AGENDA

8:00 – 9:00 Registration
9:15 – 9:45 Regulatory update
9:45 – 10:00 Targeted Financial Sanctions
10:00 – 10:45 FIC Act awareness
10:45 – 11:15 Tea Break
11:15 – 11:45 Financial intelligence reports and services
11:45 – 12:15 Reporting, goAML and updates
12:15 – 12:45 Supervision and Enforcement
12:45 – 13:25 Q&A
13:25 – 13:30 Closure
Regulatory update

12 July 2019
Changes to the anti-money laundering and combating of terror financing regulatory framework

- Commencement of section 31
- Amendments to regulations
- Amendments to Schedules 1, 2 and 3
Commencement of section 31 of the FIC Act

- Section 31 report - reported to the FIC as an International Funds Transfer Report (IFTR)
- IFTR refers to:
  - Cross-border flow of funds – includes Common Monetary Area (CMA) transactions (inbound and outbound)
  - On behalf or on the instruction of another person
- Applicable to accountable institutions that deal with the business of cross-border money transfers
- The prescribed threshold: Amounts of R5 000 and above must be reported to the FIC. No aggregation requirements for reporting international funds transfer IFTR transactions
- IFTRs must be filed as soon as possible, or at the latest within 72 hours of the accountable institution becoming aware of the transaction
- All other reporting information will be set out in the regulations
Amendments to draft regulations for cash threshold and cash threshold aggregate reporting

Draft regulations for:

• Proposed prescribed threshold amount for reporting of cash transactions to be increased from R24 999,99, to R49 999,99

• Proposed that aggregation reporting on cash thresholds to be withdrawn

• The draft regulations contain a proposal for the reporting obligations relating to aggregation to be withdrawn
Amendments to draft regulations – CTR / IFTR

• The draft amendments to regulations were approved by the Minister in February 2019 to be published for comment

• Notice was published in the Government Gazette on 28 February

• The FIC also published two guidance notes for comment
  o Guidance Note 104 – IFTR (new)
  o Guidance Note 5C – CTR

• The FIC and the National Treasury in continued discussion with the banking industry to resolve issues raised in their comments on the draft regulations to support the implementation of section 31

• Once all issues are resolved the amended regulations will come into force after tabling in Parliament and once the President proclaims section 31 to come into operation
Amendments to Schedules

- The consultation process commenced in March 2017 and consultations with relevant industries continued in 2018 and 2019
- Proposals will be made to the Minister to include new business sectors in Schedule 1 to the FIC Act
- A proposal will also be made for the FIC to oversee and enforce compliance with the FIC Act of the Designated Non Financial Businesses and Professionals (DNFBPs)
- Additional categories of institutions as accountable institutions will improve the FIC’s ability to obtain information concerning the identities and financial activities of clients of a wider range of sectors
- Improves FIC’s ability to provide high quality information to law enforcement and other government agencies
- Increase in transparency of the financial system – institutions gather information regarding client identity and transactions that can be recorded and accessed over time
- Will also bring South Africa’s legal framework against ML/TF in line with the international standards set by the FATF e.g. in respect of crypto assets service providers
Amendments to Schedule 1

Who is proposed to be included?

• Professionals providing services relating to the formation and administration of trusts and companies
• A co-operative bank as defined in the Co-operative Banks Act
• Persons who carry on the business of a credit provider
• Dealers in high value goods (include motor vehicle dealers, numismatic dealers, those that deal in precious metals and stones, yachts, etc.)
• A person who carries on the business of:
  o Exchanging a crypto asset for a fiat currency or other virtual assets
  o Conducting transactions that move a crypto asset from one crypto asset address to another
  o Safekeeping or administration of a crypto asset enabling control over a crypto asset
  o Provision of financial services related to an issuer’s offer or sale of a crypto asset
Amendments to Schedules 2 and 3

• In 2017 the Minister of Finance approved FIC’s recommendation to start a process to exit the Estate Agency Affairs Board, Independent Regulatory Board for Auditors, provincial Gambling Boards and Law Societies as supervisory bodies

• The FIC will have the responsibility to oversee and enforce compliance with the FIC Act in respect of those accountable institutions that are currently supervised by these supervisory bodies

• Schedule 3 to the FIC Act lists reporting institutions, namely, motor vehicle dealers and Kruger rand dealers

• Proposal is to delete the references to these items in Schedule 3 as these two categories of reporting institutions will be included in the new category of high value goods dealers in Schedule 1.
Amendments to Schedules

Way forward

• The consultation paper with the proposed amendments to be submitted to the Minister of Finance.

• If the Minister approves, the consultation paper together with the proposed amendments, will be published for comment for a period of about 60 days.

• Following the period of consultations, the amendments to the Schedules will be finalised and the Minister will submit the amendments to Parliament for approval.

• The final amendments to the Schedules will then be published in the Government Gazette and amendments will come into effect.
SOUTH AFRICA TO UNDERGO MUTUAL EVALUATION
South Africa to undergo mutual evaluation

- South Africa’s mutual evaluation will be undertaken by two of the organisations of which the country is a member, namely the Financial Action Task Force (FATF) and the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

- Members of the two organisations each undertake peer reviews of their members and South Africa’s evaluation is part of this process. The third member of the evaluation team is the International Monetary Fund

- FATF is an inter-governmental body that sets international standards for measures to combat money laundering, terror financing and the financing of the proliferation of weapons of mass destruction which threaten the international financial system
South Africa to undergo mutual evaluation (cont.)

• A mutual evaluation is an important opportunity for a country to have their AML/CFT framework reviewed by its peers

• In preparation for the mutual evaluation, the FIC has been working with its partners in government, supervisory bodies, representatives in the financial and non-financial sectors, and other role players to gather large volumes of information that will be considered during the evaluation process

• The evaluation team will meet with representatives from government and industry to understand how they carry out their respective functions in implementing South Africa’s measures against money laundering and terrorist financing
South Africa to undergo mutual evaluation (cont.)

• The assessment team’s conclusions will be a reflection of how well South Africa is doing in maintaining the integrity of its financial system

• Following the completion of the on-site visit, the assessment team prepares a country report

• The final adopted report will be available on the FATF and ESAAMLG public websites

• Following the adoption of the report, both the FATF and the ESAAMLG will hold South Africa accountable for the follow-up actions that the country will have to undertake to improve its system against money laundering and terrorist financing in areas identified in the report
Developing a national risk assessment

- During 2018/19, Cabinet approved the FIC’s proposal to conduct a national risk assessment and to form a committee to lead the process
- The aim of the national risk assessment is to identify the AML/CFT risks the country faces so that South African can develop a risk-based approach and appropriate responses to these threats
- While the risk assessment does feed into the FATF’s mutual evaluation, it will function independently and continue beyond 2019, informing future legislative amendments and resource allocation
- It will become a decision-making tool for government and other role players to guide the development of policies, institutional frameworks and processes
- As risks evolve over time, the assessment will be updated regularly
TARGETED FINANCIAL SANCTIONS
Administration of targeted financial sanctions by the FIC

• The sections in the FIC Act relating to targeted financial sanctions (TFS) came into operation on 1 April 2019

• Recommendation 7 of the FATF Recommendations requires member countries to implement TFS to combat the financing of the proliferation of weapons of mass destruction

• As a member of the United Nations, South Africa is required to implement Resolutions adopted by the United Nations Security Council (UNSC)

• TFS measures restrict sanctioned persons and entities from having to funds and property, and from receiving financial services in relation to these funds and property

• Accountable institutions are required to freeze property and transactions according to the financial sanctions imposed in the UNSC Resolutions
Implementation of UNSC resolutions

Mechanism for implementation – Notice by Minister of Finance

- Publication in Government Gazette
- By Minister of Finance
- Notice of adoption of the UNSC Resolution

Mechanism for implementation – Notice by Director of FIC

- Publication of persons and entities who are subject to the sanction measures by FIC’s Director
- Director will publish any additions and deletions as and when information is received from the UNSC
- Both are public statements meant to advise sanctioned individuals and/or entities and accountable institutions, and other interested parties
Implementation of UNSC resolutions

Role of the accountable institution

- May not acquire, collect or use property of such persons/entity
- May not transact or process transactions for sanctioned persons/entity
- Scrutinising of existing clients and prospective clients against sanctions list
- Accountable institution must report to FIC the property in its possession and/or under control which is owned or controlled by or on behalf of a person or an entity identified on the sanctions list (section 28A)
- A person who suspects a contravention of a targeted financial sanction obligation, must submit a suspicious activity report or a suspicious and unusual transaction report to the FIC (section 29)
- The indicator to be used – suspicious transaction report (STR) in terms of section 29(1)(b)(vi) as relates to the contravention of a prohibition under section 26B of the FIC Act
- Suspicious activity report (SAR) in terms of Section 29(1)(b)(vi) as relates to the contravention of a prohibition under section 26B of the FIC Act
Implementation of UNSC Resolutions

Role of the FIC

• Maintains updated TFS list on FIC website - list will reflect available information on persons and entities contained in the notices published by the Director of the FIC

• The Minister of Finance or a delegated authority may permit a sanctioned person or entity to conduct financial services or deal with property affected by a sanction

• This permission may extend to allowing financial services or the dealing in affected property which is necessary in the normal course of business.

