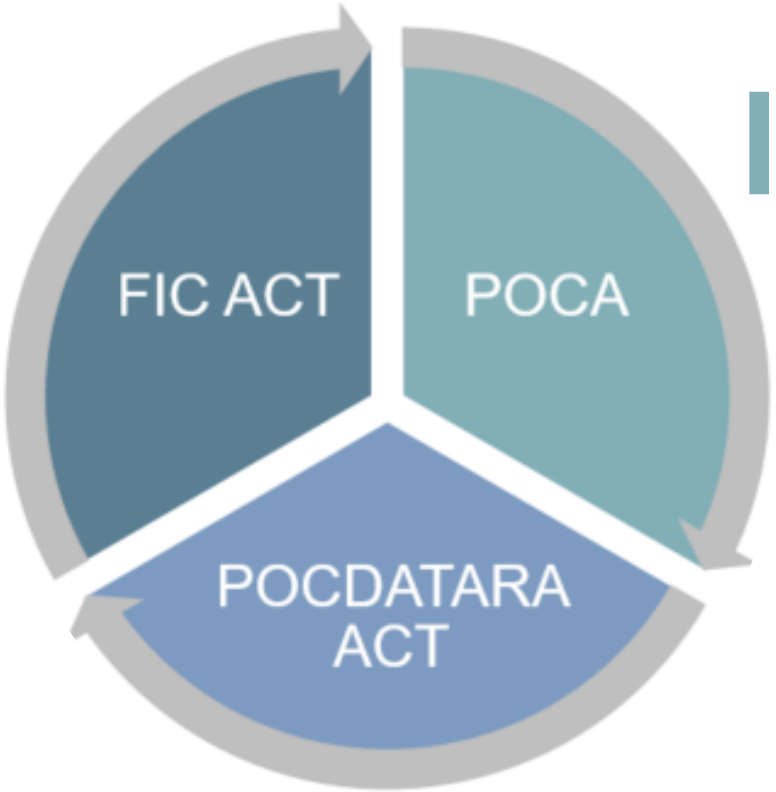
SUPERVISE AND ENFORCE **compliance** with the FIC Act

FIC has **no investigative powers**

FIC Act and South Africa's AML/CFT framework

FIC ACT

- Created FIC as South Africa's national centre for gathering and analysis of financial transaction and related data
- Places reporting and other obligations on accountable institutions and all business
- Able to 'follow the money', aimed at removing the business from the business of crime.



POCA

- Criminalises money laundering
- Sets the penalties associated with a conviction

POCDATARA Act

- Addresses terrorist activities and offence of terrorism
- Introduced measures to address the financing of acts of terrorism

Regime for Anti-Money Laundering and Combating the Financing of Terrorism

Anti-Money Laundering (AML)

Combating Financing of Terrorism (CFT)

GLOBAL

Financial Action Task Force (FATF) inter-governmental body focusing on combating ML and TF policy making and standards setting
(IMF and World Bank)

FATF

EGMONT GROUP of Financial Intelligence Units

esaamlg Eastern and Southern Africa Anti-Money Laundering Group

DOMESTIC

Financial Intelligence Centre Act, 2001 (Act 38 of 2001) [FIC Act] established the FIC and placed obligations on financial institutions and other businesses deemed vulnerable to money laundering.

The Prevention of Organised Crime Act (Act 121 of 1998) [POCA] introduced the crime of ML and set the penalties associated with a conviction.

The Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 2004 (Act 33 of 2004) [POCDATARA Act] introduced measures to address the financing of acts of terrorism.

7 key aspects to compliance

Stages of money laundering

1 PLACEMENT

MOVE DIRTY MONEY INTO THE FINANCIAL SYSTEM

CHARACTERISTICS
Intention is to use legal and illegal activities to convert proceeds into usable products

HOW | E.g. move via financial instruments such as bank accounts or insurance products

2 LAYERING

CREATE DISTANCE BETWEEN SELF AND ILLICIT PROCEEDS

CHARACTERISTICS
Create anonymity – the source (criminal activity) of illicit proceeds cannot be linked to self

HOW | Criminals create complex layers of transactions making it difficult to trace or to link money back to the original criminal activity

3 INTEGRATION

LEGITIMISE THE ILLICIT PROCEEDS

CHARACTERISTICS
The illicit proceeds are indistinguishable from legitimate funds in the financial system

HOW | Criminals are now free to spend their illicit monies. They claim the money comes from legitimate business dealings.