• The permission is granted by means of written communication with the sanctioned person or entity

• The Director of the FIC must give notice of the permission to accountable institutions and others who may have an interest in the property
UNSC Updates/Changes to UNSCRs TFS Consolidated List (Chapter VII Article 41)

FIC Alert Subscription Mailing List

Application for permitted financial services (e.g. basic living expenses; avoiding prejudice to third parties)

Accountable/Reporting Institutions submit TPR/STR/SAR

Enquiries: Resolution Process

Screening & Search Capability: Maintain updated UNSCR List & reflect available identity particulars of persons and entities as contained in Notices (FIC website: Screen & Search Tool (Software) & E-mail Template)

Prepare Notification for MoF in Government Gazette or Director Notice and publish on FIC website

Sanctions Monitoring Process: Analysis Capacity

Notification Process

FIC Q&A
THANK YOU
FIC Act awareness
Agenda

- Background to the FIC
- Risk-based approach
- Risk management and compliance programme (RMCP)
Financial Action Task Force (FATF)

- Inter-governmental International standard setting body
- FATF 40 recommendations
- Standards on anti-money laundering and combating the financing of terrorism (AML/CFT)
- 2009 mutual evaluation, gaps identified, addressed in FIC Amendment Act 2017
- 2019 mutual evaluation
FIC - Global and national footprint

- FATF 40 Recommendations
- FATF 8 Regional Bodies (ESAAMLG)
  - Supervisory Bodies
    - THE FINANCIAL SERVICES CONDUCT AUTHORITY (FSCA)
    - SOUTH AFRICAN RESERVE BANK (SARB)
    - ESTATE AGENCY AFFAIRS BOARD (EAAB)
    - THE INDEPENDENT REGULATORY BOARD FOR AUDITORS
    - LEGAL PRACTICE COUNCILE
    - THE NATIONAL GAMBLING BOARD
      - MOTOR VEHICLE DEALERS
      - KRUGER RAND DEALERS
FIC Act – Background

• 2003 – commencement of Financial Intelligence Centre Act, 2001 (Act 38 of 2001)

• 2010 – amendments to the FIC and the commencement of cash threshold reporting obligations

• 2017 – amended by the Financial Intelligence Centre Amendment Act 2017
  o As a result of the 2009 Mutual Evaluation and to align to FATF requirements and United Nations obligations
  o Rules based changed to risk-based approach Risk management and compliance programme (RMCP)
  o Enhancements to customer due diligence (CDD) requirements
  o Targeted financial sanctions
  o Exemptions withdrawn
FIC Act – Background

• Supplemented by regulations related to money laundering and terrorist financing controls
  Directives 1, 2, 3, 4 and 5

• Guidance Notes
  o GN 4B STR
  o GN 5B CTR
  o GN 6A TPR &
  o GN 7 CDD and RMCP

• Public compliance communications (PCC’s)
FIC Act – Background

Applies in conjunction with two other laws:

- Financial Intelligence Centre Act (FICA)
- Prevention of Organised Crime Act of 1998 (POCA)
- Protection of Constitutional Democracy against Terrorist and Related Activities Act of 2004 (POCDATARA)
MONEY LAUNDERING

- Illegal sources - proceeds of crime
- 3 stages - placement, layering, integration
- Process where the origin, nature and source of illegally obtained funds are concealed through the disposing or movement of funds
- Goal is to conceal the illegal nature of the source of funds

TERRORIST FINANCING

- Illegal and legal sources
- 3 stages – attracting funds, moving funds and using funds
- Intention is to use funds to support terrorist acts, terrorist organisations and individual terrorists
- Goal – to conceal financing and nature of activity being financed
FIC functions

- Process, analyse and interpret information reports
- Monitor and give guidance to accountable institutions
- Supervise and enforce compliance with the FIC Act

S45 supervisory bodies functions

- Supervise and enforce compliance with the FIC Act
- Supervisory bodies listed in scheduled 2 of the FIC Act
FIC Act – regulatory framework

Accountable institutions compliance obligations

- Customer Due Diligence
- Record Keeping
- Compliance Officer
- Risk management and compliance programme
- Reporting
- Training of employees
- Registration with the FIC
Risk-Based Approach

- Accountable institutions must follow a risk-based approach (RBA) when managing risks related to money laundering (ML) and terrorist financing (TF)
- Risk that clients might **misuse products and services** offered by accountable institutions for ML and/or TF purposes
- **Threats and vulnerabilities** of accountable institution’s being **abused** by clients in order to facilitate ML and TF
- Applying a RBA ensures that accountable institutions are able to implement **measures** that are **proportionate** with the ML/TF **risks** identified
Risk-Based Approach

Accountable institutions must:

- Identify
- Assess
- Monitor
- Mitigate
- Manage

The risk that the provision of goods and services by the accountable institution may involve or facilitate ML and/or TF.
### Risk-Based Approach

#### Risk identification - Evaluate the following:

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

In order to Identify the possible ML/TF risk each poses
Risk-Based Approach

Risk Assessment – Risk Rating

- Assign different ratings (categories) to different levels of risk
- i.e. High, Medium or Low risk from a ML / TF risk perspective
- No “one size fits all” approach
- Consequence and impact of the ML / TF risk occurring? Huge negative impact?
- Likelihood of ML/TF occurring? Highly likely to occur?
- Risk scale tailored to size of an accountable institution and range of products offered
- Risk rating may change, re-evaluation of risk rating is critical
- Risk rating methodology must be documented in RMCP
## Risk-Based Approach

### Risk matrix

i.e.: Higher risk (21-30), Medium risk (11-20), Low risk (1-10)

<table>
<thead>
<tr>
<th>Client type</th>
<th>Product type</th>
<th>Jurisdiction</th>
<th>Delivery channel</th>
<th>Occupation</th>
<th>Overall rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Person</td>
<td>Property purchase</td>
<td>6, Iran</td>
<td>6, Non face to face</td>
<td>6, Unemployed</td>
<td>25 – High risk</td>
</tr>
<tr>
<td></td>
<td>cash</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complex Legal</td>
<td>Rental fixed</td>
<td>1, South Africa</td>
<td>3, Face to face</td>
<td>1, Technology company</td>
<td>10 – Low Risk</td>
</tr>
<tr>
<td>Legal entity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Note:** Natural Person and Complex Legal entity are examples of client types. The table above shows a simplified example of risk assessment based on client type, product type, jurisdiction, delivery channel, and occupation.
Risk-Based Approach: practical example

Risk Assessment – Risk Rating

- Scenario A - Prospective Client X is unemployed, stays in a foreign high risk country in terms of the corruption perception index and insist on concluding the purchase of a house with no face to face meeting, and seeks to pay for the house in cash.

- Scenario B - Prospective Client F is employed and earns a great salary, stays in South Africa, has approach the accountable institutions S in person for its services. Prospective client F will pay for the house by means of a mortgage loan. Client F bought his first house through the accountable institution, a few years ago.
Risk-Based Approach

Risk Assessment – Risk Rating

Correct answer:
Scenario A – May possible be high risk – consider:
• Unemployed – source of funds?
• Foreign high risk country – highly likelihood of corruption
• Non-face to face – level of anonymity
• Cash – not traceable – source of funds?
• Client new to the accountable institution – no historic transactions and/or customer relationship
Risk-Assessment – Risk Rating

- Scenario C - Prospective Client G is a municipality manager (domestic prominent influential persons) and has been the subject of negative media reports. Prospective client G states that his salary is his only source of funds. Client G seeks to buy a luxurious 21 million rand house at the beach front and seeks to pay half of the amount upfront.

- Scenario D – The prospective client is company K registered in South Africa represented by person B.

- The beneficial owner of company K is a domestic prominent influential person who has been linked to alleged criminals in media reports. Company K seeks to buy a house in Camps Bay.
Correct answer:

- Scenario C and D – may possible be high risk – consider:
  - Domestic prominent influential persons associated with negative media reports
  - Higher susceptibility to corruption
  - Consider source of funds? Can a municipality manager afford a R21 million rand vacation home solely from salary received?
Risk-Based Approach

Risk monitoring, mitigation and management - treatment of risk

- Controls includes:
  - Processes, systems, resources, monitoring, reporting and training etc.
- The control must be in proportion to the risk, i.e.
  - Higher risk – enhanced due diligence
  - Medium risk – additional due diligence
  - Lower risk – simplified due diligence
- Risk will be adequately treated = level of residual risk is acceptable and within the risk appetite of the accountable institution
Risk Management and Compliance Programme (RMCP)

- Prior to October 2017, the FIC Act and money laundering and terrorist financing regulations prescribed what information should be obtain when identify different types of persons, and what documents should be reviewed in order to verify the identification information.

- Currently the FIC Act does not prescribe which documents must be used when verifying information.

- MLTFC Regulations Chapter 4 sets out the minimum information that must be provided in reports.

- Section 42 of the FIC Act places an obligation on accountable institutions to develop, document, maintain and implement a RMCP, which should state which documents are relied on for verification.
Risk Management and Compliance Programme

- **WHO**
  - All accountable institutions
  - Approved by, and responsible party are the board of directors

- **WHAT**
  - Policies, procedures, systems and controls for RBA, AML / CTF

- **WHEN**
  - Current, and ongoing reviews

- **WHERE**
  - All branches of an accountable institution
  - International application as the minimum standard

- **WHY**
  - To understand ML & TF risk facing the entity, and to allocate the appropriate time and resources
RMCP

- Risk identification
- Customer Due Diligence
- Transactional Monitoring
- Targeted Financial Sanctions
- Reporting to the FIC
- Record keeping
- Extended registration model of entity
- Implementation of RMCP
Risk Management and Compliance Programme: Customer Due Diligence

No anonymous clients

- E.g. estate agents may not do business with an anonymous client or client with apparent false or fictitious name

Single transaction

- Single transaction = transaction where amount is more than R5000
- Not conducted on a regular interval
Identification and verification

- Client information **obtained** during the **take on stage or part of the client engagement process**
- **Verification** - corroboration of the information by comparing it against the **original source, electronic data issued or reliable third party**. Information must be accurate.
- **Flexibility** to choose the type of information to establish the client’s identity and the means to verify information obtained
- The **nature and extent** of the verification to be determined on the **assessed risk** and in terms of RMCP
- Verification must occur during the course of conducting the single transaction/business relationship but must complete the verification **before it concludes a transaction**
Identification and verification

- Examples of sources of information that may be used to verify a client's identity include:
  - Records of the Department of Home Affairs
  - Records of the Companies and Intellectual Property Commission
  - Records of the South African Revenue Service
  - eNaTIS records
  - Records of the Master of the High Court.
Identification and verification

- Examples of government issued or controlled sources of information
  - Valid driver’s licence
  - Foreign identity documents
  - Passports
  - Asylum seeker or refugee permits
  - Work permits
  - Visitor’s visas
Accountable institutions must

- Identify all its prospective clients
- Identify all persons authorised to act on behalf of clients
- Verify identities
- In line with the accountable institutions RMCP

Accountable institutions must understand and obtain information on business relationship

- The nature of a business relationship
- The intended purposes of a business relationship
- Source of funds
- In line with the accountable institutions RMCP
Risk Management and Compliance Programme: Additional due diligence part of CDD

When dealing with legal persons, trust and partnerships additional due diligence measures apply. Accountable institutions must obtain information on:

- The nature of the clients business
- The ownership and control structure of the client
- In line with the accountable institutions RMCP

The FIC Act defines a “beneficial owner” in respect of a legal person as the natural person who, independently or together with another person, owns the legal person or exercises effective control of the legal person.
Risk Management and Compliance Programme: Additional due diligence part of CDD

Legal Person – Beneficial Ownership

- Identify each natural person who has **controlling interest** in the legal person (e.g. shareholding); failing which
- Identify each natural person who **exercises control over** that legal person (e.g. Proxy, voting shares); failing which
- Identify each natural persons who **exercise control of the management** of that legal person (management, directors)
- Take reasonable step to verify the identity of the beneficial owners
- In line with the accountable institutions RMCP
Risk Management and Compliance Programme: Additional due diligence part of CDD

Company X’s authorised representative wants to buy a property on behalf of Company X.

Company E owns 100% voting rights in company X.

Mr. S owns 100% voting rights in Company E.

Mr. S therefore owns 100% of Company X voting rights.

Accountable institutions must identify and verify:

- Company X’s authorised representative
- Company X
- Mr. S – because Mr. S is the Beneficial Owner of 100% of Company X
Legal persons, partnerships and trusts = vulnerable to be used for money laundering

- The lack of adequate, accurate and timely beneficial ownership information facilitates money laundering or terror financing by disguising:
  - The identity of known or suspected criminals
  - The true purpose of an account or property held by the legal entity
  - The source or use of funds or property associated with the legal entity

- The establishment of beneficial ownership is important for two reasons:
  - Understand the customer profile to properly assess the money laundering or terror financing risks associated with the business relationship
  - Take appropriate steps to mitigate the risks
Accountable institutions must obtain the following information when dealing with a PARTNERSHIP:

- Name of the partnership
- Identify every partner
- Identify the person who exercises control over the partnership
- Identify the person who is authorised to transaction on behalf of the partnership
- Take reasonable steps to verify the information and identities as obtained
Risk Management and Compliance Programme: Additional due diligence part of CDD

Accountable institutions must obtain the following information when dealing with a TRUST:

- Name and number of trust
- Address of the Master of the High Court where trust is register
- Identify the founder
- Identify the trustees
- Identify the person who is authorised to transaction on behalf of the trust
- Identify each beneficiary named in the trust deed
- Where no beneficiaries are named, obtain the particulars of how beneficiaries are determined
- Take reasonable steps to verify the information and identities as obtained

The requirements that apply to legal persons, partnerships or trust regardless even where incorporated or originated in South Africa or elsewhere.
Risk Management and Compliance Programme

Inability to conduct

- Customer due diligence,
- Obtain additional due diligence information or
- Conduct ongoing due diligence

then the accountable institution must:

- Not establish the business relationship / conduct a single transaction
- Must terminate an existing client relationship
- Consider filing a section 29 STR report
Risk Management and Compliance Programme

When dealing with a foreign prominent public official, domestic prominent influential person and/or family members or know close associates of these persons an accountable institution must:

- Obtain senior management approval to establish a business relationship
- Establish the source of wealth
- Enhanced due diligence monitoring
Risk Management and Compliance Programme
CDD

Foreign prominent public officials – schedule 3B to the FIC Act

- Head of State
- Members of a foreign royal family
- Government ministers
- Senior judicial officers
- Senior executives of state owned companies
- High ranking member of the military

Includes family members and known close associates
Risk Management and Compliance Programme
CDD

Domestic prominent influential persons – scheduled 3A to the FIC Act

- The President, Ministers and Premiers
- Members of the royal family and senior traditional leaders
- DGs and CFOs of government departments
- Executive mayors and municipal managers
- CEOs and CFOs of state entities like Eskom, Telkom, FIC, FSCA, NGB, EAAB, etc.
- Judges
- Senior officials of companies who receive certain tenders from government

Includes family members and known close associates
Risk Management and Compliance Programme: Transactional Monitoring

An accountable institution must

- Monitor transactions
- Source of funds to ensure consistent with clients business and risk profile
- Background and purpose of all complex transactions

Doubts about veracity

Where an accountable institution doubts veracity or adequacy of previously obtained information, the accountable institution must repeat the identification and verification steps taken
Risk Management and Compliance Programme: Reporting

- **S28 - CTR**: Cash payment (CTR)
- **S28A - TPR**: Terrorist Financing (TPR)
  - Financial Sanctions (TPR)
- **S29 - STR**: Money Laundering (STR/SAR)
  - Terrorist Financing (TFTR/TFAR)
  - Financial Sanctions (STR/SAR)
- **S31 - IFTR**: Cross-border money movement (IFTR)
Risk Management and Compliance Programme:
Cash Threshold Reporting (CTR)  

S28 FIC Act

- An accountable institution must report cash transactions of R24 999, 99 and above
- Cash, coins, paper money and travellers cheques (not an EFT)
- Within two 2 days of the transaction (pending regulatory update)
Risk Management and Compliance Programme: Terrorist Property Reporting (TPR)

S28A FIC Act

- An accountable institution which has in its possession or under its control property owned or controlled by or on behalf of, or at the direction of:
- A terrorist, and/or
- A sanctioned person must within the 5 days of becoming aware report that fact and the prescribed particulars to the FIC
- An accountable institution must scrutinise its client information to determine whether such person is a terrorist, and/or a sanctioned person

Guidance note 6A
Risk Management and Compliance Programme: Terrorist Property Reporting

S28A FIC Act, cont.

- An accountable institution must scrutinise its client information to determined whether such person is a terrorist, and or a sanctioned person
- Accountable institutions must be able to identify sanctioned individuals
- Screening of existing clients and prospective clients against sanctions list
- When?
  - Client take on process
  - When new lists are adopted and published
Risk Management and Compliance Programme: Suspicious and unusual transaction reporting

Section 29

- STR Regulation 23
- SAR Regulation 23A
- TFTR Regulation 23B
- TFAR Regulation 23C
Risk Management and Compliance Programme: Suspicious and unusual transaction reporting

- **STR** - refers to a suspicious or unusual activity report in respect of proceeds of unlawful activities or money laundering, or suspicious or unusual activity, or a contravention of a prohibition under section 26B. The report relates to a transaction or a series of transactions between two or more parties.

- **SAR** - refers to a suspicious or unusual activity report in respect of proceeds of unlawful activities or money laundering, or suspicious or unusual activity, or a contravention of a prohibition under section 26B. The report relates to an activity which does not involve a transaction between two or more parties or in respect of a transaction or a series of transactions about which enquiries are made, or in respect of an incomplete, abandoned, aborted, attempted, interrupted or cancelled transaction, but which transactions has not been concluded, respectively.
Risk Management and Compliance Programme: Suspicious and unusual transaction reporting

- **TFTR** - refers to a terrorist financing transaction report, where there is a suspicion or knowledge relating to the financing of terrorist and related activities where the report relates to a transaction or series of transactions between two or more parties.

- **TFAR** - refers to a terrorist financing activity report, where there is a suspicion or knowledge of the financing of terrorist and related activities. The report relates to an activity which does not involve a transaction, or is in respect of a transaction or a series of transactions about which enquiries are made or in respect of an incomplete, abandoned, aborted, attempted, interrupted or cancelled transaction, but which transactions has not been concluded, respectively.
When filing STRs, SARs, TFTRs, TFARs the suspicion or knowledge relates to:

- The proceeds of unlawful activity
- Unlawful activity
- Facilitating the transfer of proceeds of unlawful activity
- Has no apparent business or lawful purpose
- May be relevant to the investigation of an evasion or attempted evasion of a duty to pay tax evasion or attempted tax evasion
- An offence relating to the financing of terrorist and related activities
- The contravention of a prohibition under section 26B of the FIC Act; and / or
- Any structuring of a transaction or activity which is conducted for the purpose of avoiding giving rise to a reporting duty under the FIC Act
Risk Management and Compliance Programme: Record keeping

Accountable institutions must keep records of:

- Client information and transaction information
- Business relationship
- Reports submitted to the FIC
- The client 5 years from date of termination of relationship, conclusion of transaction and or submission of a report
- Electronic and hardcopies

- The Accountable institution can make use of 3rd party storage providers

- Records must be accessible and kept safe
Accountable institutions must provide ongoing training to their employees on compliance with the FIC Act and their RMCP.