…and the cycle continues

Regulated sectors and the seven key aspects of compliance

FIC Act identifies financial and non-financial sectors vulnerable to money laundering including:


Estate agents


Banks


Attorneys


Gambling sector


Motor vehicle dealers


Forex dealers

Minimum requirements from these sectors are:

Identify and verify client identities (ID, KYC) (S21)	Develop risk management and compliance programme (S42)	Keep records of transactions (5 years) (S22)	Provide ongoing training on FIC Act requirements to staff (S43)	Submit reports to the FIC (STRs, CTRs and IFTRs) (S27, S28A, S29, S31)	Register with the FIC (S43B)	Comply with the FIC Act - Compliance Officer (S42A)

Risk based approach applied

Crypto currency service providers (CASPs) will be added soon

Risk-based approach

- Accountable institutions must follow a risk-based approach (RBA) when managing risks related to ML and TF
- Applying a RBA ensures that accountable institutions are able to implement measures that are in proportion to the ML and/or TF risks identified
- Accountable institutions must identify, assess, monitor, mitigate and manage their ML and/or TF risks
- Must manage the risk that the provision of goods and services by the accountable institution may involve or facilitate ML and/or TF.
- Accountable institutions must evaluate the following as part of their risk assessment to identify possible ML and/or TF risks:

Products and services	Delivery channels	Location	Client type	Other factors
• Third party payments • Cash / EFT • Cross-border flow of money • Duration of relationship or transaction	• Direct relationship • Working through intermediary • Face-to-face or non-face-to-face	• SA / foreign jurisdiction • High risk countries • Client confidentiality in foreign jurisdiction • Weak regulatory oversight	• Natural / Legal person • Complex structures • Politically exposed? • Prominence • Adverse information • Negative media • ML findings • Transactional patterns	• ML approach • Sanctions • Strategy of entity • Regulatory fines in similar industries • Learnings / typologies

Reporting: Cash threshold reports (CTRs)
FIC Act section 28

- Section 28 of the FIC Act – CTR (not about suspicion – **mere factual report** / does not address element of guilt)
- Cash threshold amount exceeding **R24 999.99** cash received or paid (what is cash: coin and paper money and traveller's cheques)
- Aggregation over a 24-hour period – regulation 22B and 24 (period of reporting)
- Report within two business days after becoming aware
- Failure to report – section 51 offence; Penalty section 68(1) (criminal or administrative penalty – payable by means of the imposition of a fine)

Reporting: Suspicious and unusual transaction reports (STRs) FIC Act Section 29

Defining a suspicion

- Who must report STRs? This obligation applies to:
  - A person who carries on a business
  - A person who is in charge of a business
  - A person who manages a business or
  - A person who is employed by a business
- Section 29 - STRs have **no cash threshold** (cash received by an institution is not always of a suspicious nature)
- Time period for reporting – ASAP (not later than 15 working days – Regulation 24)
- Continue transaction (section 33) and protection of person making report (section 38)
- Section 29 (3) – Non-disclosure to any person including the subject of the report of the STR filed with the FIC
- FIC's Guidance note 4

FIC's power to disclose information

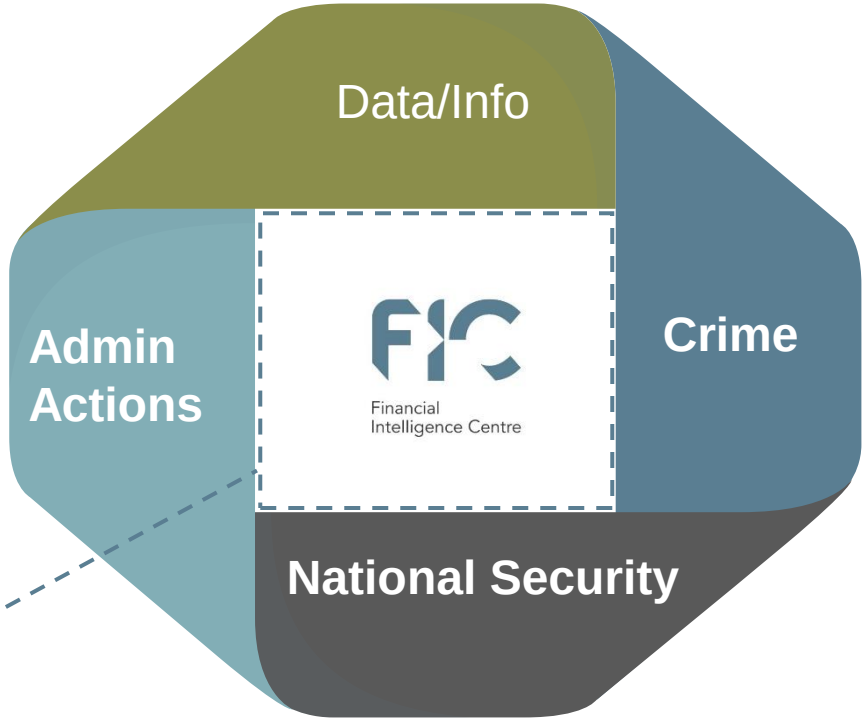
Financial Intelligence Centre

Section 41 of the FIC Act provides that, in general, the FIC **may not disclose** its confidential information.

However, section 40 creates a number of **exceptions** to the general rule. It provides that the FIC must make information reported to, or obtained or generated by it, available to Law Enforcement Agencies and Supervisory Bodies for follow-up investigations or administrative action.

Stakeholders

- Accountable Institutions
- Reporting Institutions
- Government departments (CIPC, DHA, NT, SARB)
- Data Providers



- South African Revenue Services
- Special Investigating Unit
- Public Protector
- Supervisory bodies (e.g. SARB, FSCA)
- National Treasury
- Commissions of inquiry

Provide intelligence upon REQUEST or at the INITIATIVE of the FIC

- National Intelligence Co-ordinating Committee (NICOC)
- State Security Agency
- Defence intelligence
- Foreign FIUs (Egmont Group)
- DIRCO

- Justice Crime Prevention and Security Cluster
- SA Police Service
  - General Detectives
  - Directorate for Priority Crime Investigation
  - Crime Intelligence
- National Prosecuting Authority
  - National Prosecuting Services
  - Asset Forfeiture Unit
  - Investigative Directorate
- Independent Police Investigative Directorate
- An investigative division in an organ of state
- An investigating authority
  - Department of Environmental Affairs
  - Department of Correctional Services

Section 40: FIC makes information reported to it, and information obtained in terms of its mandate, available to specified stakeholders

Information sharing/handling conditions

The FIC want the users to regularly consult about the SCOPE of their investigations and USAGE of the FIC info.

The information is **sensitive** and **classified**

No person is entitled to be in **possession** of financial intelligence information unless the person's possession is justified by the FIC Act

The information may not be compromised in any way through any **disclosure to any person** who is not required to use the information.

The information may not be disclosed, in particular, directly or indirectly to individuals or entities that form the **subject matter of the report**

Status of information shared by FIC

Procedural arrangements and safeguards (handling conditions): Section 40(3)

Information (domestic and international) in financial intelligence report is not evidence **(including supporting bank statements)**, is to be used for **intelligence purposes** only; may only be used to investigate suspected unlawful activity or when relevant, to the extent of the recipient's statutory function.

The recipient of FIC information must immediately notify and forewarn the FIC of any demand or any **legal proceedings** (including any notice of intended legal proceedings) to seek access to, or the disclosure of, the information received from the FIC.

Misuse of information – **offence** in terms of section 60 (section 68 penalty). Applicable to any person who discloses information held by or obtained from the FIC – shared otherwise than in accordance with section 40 or 41 and as per section 60(2).

Information that the FIC can provide

There are six areas the FIC will look at when deciding on what information is to be provided

FINANCIAL INFORMATION (SEC 27)

- Tracing of bank accounts (51 banks)
- Long-term Insurance portfolios (89 entities)
- Gambling Information (3130 entities)
- Foreign exchange dealers (362 entities)
- Money remitters (265 entities)

REPORTS RECEIVED

- Suspicious and unusual transaction reports (Sec 29)
- Cash threshold reports (Sec 28) >R25k
- Terrorist property reports (Sec 28A)
- Reports from supervisory bodies (Sec 36)
- Additional information on regulatory reports received (Sec 32)

POWERS TO SUPPORT INVESTIGATIONS

- Freezing of bank accounts – 10 days (section 34)
- Monitoring of bank accounts (section 35)
- Certificate confirming regulatory reports received (section 39)
- Access to records by warrant (section 27A) (evidence)

INTERNATIONAL INFORMATION

- Requests – Egmont for financial info with other FIUs globally (Sec 40)
- Cross-border monetary flows – Reserve Bank
- Cross-border Movement Control System (MCS) – Home Affairs

ASSETS

- Deeds info– Property
- Vehicle registrations - NaTIS

OTHER RELEVANT INFORMATION

- Legal persons CIPC, NPOs and Trusts
- Government Data: Population, Movement, BAS, Persal
- Paid subscription services
- Open source and/or desktop analysis
- Analysis of bank statements / big data
- Link analysis

BREAKOUT SESSION – 15 MINUTES

1. How is financial intelligence shared with your respective agency? i.e., what processes do you have to go through to obtain intelligence / assistance from your FIU?
2. Have any of the group members ever logged a request with the FIU?; If yes, was the intelligence useful? Was it responded to timeously?
3. Have you ever received proactive financial intelligence from your country's FIU? If so, did the intelligence result in tangible results (i.e., further investigation, prosecution, etc.)?
4. In your view, does your country's law enforcement agencies make adequate use of the FIU? (Please elaborate).