Training levels and intervals to be specified in the RMCP.
THANK YOU
Achievements as a result of the production and utilisation of financial intelligence reports and services to assist in the identification and combating of crime
OUTLINE

- Life cycle of a Statutory Report
- Statistical overview of reporting: all scheduled entities
- Accountable vs reporting entities
- Selected Reporting Categories
- Targeted Financial Sanctions (TFS)
- What makes a good STR
- Case Studies and Typologies
- Indicators
- Statistical overview of production
### Life cycle of a regulatory report

<table>
<thead>
<tr>
<th>Accountable institution/business - Risk/Trigger</th>
<th>Institutional internal processes</th>
<th>Regulatory Reports</th>
<th>goAML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigating Authority / Investigative division in an Organ of State</td>
<td>SIU</td>
<td>Public Protector</td>
<td>Initiate proactive financial intelligence reports</td>
</tr>
<tr>
<td>NPA</td>
<td>LEAs</td>
<td>Respond to reactive financial intelligence</td>
<td></td>
</tr>
<tr>
<td>Foreign FIUs</td>
<td>Intelligence Services</td>
<td>SARS</td>
<td></td>
</tr>
<tr>
<td>Supervisory bodies</td>
<td>Defense Intelligence</td>
<td>IPID</td>
<td></td>
</tr>
</tbody>
</table>

Construct a narrative on the type and extent of illegal activities involved through the approach of following the money.
Statistical Overview of Reporting
Number of Reports: Year on Year

INCREASE OF 5.2%
Statistical Overview
All Report Types: 2018/2019

Section 28: 5,214,568 (94.7%)
Sec 28A: 308 (0.056%)
Section 29: 2,884,344 (5.2%)

TOTAL: 5,503,310
Composition of Sec 29 Reports

SAR: 71,696
STR: 144,730
STRB: 71,818
TFAR: 30
TFTR: 160

TOTAL SEC 29: 288,434
5.2% of total reports
<table>
<thead>
<tr>
<th>Schedule 1: Item No.</th>
<th>Total registered entities at 31 March 2018</th>
<th>Total registered entities at 31 March 2019</th>
<th>Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE - Business entity with a reporting obligation in terms of Section 29 of the FIC Act</td>
<td>91</td>
<td>128</td>
<td>37</td>
</tr>
<tr>
<td>1 Attorneys</td>
<td>13 322</td>
<td>14 298</td>
<td>976</td>
</tr>
<tr>
<td>2 Trust companies</td>
<td>173</td>
<td>189</td>
<td>16</td>
</tr>
<tr>
<td>3 Estate agents</td>
<td>10 242</td>
<td>10 444</td>
<td>202</td>
</tr>
<tr>
<td>4 Authorised users of an exchange</td>
<td>184</td>
<td>156</td>
<td>-28</td>
</tr>
<tr>
<td>5 Unit trusts (collective investment schemes managers)</td>
<td>85</td>
<td>77</td>
<td>-8</td>
</tr>
<tr>
<td>6 Banks</td>
<td>41</td>
<td>37</td>
<td>-4</td>
</tr>
<tr>
<td>7 Mutual banks</td>
<td>4</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>8 Long-term insurers</td>
<td>89</td>
<td>94</td>
<td>5</td>
</tr>
<tr>
<td>9 Gambling</td>
<td>3 130</td>
<td>3 590</td>
<td>460</td>
</tr>
<tr>
<td>10 Foreign exchange agent or company</td>
<td>362</td>
<td>289</td>
<td>-73</td>
</tr>
<tr>
<td>11 Money lender against securities</td>
<td>73</td>
<td>79</td>
<td>6</td>
</tr>
<tr>
<td>12 Investment advisors or intermediaries</td>
<td>8 556</td>
<td>8 441</td>
<td>-115</td>
</tr>
<tr>
<td>13 Issuer of travellers’ cheques and money orders</td>
<td>165</td>
<td>159</td>
<td>-6</td>
</tr>
<tr>
<td>14 Postbank</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>15* ……………………</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 Ithala Bank</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>17* ……………………</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18* ……………………</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 Money remitters</td>
<td>265</td>
<td>252</td>
<td>-13</td>
</tr>
<tr>
<td>Schedule 3: Item No.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Motor vehicle dealers</td>
<td>3 809</td>
<td>3 891</td>
<td>82</td>
</tr>
<tr>
<td>2 Kruger rand dealers</td>
<td>206</td>
<td>223</td>
<td>17</td>
</tr>
<tr>
<td>Grand Total</td>
<td>40 799</td>
<td>42 353</td>
<td>1 554</td>
</tr>
</tbody>
</table>

* Items 15, 17 and 18 were deleted from Schedule 1 to the FIC Act in 2010
Variance: Registered Entities 2017/2018 vs 2018/2019

- Attorneys: 14,298 vs 13,322 (976)
- Estate Agents: 10,444 vs 10,242 (202)
- Investment advisors or intermediaries: 8,441 vs 8,556 (-155)
- Motor Vehicle Dealers: 3,891 vs 3,809 (82)
- Gambling sector: 3,590 vs 3,130 (460)
Reporting by Attorneys

CTR: 2348
CTRA: 156
SAR: 35
STR: 395
STRB: 0
TPR: 0

0.05% of all reports
Reporting by Estate Agents

- CTR: 3,335
- CTRA: 1,697
- SAR: 4
- STR: 7
- STRB: 0
- TPR: 306

0.098% of all reports
Reporting by Gambling Sector

- CTR: 114,367
- CTAR: 324,655
- SAR: 649
- STR: 1,414
- STRB: 0
- TFAR: 1
- TFTR: 0
- TPR: 0

8% of all reports
Reporting by Investment Advisors or Intermediaries

CTR: 10,958
CTAR: 812
SAR: 1,046
STR: 1,244
STRB: 0
TFAR: 3
TFTR: 1
TPR: 0

0.25% of all reports
Reporting by Motor Vehicle Dealers

CTR: 28,095
CTAR: 2,976
SAR: 128
STR: 4,464
STRB: 5,682
TFAR: 2
TFTR: 155
TPR: 0

0.75% of all reports
## Good and Bad Practices

<table>
<thead>
<tr>
<th>GOOD PRACTICE</th>
<th>BAD PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection of appropriate indicators</td>
<td>Selection of default indicators</td>
</tr>
<tr>
<td>• Enables FIC to correctly assess and prioritise reports</td>
<td>• Hampers the analysis efforts of the FIC (Trends analysis and Typologies)</td>
</tr>
<tr>
<td>Selecting the correct report type SAR/STR/CTR</td>
<td>Selection of incorrect report types SAR/STR</td>
</tr>
<tr>
<td>• Provides the FIC with a clear picture of the flow of funds in terms of STRs</td>
<td>• Providing the FIC with inaccurate/incomplete information</td>
</tr>
<tr>
<td></td>
<td>• Mismatch of data as each report type has relevant fields that assist in identifying certain behaviors of subjects</td>
</tr>
<tr>
<td></td>
<td>• A CTR is filed when a subject exceeds the threshold amount, therefore when an entity deems it necessary to file a STR as well, this requires further information as to why the transaction or attempted transaction was deemed suspicious.</td>
</tr>
<tr>
<td></td>
<td>• Reports where transactions were not yet concluded, or when fraudulent documents were submitted and no transactions were concluded, should be filed as SARs.</td>
</tr>
</tbody>
</table>
### Good and Bad Practices

<table>
<thead>
<tr>
<th>GOOD PRACTICE</th>
<th>BAD PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detailed “reasons for suspicion”</td>
<td>No details pertaining to the reason for suspicion</td>
</tr>
<tr>
<td>• KYC information, previous transacting patterns and expected sources of income provide context to the report</td>
<td>• Hampers the FIC’s ability to correctly assess and prioritise the reports as well as provide law enforcement with timeous and relevant intelligence products.</td>
</tr>
<tr>
<td>• A report that can answer most of the 5W1H (Who, what, when, where, why and how) is considered a good report</td>
<td>• Provide minimal information in the “reason for suspicion” field</td>
</tr>
<tr>
<td></td>
<td>• One line/ one word explanations, no context.</td>
</tr>
</tbody>
</table>
### Good and Bad Practices

<table>
<thead>
<tr>
<th>GOOD PRACTICE</th>
<th>BAD PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct completion of fields on goAML</td>
<td>Incorrect or incomplete information provided on goAML</td>
</tr>
<tr>
<td>• Enables goAML to correctly link the report to previous reports submitted on a subject or entity by other AIs or RIs</td>
<td>• goAML cannot correctly link the subject or entity to previous reports filed.</td>
</tr>
<tr>
<td>• Completion of transactions in the correct fields enables goAML to aggregate the amount of funds involved as well as the number of reports a subject or entity is involved in.</td>
<td>• Incorrect capturing of data/amounts e.g.. R277 500-00 captured as R2 775 000-00.</td>
</tr>
<tr>
<td>• Completion of transactions provides a snapshot of the transacting pattern of the reported subject and complements the grounds of suspicion</td>
<td>• Specifying in the “reason for suspicion” field, “Cash Threshold” but the transaction mode/manner in which the payment was made, was in the form of “Electronic Fund transfers” and not actual cash payments.</td>
</tr>
<tr>
<td>• Capturing of GIS/address information enables the FIC to geolocate suspicious activities/transactions</td>
<td>• Transaction mode/manner in which payments were made should consistently be captured the same throughout the transaction. (E.g.. EFT and later in the transaction cash)</td>
</tr>
</tbody>
</table>
What makes a good report

Provide clear and concise information i.e.:

- **Who:** The subject, its associates and relationships
- **What:** The transaction or activity
- **When:** Date of detection, date of occurrence, span of time
- **Where:** Location of the client and where the transaction occurred
- **How:** Describe how the activity/transaction was completed or attempted
- **Why:** Results of your investigation into why the activity/transaction is reported/suspicious
Minimum Reporting Requirements from an analytical perspective

- Source of Income – Adequate provision of this information is necessitated to understand the activity conducted in the account.
- Source of Wealth – Where applicable, this declaration will clarify the position of an individual and either affirm or negate suspicions in terms of the subjects’ net worth.
- Mobile telephone numbers linked to accounts / All contact details.
- Domestic Prominent Influential Person (DPIP) – State that a DPIP was identified and the means of identification.
- Foreign Prominent Public Official (FPPO) – State that a FPPO was identified and by what means the identification took place.
- Report **Beneficial Ownership** as identified.
  - The natural person(s) who directly or indirectly holds a minimum percentage of ownership interest in the legal person (threshold approach);
  - Shareholders who exercise control alone or together with other shareholders;
  - Natural person(s) who exerts control without ownership by participating in the financing of the business, close/intimate family relationships, contractual associations etc.
TARGETED FINANCIAL SANCTIONS

Where in the FIC Act is TFS discussed?