CRYPTO ASSETS

Financial Intelligence Centre

WHY do we use crypto currency?

FAST

Digital generation – fast

FLEXIBLE

Global market, cross-border trade, travel and movement of people – 12 000 different cryptos

INSTANT

Transactions are instant, non-face-to-face, cross jurisdictional and largely anonymous

FREEDOM

Financial freedom – outside of formally regulated economy. No need for middleman

GROWTH

Remarkable growth potential – investments

ANONYMITY

Designed with privacy in mind – anonymity.
My name is *Mr/Ms…*
a548f3637357c3f74871b3d8c3451653f46702d96ac7bfcc3ee5f17e74fa6460

Even though most exchanges perform KYC/CDD

"What the internet did for communications, blockchain will do for trusted transactions" (IBM CEO: Ginny Rometty)

FIAT CURRENCY VS CRYPTO CURRENCIES

FIAT CURRENCY

- Minted and regulated by the **central bank**.
- **Centralised** and backed by the South African government.
- **No cap** – the amount of fiat currency in circulation is determined by the central bank.
- Cash transactions that occur are **not published publicly** and cannot be seen since the first minted FIAT currency.

CRYPTO CURRENCIES

- Created by computers within the network.
- **Decentralised** and not backed by anyone.
- Bitcoin has a **cap** of 21 million coins.

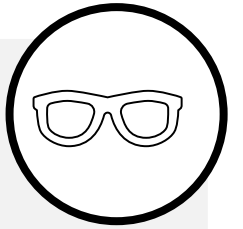
$$\sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21000000$$

- Created through the blockchain protocol code, based on **mathematical** equations.
- The **blockchain has published** all transactions since 2009.

Financial Intelligence Centre

Case Study: Allegations of fraudulent government contracts

SAMLIT MEMBERS' FLAGS

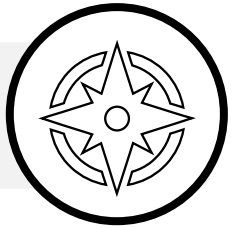


At the outset, media reports about a **PEP benefiting** from government tenders related to CV-19 relieve efforts. Based on **regulatory reports and comprehensive analytical products** received from **SAMLIT members,** the FIC assisted the Special Investigation Unit (SIU) (as part of its operational work in the **Fusion Centre**) in an alleged irregular **communication contract** which was exposed in the media. The total **payments over a 9-month period** from the government department to the service provider, linked to a PIP, amounted to **R150m**.

FINANCIAL FLOWS

With the assistance of SAMLIT members the FIC conducted a financial flow analysis which **identified 163 beneficiary bank accounts** and payments towards 3 credit cards from the service provider.

SECURING THE MONEY

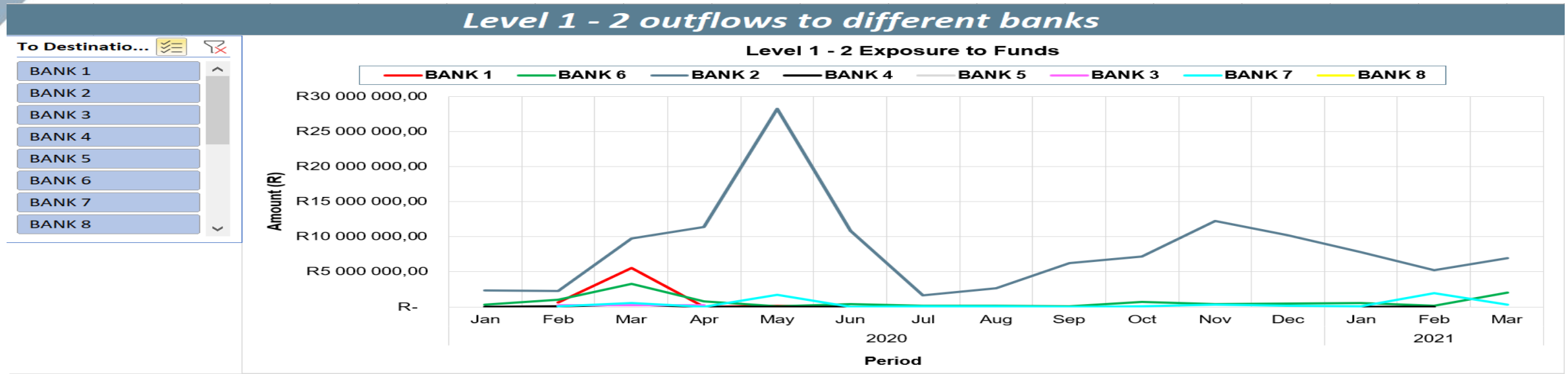


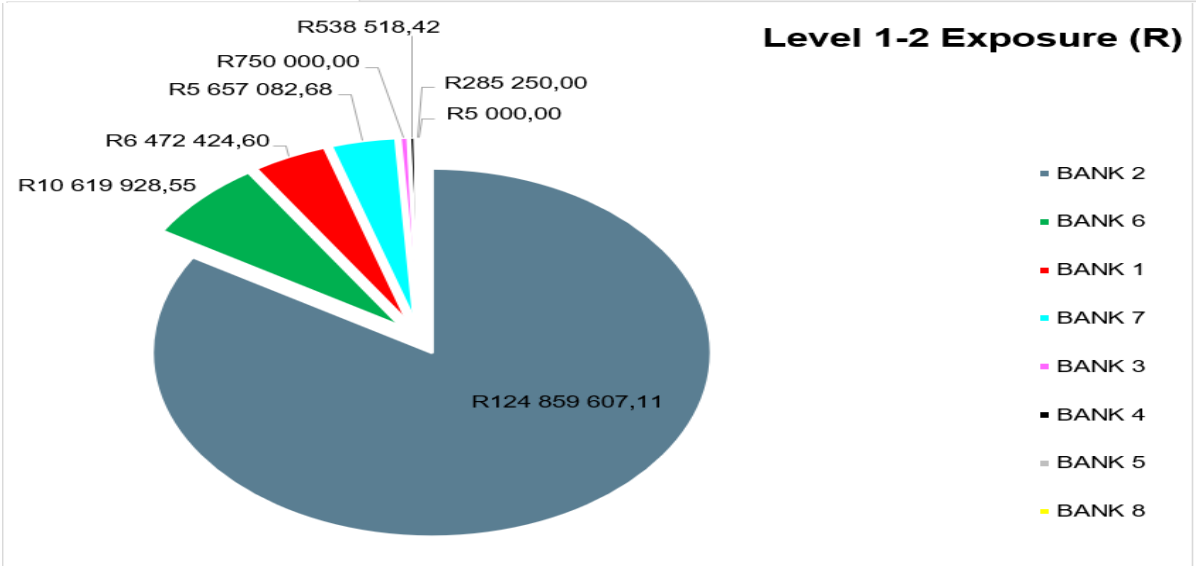
Through this **complex analysis process** the FIC issued section 34 directives to financial institutions securing R22m.

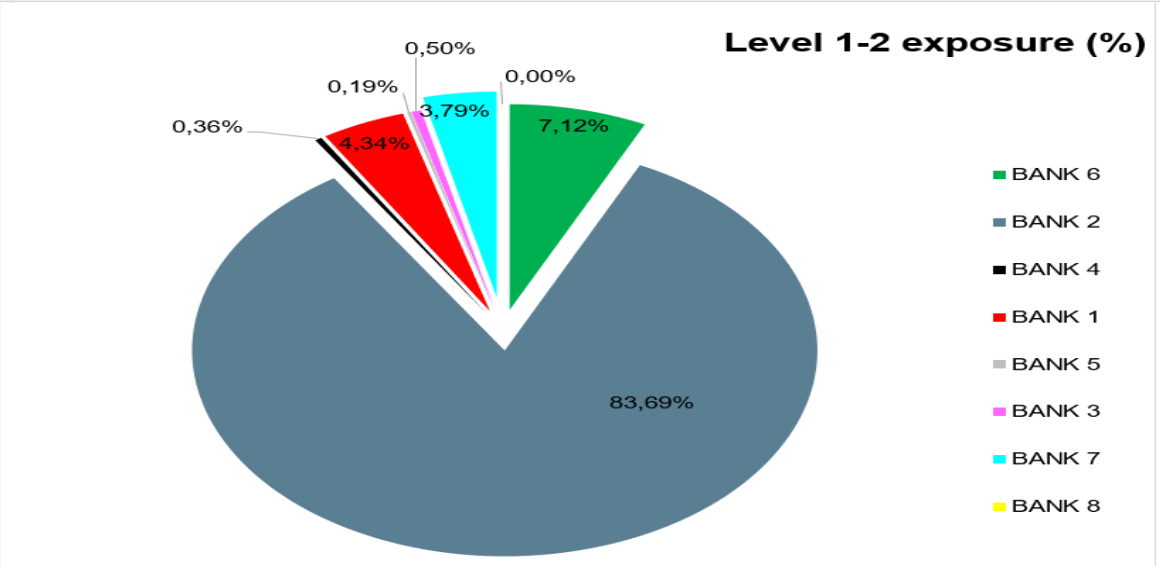
EVIDENCE PRODUCED

Using some of the financial flow analyses completed the FIC deposed an affidavit in support of a SIU Special Tribunal order which identified twelve (12) respondents and **preserved R22 million**. The SIU instituted **review proceedings** with the aim of recovering the full R150 million.