• Section 26A, 26B and 26C, 28A(1)(c) and 29(1)(b)(vi)

• TFS measures generally restrict sanctioned persons and entities from having access to funds and property under their control and from receiving financial services in relation to such funds and property.
Role of Monitoring & Analysis: Daily Routine Screening

1. Filed reports in database
2. Screened against TFS list; matches are found according to pre-determined rules
3. Report generated indicating possible matches
4. Sanctions officers conduct further checks to confirm/refute match
5. Matches are referred to operational analysts for further investigation and possible referral
6. If no match, the file/task is closed
CASE STUDIES USING FINANCIAL INTELLIGENCE TO COMBAT CRIME
Case study 1: VAT fraud

FIC involvement
The FIC assisted SARS in a case involving an individual and his business that were allegedly part of a large VAT refund fraud scheme.

The Scheme
The scheme used several gold and diamond businesses as a front.

How VAT fraud was committed
The subjects involved were suspected to be “round-tripping” – trading between each other so that the same batch of gold was exported in one form and imported back in a different form. This process was repeated many times in order to claim significant VAT refunds from SARS.

Using financial intelligence
The FIC identified and analysed suspicious transactions, and subsequently issued a certificate on the regulatory reports it had received to confirm that they were admissible as evidence and could be used in court to support SARS’ application against the subjects.
Case study 2: Fraud and corruption

The FIC received an STR linked to a businessman indicating that his transactional activities had criminal features of fraud and corruption.

When the subject opened his personal bank account he claimed to be employed by an entity and provided a payslip from this entity. However, the FIC’s analysis revealed that the subject only received one payment from this entity into the personal account over a two-year period. Most of the funds emanated from the subject’s business and investment bank accounts. The business bank account was being credited with large amounts of money from three entities, including the subject’s alleged employer.

Funds were mostly disposed of through cash withdrawals and electronic fund transfers to different bank accounts linked to the subject. Large sums were paid to different individuals and car dealerships. The business bank account did not reflect transactions indicative of operational expenses, such as salary payments for employees.

The FIC submitted its findings to the South African Police Service for the investigation.
Case study 3: Exposing corruption and tax evasion

• The FIC received information indicating that a **politically exposed person** had bought various **vehicles** for his family members using electronic fund transfers.

• The FIC’s analysis revealed that over a period of seven years the individual had received more than R2 million in **cash** through his personal account and more than R20 million was paid into an entity’s account linked to the person.

• None of the funds in the entity’s account were used on **business expenses** like salaries, rent and payments to SARS. Instead, the money had been transferred between the two accounts and used for personal and lifestyle expenses.

• The FIC prepared a **proactive financial intelligence report** to law enforcement and the SARS for investigation.
Case study 4: Fraudster stealing from employer caught

1. **BACKGROUND**
   The FIC assisted the Asset Forfeiture Unit in a case where an employee of a company had defrauded her employer of more than R15 million by colluding with a legitimate supplier of transport services for her employer’s staff.

2. **MODUS OPERANDI**
   The subject, employed as a creditor’s clerk, told her company’s transport service provider that the employer was purposefully manipulating its invoices to escape input tax liability and save money.

3. **COLLUDING WITH SUPPLIERS**
   She said she would ensure that the VAT was correctly calculated and paid into the supplier’s account. However, since the employee was doing this without the employer’s knowledge or authority, she asked the service provider to transfer half of the “VAT” amount into her personal account as her share for helping the transport provider retrieve the “VAT” that was due to it.

4. **AMOUNT INVOLVED**
   This continued for several months. By the time the employee was caught she had stolen more than R15 million.

5. **HEADING**
   The FIC analysed the employee’s accounts and traced assets that had been acquired with the funds. Through this process, a large amount of money left in the employee’s account was blocked. After the FIC identified several assets that were purchased using the stolen funds, the Asset Forfeiture Unit obtained a restraint order. The assets included immovable property, motor vehicles and other household contents.
Case study 5: Rhino horn trafficker bust

BACKGROUND
An investigating team asked the FIC to provide information on individuals allegedly involved in illegal rhino horn trafficking.

CRIME
The subjects, all based in Mpumalanga, were dealing with large amounts of cash, mainly used to recruit people to poach or procure rhino horns.

RESULTS
Based on the FIC’s financial intelligence produced, the investigating team conducted surveillance that led to the arrest of the subjects.

REPORTS
The FIC had received several regulatory reports on these individuals.

SYNDICATE
The subjects were later linked to several rhino killings in Kruger National Park and other national parks.
### Case study 6: E-mail fraud scams US company

<table>
<thead>
<tr>
<th><strong>US</strong></th>
<th><strong>South Africa</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• The US required assistance in a case involving the <strong>defrauding of a company registered in the United States</strong>.</td>
<td>• The FIC discovered that part of the funds had already been used and the rest had been transferred to another South African bank account.</td>
</tr>
<tr>
<td>• A company employee received a fraudulent e-mail from an address similar to a colleague’s address, instructing him to transfer funds to a bank account for the purchase of a vehicle.</td>
<td>• After verifying the facts and obtaining the necessary documentation from investigators, the FIC issued an instruction directing the bank not to proceed with any transactions on the two identified accounts, which at the time had a cumulative balance in excess of R500 000.</td>
</tr>
<tr>
<td>• The employee transferred R607 000 before realising that the e-mail was fraudulent.</td>
<td>• The Asset Forfeiture Unit was granted a preservation order allowing it to seize and repatriate the funds to the USA in these two accounts.</td>
</tr>
</tbody>
</table>
Case study 7: Ponzi scheme bust

- The FIC received several STRs indicating that an entity and its directors may be operating a **Ponzi investment scheme**. The entity's two bank accounts were receiving large cash deposits. Looking at information available on the internet, the FIC discovered that the scheme was being advertised online, promising its investors inflated opportunities.

- The Ponzi scheme was operating **through multiple entities and individuals**. Funds were mainly received through cash deposits and then transferred to others involved in the scheme. The funds paid by existing investors were used to pay new investors.

- The FIC requested bank statements for all the entities and individuals involved in running the scheme using Section 27A of the FIC Act. After receiving all the bank documents, the FIC **analysed the transactions**. It also requested an affidavit from the Financial Sector Conduct Authority, which confirmed that the main entity was not authorised as a financial services provider.

- The FIC drafted an affidavit, which led to the Hawks Commercial Crime division **opening an investigation into the scheme**. The Hawks then sent the case to the National Prosecuting Authority for a decision.
Case study 8: Cyber theft in the US

USA

• The FIC’s counterpart in the United States, the Financial Crimes Enforcement Network, reported that four subjects with links to South Africa may have been implicated in an international cyber theft scheme that has been operating between 2014 and 2018.

• The scheme involved phishing, spear-phishing, hacking and intrusion tactics to gain access to victims’ e-mail accounts and funds. The subjects then engaged “mules” in the United States to transfer illicit funds to overseas bank accounts. About US$2 million was identified, but according to the Federal Bureau of Investigation between US$5 million and US$10 million may have been transferred to various destinations.

South Africa

• Intelligence indicated that the subjects may have several individuals in South Africa assisting with the scheme.

• The FIC identified various local bank accounts linked to the subjects and the information was subsequently referred to the Hawks and the Asset Forfeiture Unit was granted a preservation order allowing it to seize and repatriate the funds to the USA in these two accounts.
## Case study 9: Working with Denmark to track stolen millions

<table>
<thead>
<tr>
<th>Denmark</th>
<th>South Africa</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Denmark’s financial intelligence unit asked the FIC to provide</td>
<td>- Through its analysis the FIC identified cash and assets linked to the</td>
</tr>
<tr>
<td>information on four Danish nationals (a mother and her three adult</td>
<td>subject. Based on the Asset Forfeiture Unit’s request, the FIC froze</td>
</tr>
<tr>
<td>children).</td>
<td>R6.7 million.</td>
</tr>
<tr>
<td>- The main subject (the mother) was suspected of defrauding her former</td>
<td>- The AFU has since seized and returned the funds to the Danish government.</td>
</tr>
<tr>
<td>employer, the Danish National Board of Social Services.</td>
<td></td>
</tr>
<tr>
<td>- She had been dismissed by that employer and subsequently fled to</td>
<td></td>
</tr>
<tr>
<td>South Africa.</td>
<td></td>
</tr>
</tbody>
</table>
The FIC received regulatory reports on deposits into the accounts of 21 individuals predominantly from low income rural areas. The FIC’s analysis revealed that the individuals had given their personal details to a money remittance syndicate, enabling it to open accounts with a cryptocurrency exchange. Over a period of four months the syndicate deposited R415 million into the 21 accounts held with the crypto currency exchange. The funds were exchanged for Bitcoin and a total of XBT 3 081 was transferred to and withdrawn from Chinese crypto currency exchanges.

The accounts were being accessed from outside South Africa, predominantly from Hong Kong and Beijing, which was not possible as none of the implicated individuals had passports and therefore could not travel to these countries.

The FIC prepared proactive financial intelligence reports and referred the matter to law enforcement agencies, and the implicated individuals were referred to the South African Police Service and the SARB for contravening exchange control regulations, evading tax and money laundering.
Case study 11: Abalone poachers arrested

The FIC supported Law Enforcement Agencies (LEAs)

NPA and AFU investigated certain government officials

As a result, a number of officials have been arrested and are facing charges of racketeering, theft, defeating the ends of justice and corruption.

The FIC's intelligence was used to trace assets, bank accounts and relevant financial information of the implicated officials and syndicate members.

It was alleged that these officials were involved in an abalone poaching syndicate.
Case study 12: Drug lab bust in Limpopo

**BACKGROUND**
Limpopo has seen a surge in drug abuse recently. The FIC was part of an intelligence-led narcotics operation in the province. Several dealers had been identified and arrested.

**FINDINGS**
The FIC profiled all subjects which indicated that both these individuals, who lived in Kempton Park, Gauteng, could be supplying drugs to Limpopo.

**RESULTS**
Money and machines used in the production of drugs were also seized. The arrested subjects are currently appearing in court.

**2018**
STRs

**2019**
Kingpins

**Outcome**

**ANALYSIS**
By gathering and analysing financial information, the FIC was able to identify a Nigerian national who was receiving cash payments from Polokwane, Bela Bela and Mokopane. A large portion of the funds received were then transferred to another individual known to the FIC before this matter.