Level 1 – 2 outflows to different banks







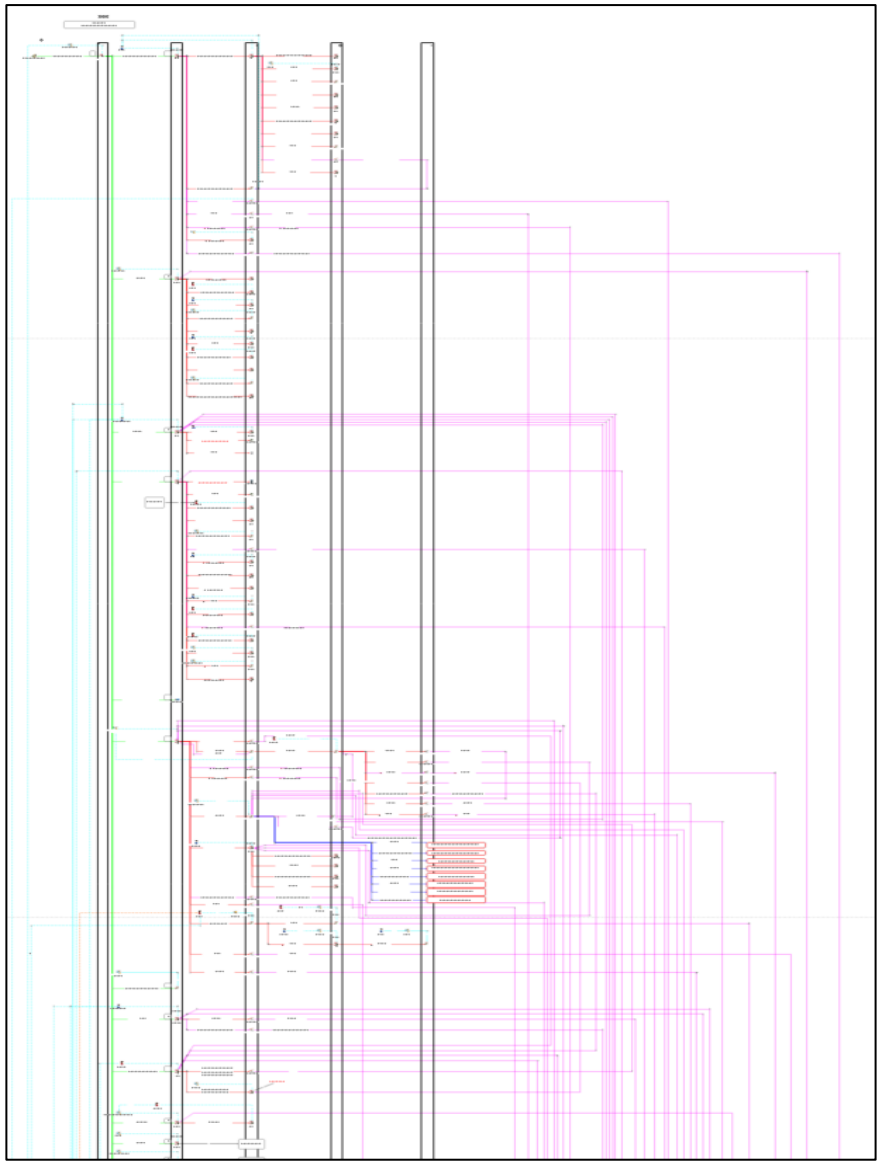
Complexity of the matter

MULTIPLE BANK ACCOUNTS

FIC traced the funds from the Department to supplier through **one hundred sixty-three (163) second level** beneficiary accounts and three (3) credit cards.

ADDITIONAL BANK ACCOUNTS

Forty-four accounts were further analysed to **level three** identifying a further **two hundred third level** beneficiary accounts through **1422 transactions**.



ASSETS FROM THE PROCEEDS

Assisting the Asset Forfeiture Unit (AFU) the FIC identified **additional assets that were purchased to the value of approximately R6m** through multiple layers of transactions.