**SYNDICATE**
Law enforcement conducted a search and seizure operation and arrested six suspects. It found and dismantled a laboratory, which contained nyaope and heroine worth millions.
For the period 2018/2019 the FIC published the following typologies reports:

- **Typologies and Case Studies - Published Date : March 2019**
  - Casinos and the gambling industry
  - Property sector

- **Scams and Typologies - Published Date : December 2018**
  - Scams (Crypto, Initial Coin offerings and Identity fraud
  - Typologies (PIPs, Drugs trafficking, rhino poaching and armed robberies

- **Typologies - Published Date : September 2018**
  - Cybercrime, courier scams, inheritance fraud, online shopping, online gaming, crypto (Ponzi's) and fake jobs

- **Typologies - Published Date : May 2018**
  - 3rd party accounts, change of bank detail, casinos, corruption, narcotics, cybercrime, Ponzi, Tax evasion and environmental crimes

Detection Indicators

- High end **vehicle purchases** that are seemingly not in line with the expected income of the customer.
- Concealment/misuse within **Business** structures
- Illogical business **activity** - why do multiple transfers at a higher charge
- Multiple **transactions** in a short time period with no underlying business rationale
- Use of **False** Identities and documents / Missing documentation normally to be expected from a legitimate business
- Purchasing of property in **family** members’ names.
- Purchasing of valuable **commodities** / **extreme luxury goods**, normally associated with extremely wealthy persons (Brand Name Boutique Clothing, expensive watches and expensive electronic goods etc.)
- Gambling activities - significant year on year **increase** in turnover / not in line with the expected income of the customer.
- Declared Source of Income **not aligning** to activity of the customer /exceeds the expected deposits for the customer.
STATISTICS
Crime Types Investigated 2013 to 2018

Operational Focus

Our priority focus areas:

- Fraud
- Narcotics
- Tax related
- Corruption
- Money Laundering
- Investment scams
Domestic and International requests from Law Enforcement Agencies for information responded to (2014-2018)

Proactive matters referred to Law Enforcement Agencies (2014-2018)
Suspected proceeds of crime frozen 2014-2019

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>Millions in Rands</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2014/2015</td>
<td>181.0</td>
</tr>
<tr>
<td>FY 2015/2016</td>
<td>184.6</td>
</tr>
<tr>
<td>FY 2016/2017</td>
<td>149.3</td>
</tr>
<tr>
<td>FY 2017/2018</td>
<td>3027.9</td>
</tr>
<tr>
<td>2018/2019</td>
<td>2143.2</td>
</tr>
</tbody>
</table>

Section 34 freezing of accounts
Proceeds of crime recovered using FinInt
Focused approach

- The FIC adopted an approach to classify matters that are high, medium and lower priority to ensure resources get appropriately allocated and proper focus is given to financial intelligence reports which are prepared. This will ensure that high priority matters get tracked through the full value chain of the investigation and show the expected outcome and impact.

- As we take pride in delivering service / providing products of high quality and in pursuance of continuous improvement we require authorised officers to evaluate and provide feedback on the outcome of matters of the financial intelligence disseminated.
Analysis in numbers - 2018/2019

- Reports received: 288,434 & 5.5mil
- Individuals and entities analysed: 15,663 & 15,295
- Bank accounts monitored: 45
- Bank accounts frozen: 46
- Affidavits issued: 29
- Proactive and Reactive Intelligence Reports issued: 1,054 & 1,840
- Contributions to recovery: R2.1billion

Reports received – suspicious and cash threshold.
Enquiries with Accountable Institutions and requests for further information.
Bank accounts: R52 million frozen.
CONCLUSION

• The FIC continuously strives to improve the quality of the financial intelligence it produces on proactive and reactive level, and this contributes to the combating of crime as identified through government-wide strategies.

• The FIC will continue to proactively identify crime patterns using its regulatory data streams and address the majority of requests for financial intelligence from authorised institutions.

• Operational functions include supporting law enforcement efforts, resulting in successful investigations, prosecutions and where possible, the freezing, preservation or confiscation of the proceeds of crime.
THANK YOU
Registration and Reporting Feedback
AGENDA

- Registration – updating entity and/or user details
- Reporting to the FIC – reports that can be submitted
- Information required for reporting
- Common reporting mistakes
- General reporting feedback and recommendations
- Reporting regulations updates
- Background and reference documents
Registration – updating entity and user details

Updating entity details (Directive 1 & Directive 4)

- The compliance officer or reporting officer needs to logon to goAML, select MY GOAML and then select My Org Details
- Update all entity details (including contact person, entity email, telephone and address), attach supporting documents when applicable and select Submit Request
- AI/RIs must keep copies of the entity registration confirmation as this cannot be re-issued
- NB - Directive 1 instructs all reporting entities to maintain their details on the FIC’s electronic platform

Updating User Details (Directive 2)

- The user needs to log on to goAML, select MY GOAML and then select My User Details
- Update all user details (including identification number, email, telephone and address), attach supporting documents when applicable and select Submit Request
- NB - Directive 2 instructs that users are not allowed to share their logon credentials
Reporting to the FIC
– reports that can be submitted

- Suspicious and unusual transaction report (STR)
  - Section 29
    - Suspicious and unusual transaction Report (STR)
    - Suspicious or unusual activity report (SAR)
    - Terrorist financing activity report (TFAR)
    - Terrorist financing transaction report (TFTR)

- Cash threshold report (CTR)
  - Section 28
    - Cash threshold report (CTR)
    - Cash threshold report aggregation (CTRA)

- Terrorist property report (TPR)
  - Section 28A
    - Terrorist property report (TPR)
    - Accountable institutions only
Reporting Feedback

- All reports must be submitted on goAML
- Each user must login with their own user credentials to submit reports
- Ensure that the correct report type is selected
- Ensure that reports are submitted under the correct branch and the correct schedule item
- Reports must be completed as comprehensively as possible
- Reports must be reviewed before being submitted – NO changes can be done once a report has been successfully processed
- The message board must be constantly monitored for report receipts
Information Required for Reporting

Parties Involved

• **Two Parties** for every transaction – Payer and Receiver of Funds

• **Type of Party** – Natural Person/Entity/ Account

• For a transaction one of the parties should be “**my client**” which means the full client details must be provided

Transaction/Activity Information

• If reporting a transaction then the **full details** of the **transaction** must be reported e.g. amount, transaction date, transaction location

• If reporting an activity then the full details of the activity must be reported e.g. date occurred, what happened etc.

**Goods and Services** involved if there are any
### Person, Entity or Account?

The relationship between person, entity and account when reporting a transaction on the reporting platform of the FIC (goAML).

<table>
<thead>
<tr>
<th>FROM</th>
<th>TO</th>
<th>Person</th>
<th>Entity</th>
<th>Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person</td>
<td>e.g. Person 1 pays Person 2 cash for goods/services in person</td>
<td>e.g. Person pays Entity cash for goods/services on premises</td>
<td>e.g. Person makes a cash deposit into personal account at Bank</td>
<td></td>
</tr>
<tr>
<td>Entity</td>
<td>e.g. Entity pays Person cash refund for goods/services on premises</td>
<td>e.g. Entity A pays Entity B cash for goods/services on premises</td>
<td>e.g. Entry A makes cash deposit into business account at Bank</td>
<td></td>
</tr>
<tr>
<td>Account</td>
<td>e.g. Person makes a cash withdrawal at Bank ATM</td>
<td>e.g. Conductor from Entity A makes a cash withdrawal in Bank branch</td>
<td>e.g. Electronic payment between two accounts</td>
<td></td>
</tr>
</tbody>
</table>
Information Required for Reporting

- The Money Laundering and Terrorist Financing Control Regulations outlines minimal client information and transactional data to be reported when a regulatory report i.t.o. sections 28, 28A and 29 of the FIC Act is submitted on goAML.

- Readily available information relates to information that ought to be obtained during the client identification and verification phase (e.g. CDD) and during the course of normal business (i.e. to make a transaction commercially viable).
Reporting Issues Identified

- Non-adherence to defined reporting timelines
- Not all products and services identified
- Reports not completed in full – missing client or transaction information
- Reports not being checked before being submitted to FIC
- Not all reportable events identified
- Rejected reports not remediated
General recommendations when filing a report in terms of S28

Reporting entities need to note the following in terms of their cash threshold transaction reporting:

- Only report **cash** transactions (**EFTs** / interbank transfers are not reportable)
- Remember to check your **bank statements** frequently (i.e. cash transactions conducted at your **premises** as well as deposited directly into your **bank account(s)** need to be considered)
- Define your **aggregation period** and document it in the risk management and compliance programme. This must be applied **consistently** to ensure that you can be **measured** accordingly
- When your entity receives frequent cash deposits/payments it may be valuable to conduct a lookback of the **previous day’s cash transactions**, apply aggregation and report to the FIC (i.e. **transaction plus one** = awareness therefore starts the following business day)
General recommendations when filing a report in terms of S28

- CTRA should only include multiple transactions conducted by the **same client** (i.e. single client view per AI/RI). AI/RIs are not allowed to group multiple clients and report them in the same CTRA (i.e. one CTRA per client).

- Cash deposits received versus cash payments made must be aggregated and reported separately (no netting off or summary of transactions is allowed).

- When submitting a CTR/CTRA, the transaction mode and fund type should either be “**Cash Received by AI/RI**” or “**Cash Paid by the AI/RI**”.