CRIMINAL CASE

The matters is being dealt with in the **Fusion Centre** and the **criminal investigation is ongoing** and the FIC assists with **financial intelligence guiding** the investigation,

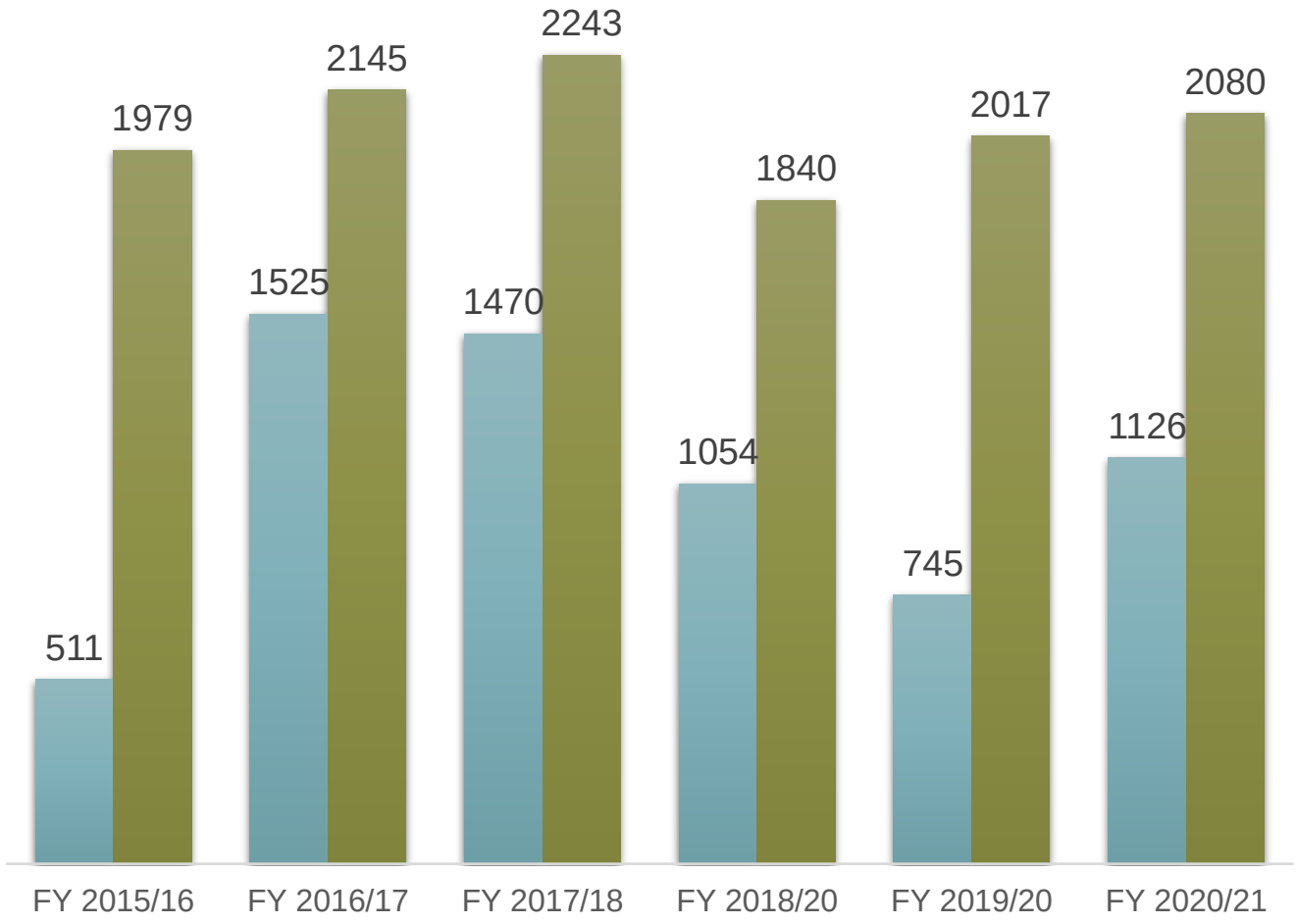
Statistical view of disseminated proactive and reactive financial intelligence

01

1126 proactively disseminated financial intelligence reports to FIC Act section 40 stakeholders

02

2 080 produced upon request for information from all FIC Act section 40 stakeholders