- When reporting your client the **client’s identity number, nationality and country of residence** fields need to be completed (in case of non-RSA ID and passport document the **issuing country** will also need to be completed).
General recommendations when submitting a report in terms of S29

A regulatory report filed in terms of section 29 of the FIC Act should provide the following answers:

- **Why** *(why are you filing = why do you feel uneasy or find the transaction unusual?)*
- **What** *(what caused you to submit the report = what was the indicators or red flags?)*
- **How** *(how did it occur = list specific modus operandi, behaviour and/or transaction modes)*
- **When** *(when did it occur = is it once off versus a series of transactions or events)*
- **Who** *(who was involved = is it one or more persons, entities or accounts)*
- **Where** *(location where this occurred)*
General recommendations when submitting a report in terms of section 29

General Tips:

• Complete the report in full
• If the suspicion was based on a transaction ensure that you capture the transaction information
• Clearly articulate why you find that particular transaction/activity suspicious
• Ensure you capture the **reason** field which is where you capture the “grounds of suspicion”
• Ensure that you capture the **action** field where you describe what action you took after the suspicion was formed
• Attach available **supporting documents** with the original report - this enables the FIC to see the entire picture from the onset
Regulatory Reporting – Recommendation for Reporting Entities

Reporting entities need to review their internal reporting processes and verify that all the products and services offered are mapped and reported correctly:

- Reporting entities should have documented reporting processes that outline the steps to be followed for the detection, monitoring, reporting and remediation of regulatory reports submitted to the FIC.

- The processes should outline the steps to be followed internally to conduct pre-validation and remediation of source systems.

- Reporting processes should be applied consistently across all business areas and should incorporate the regulatory reporting timeframes specified (i.e. 48 hours for CTR or CTRA and 15 days for SAR/STR etc.).

- Reporting entities should conduct regular reviews of all regulatory reports submitted to ensure they meet the prescribed requirements.
Reporting Entities need to provide frequent and practical training to their employees:

- Reporting entities should ensure that their staff receive adequate training
- Staff training should include practical sessions that enable staff to successfully submit regulatory reports on goAML (i.e. utilising the FIC UAT site)
- FIC published a registration user guide, regulatory reporting user guides, guidance (e.g. Guidance Note 05B and goAML Notices) and scenario examples to assist external entities to train their staff
- These publications must be used together with the Regulations to ensure that users are trained effectively and that reporting entities discharge their obligations accordingly
Reporting Recommendations - Record Keeping

- AI/RIs are advised to have adequate **record management processes** in place.

- The FIC recommends that AI and RIs keep copies of all submitted regulatory reports, messages (report receipts and request for information) on their internal systems

- All submitted reports can be **viewed and downloaded** under the **Submitted Reports** menu on goAML

- User must **download and save** copies of all regulatory reports submitted for **record keeping** purposes

- The reports must be downloaded within 30 days.

- Reports that get rejected must be **reverted** and **remediated/fixed**
Remediation of Rejected Reports

- All rejected reports must be remediated.
- Regulatory reports that have been rejected will clearly indicate the reason for rejection.
- The user must ensure that these regulatory reports are reverted and remediated accordingly.
- Ensure that you view the message on the Message Board that indicates the reason for rejection and revert the report in the Submitted Reports menu.
- After the report has been reverted it will be found under DRAFTED REPORTS.
- Web reports must be remediated as per the defined process whereby it is reverted back to draft status, edited, fixed and resubmitted.
- N.B. - Do not submit a new report as it creates duplicate and the original rejected report remains unresolved.
- Please refer to the user guides for further guidance.
Users are able to **save** regulatory reports before submitting them and can complete them at a later stage.

These reports are available in the **drafted reports** menu for **editing** and submitting.

Rejected regulatory reports captured on the web that get reverted may be **edited, remediated/fixed** and **resubmitted** to the FIC.

Users must check this menu on a regular basis and ensure all reports are completed and submitted.
Background and reference documents

Documents are available on the FIC website and tutorial videos on FIC’s YouTube account (i.e. registration and how to capture a CTR and STR)

- Registration in terms of section 43(B) of the FIC Act – Public Compliance Communication 05C
- Guidance Note 04B (STRs/SARs/TFTRs/TFARs in terms of section 29 of the FIC Act)
- Guidance Note 05B (CTRs/CTRAs in terms of section 28 of the FIC Act)
- Guidance Note 06A (TPRs in terms of section 28A of the FIC Act)
- Guidance Note 07 (RBA)
- Registration user guide
- Regulatory reporting user guides (per regulatory report type, e.g. CTR, CTRA, SAR, STR, TPR etc.)
- goAML web notice 04 (Remediation process)
- goAML web notice 05 (Feedback to all reporting entities)
## Amendments to the Reporting Obligations

<table>
<thead>
<tr>
<th>Current</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTR threshold set at R24,999.99</td>
<td>CTR threshold to be set at R49,999.99</td>
</tr>
<tr>
<td>CTR reporting period set to 2 days</td>
<td>CTR reporting period to be set to 3 days</td>
</tr>
<tr>
<td>CTRA to be reported</td>
<td>CTRA to be reportable</td>
</tr>
</tbody>
</table>

N.B. These amendments will only come into effect once the new obligations have been approved and have been communicated by FIC.
THANK YOU
Supervision and Enforcement
FIC Act supervision and enforcement model

- The FIC and supervisory bodies (SBs) are responsible for supervising and enforcing compliance with the FIC Act and any order, determination or directive made in terms of the FIC Act by all accountable and reporting institutions (AIs and RIs).

- The FIC is responsible for facilitating effective supervision and enforcement by SBs.

- The FIC is responsible for supervising and enforcing non-compliance with the FIC Act on AIs regulated or supervised by a SB, or where the SB fails to fulfil its responsibilities [s4(g)(ii), 45(3), 45B(6)(a)].
## Current supervisory model

<table>
<thead>
<tr>
<th>Accountable and Reporting Institutions</th>
<th>Supervisory Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks &amp; Mutual Banks</td>
<td>South African Reserve Bank</td>
</tr>
<tr>
<td>Long Term Insurance</td>
<td>• Prudential Authority</td>
</tr>
<tr>
<td>Dealers in Foreign Exchange</td>
<td>• Financial Surveillance Department</td>
</tr>
<tr>
<td>Redeemers of Travellers’ Cheques, Money Orders</td>
<td>• National Payment System Department</td>
</tr>
<tr>
<td>Money Remitters</td>
<td></td>
</tr>
<tr>
<td>Authorised User of an Exchange</td>
<td>Financial Sector Conduct Authority</td>
</tr>
<tr>
<td>Collective Investment Scheme Managers</td>
<td></td>
</tr>
<tr>
<td>Financial Services Providers</td>
<td></td>
</tr>
<tr>
<td>Trust Companies</td>
<td>Financial Intelligence Centre</td>
</tr>
<tr>
<td>Entities that lend money against the security of securities</td>
<td></td>
</tr>
<tr>
<td>Postbank</td>
<td></td>
</tr>
<tr>
<td>Ithala Development Finance Corporation Limited</td>
<td></td>
</tr>
<tr>
<td>Motor Vehicle Dealers</td>
<td></td>
</tr>
<tr>
<td>Kruger rand Dealers</td>
<td></td>
</tr>
<tr>
<td>Practicing Attorneys</td>
<td>Provincial Law Societies</td>
</tr>
<tr>
<td>Estate Agents</td>
<td>Estate Agency Affairs Board</td>
</tr>
<tr>
<td>Gambling Institutions</td>
<td>Provincial Gambling Boards</td>
</tr>
</tbody>
</table>
Proposed tripartite supervisory model
## Proposed Supervisory Model

<table>
<thead>
<tr>
<th>Accountable Institutions</th>
<th>Supervisory Bodies</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Banks &amp; Mutual Banks</td>
<td>South African Reserve Bank</td>
</tr>
<tr>
<td>• Long Term Insurance</td>
<td>• Prudential Authority</td>
</tr>
<tr>
<td>• Dealers in Foreign Exchange</td>
<td>• Financial Surveillance Department</td>
</tr>
<tr>
<td>• Redeemers of Travellers' Cheques, Money Orders</td>
<td>• National Payment System Department</td>
</tr>
<tr>
<td>• Money Remitters</td>
<td></td>
</tr>
<tr>
<td>• Authourised User of an Exchange</td>
<td>• Financial Sector Conduct Authority</td>
</tr>
<tr>
<td>• Collective Investment Scheme Managers</td>
<td></td>
</tr>
<tr>
<td>• Financial Services Providers</td>
<td></td>
</tr>
<tr>
<td>• Trust Companies</td>
<td></td>
</tr>
<tr>
<td>• Entities that lend money against the security of securities</td>
<td></td>
</tr>
<tr>
<td>• Postbank</td>
<td></td>
</tr>
<tr>
<td>• Ithala Development Finance Corporation Limited</td>
<td></td>
</tr>
<tr>
<td>• Motor vehicle dealers</td>
<td></td>
</tr>
<tr>
<td>• Kruger rand dealers</td>
<td></td>
</tr>
<tr>
<td>• Practicing Attorneys</td>
<td></td>
</tr>
<tr>
<td>• Estate Agents</td>
<td></td>
</tr>
<tr>
<td>• Gambling institutions</td>
<td></td>
</tr>
<tr>
<td>• New accountable Institutions</td>
<td></td>
</tr>
<tr>
<td>• Financial Intelligence Centre</td>
<td></td>
</tr>
</tbody>
</table>
FIC supervisory model

- Enforcement
- Inspections
- Compliance Monitoring
- Public Compliance Communications and Guidance Notes
- Public Awareness and Public Queries
FIC Act inspections

- The purpose of inspections is to determine the institutions’ level of compliance

- The FIC and SBs cannot use the inspections powers to investigate any criminal conduct

- Should the FIC or SB detect any criminal conduct during an inspection, it will refer the matter to law enforcement to investigate

- Allegations of criminal conduct may be an indication that an AI has not complied with the FIC Act and may lead to an inspection

- Inspectors must be in possession of their certificate when conducting inspections and must present this upon request

- Inspections are to be conducted on reasonable notice, at a reasonable time and within ordinary business hours.
FIC Act inspections (cont.)

- Inspectors require a warrant to conduct inspections on unlicensed businesses or at private residences unless consent is given by the person apparently in control of the business and/or the occupant of the private residence.

- In the inspection process, it is a criminal offence if an institution:
  - Fails to appear for questioning
  - Fails to produce any document relating to the affairs of the institution
  - Fails to grant access to premises and reasonable assistance to the inspector
  - Fails to allow an inspector to examine, make copies of or seize relevant documents
  - Obstructs, hinders or threatens an inspector
  - Fails to comply with a reasonable request of an inspector
  - Gives false information.
## Ambit of FIC Act inspections

<table>
<thead>
<tr>
<th>Compliance Duty</th>
<th>Section</th>
<th>Regulations</th>
<th>Directives, Guidance Notes &amp; PCCs</th>
<th>Exemptions</th>
<th>Administrative Sanction</th>
<th>Criminal Sanction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Due Diligence</td>
<td>20A, 21, 21A to 21H</td>
<td>N/A</td>
<td>GN 7</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>N/A</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>22, 22A 23 &amp; 24</td>
<td>20</td>
<td>PCC 02</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>N/A</td>
</tr>
<tr>
<td>Reporting</td>
<td>CTR 28</td>
<td>22, 22B &amp; 22C, 24</td>
<td>GN 5B</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>15 years or R100 million</td>
</tr>
<tr>
<td></td>
<td>TPR 28A</td>
<td>22, 22A, 23B, 23C, 24</td>
<td>GN 6</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td></td>
</tr>
<tr>
<td></td>
<td>STR 29</td>
<td>22, 23, 23A, 24</td>
<td>GN 4A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Management &amp; Compliance Programme</td>
<td>42</td>
<td>N/A</td>
<td>GN 7</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>N/A</td>
</tr>
<tr>
<td>Training</td>
<td>43</td>
<td>N/A</td>
<td>GN 7 &amp; PCC 18</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>N/A</td>
</tr>
<tr>
<td>Governance of AML &amp; CFT</td>
<td>42A</td>
<td>N/A</td>
<td>GN 7</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>N/A</td>
</tr>
<tr>
<td>Registration</td>
<td>43B</td>
<td>27A</td>
<td>Dir 2, PCC 5C</td>
<td>NO EXEMPTIONS</td>
<td>Natural Person = R10 million Legal Person = R50 million</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Common Inspection Findings
1. Customer due diligence not understood and applied correctly

2. Cash threshold transactions not reported or reported late
   - Dual reporting
   - Cash threshold report aggregation

3. Suspicious or unusual transactions not reported or reported late

4. Risk management and compliance programme not developed, not understood or incorrectly implemented

5. No employee training or training provided is superficial, sporadic and incomplete

6. Compliance not a board or senior management responsibility

7. Compliance officer not of sufficient competence or seniority

8. Failure to register or late registration

9. Failure to comply with Directive 4 – update registration details and activate profile on goAML
Administrative Sanctions
Sanctions

- Serious non-compliance or non-adherence to remedial directions may lead to sanctions

- Sanctions should be proportionate, effective and persuasive

- Effective sanctions should:
  - Change behavior
  - Deter non-compliance by others
  - Eliminate financial gain or benefit from non-compliance

- Sanctions in terms of the FIC Act:
  - Caution
  - Reprimand
  - Directive to take remedial action
  - Restrict or suspend certain business activities
  - Financial penalty
Sanctioning process

1. Identification of a case involving serious and extensive non-compliance
2. Notice of Intention to Sanction
3. Matter reconsidered in light of representations and mitigating factors
4. Notice of Sanction
5. 3rd Assessment – Director considers matter and sanction recommendations
6. 2nd Assessment – Director considers matter and sanction recommendations
7. Representations
8. 1st Assessment – Notice of Intention to Sanction
Administrative Sanctions

- The FIC imposed the first administrative sanction in terms of the FIC Act in March 2015
- To date, the FIC has issued in excess of 60 sanctions to the total value of approximately R42.3 million
- In the 2018/2019 financial year, the FIC issued 21 financial sanctions against non-compliant motor vehicle dealers
- To date, supervisory bodies have imposed a total of 30 sanctions on accountable institutions in excess of R244 million.
## Sanctions imposed by the FIC during 2018/2019

<table>
<thead>
<tr>
<th>ENTITY</th>
<th>SANCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Auto Group (Pty) Ltd t/a Centurion Select</td>
<td>Financial penalty – R1 170 363 with R600 000 payable immediately and R570 363 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Sandown Motor Holdings (Pty) Ltd t/a Mercedes Benz Northcliff</td>
<td>Financial penalty – R2 282 489 with R570 000 payable immediately and R1 712 489 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Luxury Tech CC t/a Right Cars</td>
<td>Financial penalty – R3 658 686 with R900 000 payable immediately and R2 758 686 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Autocare Car Sales (pty) Ltd</td>
<td>Financial penalty – R113 440 with R50 000 payable immediately and R63 440 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Hyde Park Auto (Pty) Ltd t/a Sandton Auto</td>
<td>Financial penalty – R5 244 758 with R1 300 000 payable immediately and R3 944 758 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Lemontco (Pty) Ltd t/a Eldoraigne Motors Centurion</td>
<td>Financial penalty – R5 000. Directive to remediate</td>
</tr>
<tr>
<td>Strauss &amp; Reynders CC t/a The Motor Land Group</td>
<td>Financial penalty – R359 851 with R50 000 payable immediately and R309 851 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Barons Bellville</td>
<td>Financial penalty – R191 531 with R95 756.50 payable immediately and R95 756.50 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Toyz Auto</td>
<td>Financial penalty – R239 880 with R50 000 payable immediately and R189 880 suspended for three years. Directive to remediate</td>
</tr>
</tbody>
</table>
## Sanctions imposed by the FIC during 2017/18

<table>
<thead>
<tr>
<th>ENTITY</th>
<th>SANCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspecta Car Gezina</td>
<td>Financial penalty – R503 549 with R100 000 payable immediately and R403 549 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>BB Mount Fuji Motors</td>
<td>Financial penalty – R1 131 848 with R65 924 payable immediately and R65 924 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Human Motors Bloemfontein (Pty) Ltd t/a Human Auto</td>
<td>Financial penalty – R594 152 with R100 000 payable immediately and R494 155 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Werda Toyota Louis Trichardt</td>
<td>Financial penalty – R1 052 678 with R250 000 payable immediately and R802 678 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>We Buy Cars</td>
<td>Financial penalty – R2 150 031 with R550 000 payable immediately and R1 600 031 suspended for three years. Directive to remediate</td>
</tr>
<tr>
<td>Lisabank Repossession Warehouse</td>
<td>No financial penalty. Reprimand and caution issued</td>
</tr>
<tr>
<td>Variety Motors CC</td>
<td>Financial penalty – R372 507 with R20 000 payable immediately and R352 500 suspended for three years. Directive to remediate</td>
</tr>
</tbody>
</table>
Sanctions imposed by SBs during 2018/19

<table>
<thead>
<tr>
<th>SUPERVISORY BODY</th>
<th>ENTITY</th>
<th>SANCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve Bank</td>
<td>HSBC</td>
<td>Non-compliance with Section 42: Internal rules (inadequate processes and methods to detect and report suspicious and unusual transactions). Financial penalty: R15 000 000, with R7 500 000 payable immediately and the remaining R7 500 000 suspended for a period of three years.</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Bidvest Bank</td>
<td>Non-compliance with Section 28: Filing CTRs and Section 43(a): Training on the FIC Act and accountable institutions internal rules. Financial penalty: R5 250 000</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Sikhona Forex (Pty) Ltd</td>
<td>Non-compliance with sections 21 and 22 of the FIC Act</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Sikhona Forex (Pty) Ltd</td>
<td>Caution</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Tower de Change (Pty) Ltd</td>
<td>Non-compliance with sections 21, 28 and 29 of the FIC Act</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Tower de Change (Pty) Ltd</td>
<td>Financial penalty: R280 000</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Travelex Africa foreign Exchange (Pty) Ltd</td>
<td>Non-compliance with sections 29 and 43 of the FIC Act</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>Travelex Africa foreign Exchange (Pty) Ltd</td>
<td>Reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Financial Sector Conduct Authority</td>
<td>Satrix Managers (RF) (Pty) Ltd</td>
<td>Non-compliance with: Registering; Verifying clientele; Filing CTRs</td>
</tr>
<tr>
<td>Financial Sector Conduct Authority</td>
<td>Satrix Managers (RF) (Pty) Ltd</td>
<td>Financial Penalty: R60 000</td>
</tr>
</tbody>
</table>
Payment of administrative sanctions

- Financial penalties are paid into the National Revenue Fund as administered by the National Treasury.

- An administrative sanction does not constitute a previous conviction in terms of the Criminal Procedure Act.

- The administrative sanction has to be made public unless the institution demonstrates exceptional circumstances justifying confidentiality.

- Default judgement may be obtained against an institution that fails to pay the financial penalty.
Appeals

• An institution may appeal the decision to impose an administrative sanction to the Appeal Board
• The appeal must be lodged within 30 days of receiving the Notice of Sanction
• The appellant must pay a fee of R10 000 towards the administrative costs of the appeal, which may be wholly or partly refunded if appellant successful
• Both parties are entitled to legal representation in the appeal
• The Appeal Board may:
  o Confirm, set aside or vary the sanction
  o Refer a matter back to the FIC/SB for consideration or reconsideration
• The Appeal Board cannot make any order as to costs in the appeal
• Decision of the Appeal Board may be taken on a further appeal to the High Court.
Appeal process

- Notice of Sanction
- Notice of Appeal
- FIC Answering Affidavit
- Institution's Replying Affidavit
- Heads of Argument
- Appeal Hearing & Decision
Appeal process

• The legal test on appeal – the sanction will only be interfered with if it is “startlingly inappropriate”

• To date, 10 appeals have been adjudicated by the Appeal Board
  o 7 appeals against sanctions imposed by the FIC
  o 3 appeals against sanctions imposed by the SARB

• 1 decision of the Appeal Board taken on a further appeal to the High Court on the issue of costs

• Majority of appeals were lodged against the quantum of the fine imposed.
Conclusion

“The only thing necessary for the triumph of evil is for good men to do nothing.”
~Edmund Burke~
THANK YOU
CONTACT US

www.fic.gov.za

Compliance Contact Centre
012 641 6000
THANK YOU