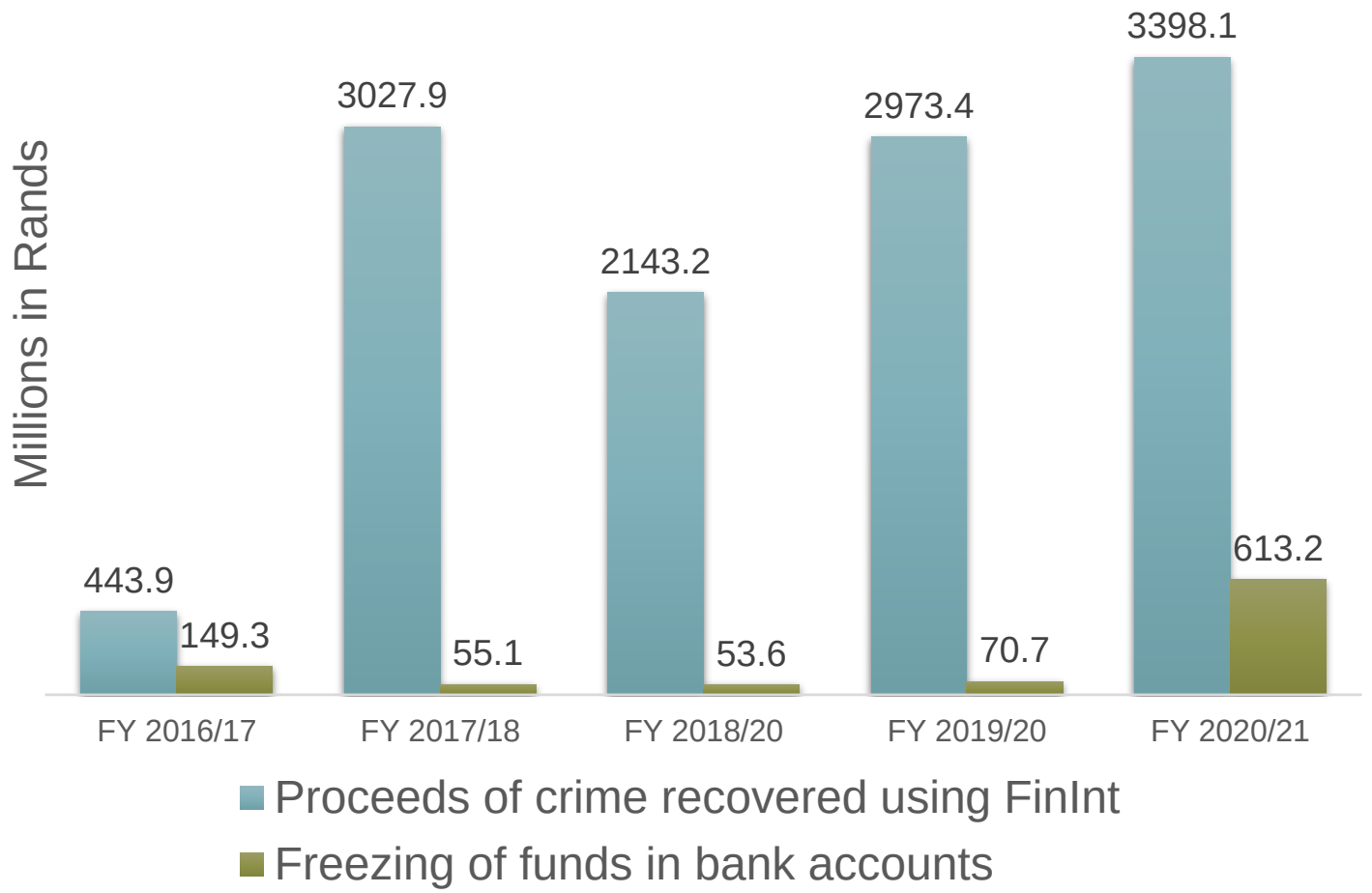
Suspected proceeds of crime recovered 2015 to 2021

01

Proceeds recovered by stakeholders using financial intelligence produced by the FIC [FY 2020/21 R3,3 b]

02

Freezing proceeds in bank accounts using section 34 of the FIC Act [FY2020/21 – R613,2m]



Case study:
Fraud and money laundering through crypto currencies

- The FIC received an alert from a **neighbouring jurisdiction** that a person was defrauded of a large amount of money that was transferred to a South Africa financial institution. Some funds were transferred to a cryptocurrency exchange and converted into a **basket of cryptocurrencies**, including Bitcoin. Some funds were irrecoverable because they were transferred to other cryptocurrency exchanges in foreign jurisdictions.
- The FIC froze some of the **virtual currency (Bitcoin, Bitcoin Cash and Ripple)** held with the cryptocurrency exchange using a section 34 directive. It also provided an affidavit that led to the Asset Forfeiture Unit obtaining a preservation order from the High Court in Johannesburg.
- **To note:**
  - Both addresses traced to BITTREX – exchange based in Las Vegas, USA
  - In 24 hours – R500,000.00 moved through 3 countries!

Financial Intelligence Centre

THANK YOU

Monitoring and Analysis | MAA.requests@fic.gov.za | 012 – 641 6000 | www.fic.gov.za