<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07:30 – 08:00</td>
<td>Registration</td>
</tr>
<tr>
<td>08:00 – 08:15</td>
<td>Welcome</td>
</tr>
<tr>
<td>08:15 – 09:00</td>
<td>The value of financial intelligence in supporting the criminal justice system</td>
</tr>
<tr>
<td>09:00 – 09:45</td>
<td>Risk Based Approach and the RMCP</td>
</tr>
<tr>
<td>09:45 – 10:30</td>
<td>Customer Due Diligence and Enhanced Due Diligence</td>
</tr>
<tr>
<td>10:30 – 11:00</td>
<td>Q&amp;A</td>
</tr>
<tr>
<td>11:00 – 11:30</td>
<td>Tea Break</td>
</tr>
<tr>
<td>11:30 – 12:00</td>
<td>Registration and Reporting</td>
</tr>
<tr>
<td>12:00 – 12:30</td>
<td>Supervision and Enforcement with the FIC Act</td>
</tr>
<tr>
<td>12:30 - 13:00</td>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
The Value of Financial Intelligence in Supporting the Criminal Justice System
SCOPE

- Life cycle of a Statutory Report
- Statistical overview of reporting: all scheduled entities
- Registered vs reporting entities
- Selected Reporting Categories
- Good & bad practices
- What makes a good STR
- Case Studies and Typologies
- Indicators
- Statistical Overview
SCHEDULED REPORTING ENTITIES VS STATUTORY REPORTING

- **Banks**: 0.10%
- **Rest**: 4.16%
- **Gambling**: 7.67%
- **Motor Vehicle Dealers**: 9.34%
- **Investment advisors or intermediaries**: 20.97%
- **Estate Agents**: 25.10%
- **Attorneys**: 32.65%

Total:
- **Scheduled Reporting Entities**: 84.32%
- **Statutory Reporting**: 15.68%
STATISTICAL OVERVIEW – REPORTING: ALL SCHEDULED ENTITIES

Section 28: 4,884,417 (93.65990%)
Sec 28A: 1 (0.00002%)
Section 29: 330,639 (6.34008%)

Total: 5,215,057
STATISTICAL OVERVIEW – COMPOSITION OF S 29 REPORTS

TOTAL SEC 29
330,639
6.34008%
SCHEDULED REPORTING ENTITIES VS ACTUAL REPORTERS

- Attorneys: 13,322 (32.65%)
- Estate Agents: 10,242 (25.10%)
- Investment advisors or intermediaries: 8,556 (20.97%)
- Motor Vehicle Dealers: 3,809 (9.34%)
- Gambling: 3,130 (7.67%)
REPORTING BY ATTORNEYS

- CTR: 13,322 (32.65%)
- SAR: 46 (0.05% of all reports)
- STR: 76 (0.05% of all reports)
- STRB: 0
- TFAR: 1
- TFTR: 0

Attorneys: 13,322

3,68% 490
REPORTING BY GAMBLING SECTOR

Gambling sector reporting:
- CTR: 376,989
- SAR: 448
- STR: 1,445
- STRB: 0
- TFAR: 0
- TFTR: 0

7.67% of all reports from the gambling sector

7.27% of all reports
REPORTING BY INVESTMENT ADVISORS OR INTERMEDIARIES

8,556 reports, 20.97% of all reports

- CTR: 26,462
- SAR: 371
- STR: 793
- STRB: 0
- TFAR: 0
- TFTR: 0

1,55% of all reports

Investment advisors or intermediaries
REPORTING BY MOTOR VEHICLE DEALERS

Motor Vehicle Dealers

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTR</td>
<td>37,536</td>
<td>38.38%</td>
</tr>
<tr>
<td>SAR</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>STR</td>
<td>4,394</td>
<td></td>
</tr>
<tr>
<td>STRB</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TFAR</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>TFTR</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

0.89% of all reports
## GOOD & BAD PRACTICES

<table>
<thead>
<tr>
<th>GOOD PRACTICE</th>
<th>BAD PRACTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Selection of appropriate indicators</strong></td>
<td><strong>Selection of default indicators</strong></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>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Selecting the correct report type SAR/STR/CTR</strong></th>
<th><strong>Selection of incorrect report types SAR/STR</strong></th>
</tr>
</thead>
<tbody>
<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 & 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 & 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 eg. 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. (Eg. EFT and later in the transaction cash)</td>
</tr>
</tbody>
</table>
WHAT MAKES A GOOD STR/SAR?

Provide clear and concise information.

- **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.
The Centre highlights the following case studies as examples of successes from an analysis perspective.
1) Human Trafficking - Trafficking Thai women

- The FIC was asked to assist with an investigation involving Thai women entering South Africa illegally to work in a brothel.

- The brothel, in Durban North, was allegedly disguised as a bed-and-breakfast establishment and run by a Community Policing Forum member and his wife, who is of Thai origin. Following a tip-off, law enforcement authorities raided the property and arrested the couple and 12 Thai women.

- The FIC had received several alerts linked to the key subject, where he was reported for remitting funds as “gifts” to a single recipient in Thailand. More than R4 million was sent to this person over the period. This information supports the allegations against the subject.
2) Organised Crime syndicate

- The FIC supported a law enforcement investigation between 2014 and 2017 that resulted in the successful pursuit and arrest of a **large syndicate** on charges relating to murder, attempted murder, kidnapping, VAT fraud, and cloning of stolen motor vehicles. The South African Revenue Service and the Asset Forfeiture Unit confiscated about R486 million from the syndicate.

- During this investigation the FIC analysed reports and financial transactions that led to the identification of another large **foreign syndicate** that was hydroponically cultivating **cannabis**. The syndicate was operating both domestically and internationally.

- The FIC’s analysis during 2017/2018 of financial data assisted to identify:
  - **Individuals** running hydroponic operations in the North West, Gauteng and the Free State. Four of these illicit operations were successfully disrupted and the subjects arrested. Equipment valued at about R5 million was seized.
  - **Properties** purchased with the suspected proceeds of crime in the KwaZulu-Natal South Coast region. This information helped uncover eight hydroponic cannabis laboratories in KwaZulu-Natal.

- Four foreign nationals and three South Africans were arrested. The authorities made additional arrests in Gauteng and confiscated equipment, vehicles and cannabis products to the **value of about R26 million**.
3) Theft and money laundering

- The FIC received a request regarding a subject who **allegedly stole about R460 million** from her employer over a period of eight years. She reportedly duplicated payments to legitimate clients and service providers, paying money directly into her deceased husband’s bank account.

- Through financial profiling, the FIC established that funds were going into a relative's bank account and then used **to buy luxury vehicles and several properties**. The money was also used to fund gambling activities and family holidays, and donations to family members.

- The FIC’s analysis of the husband’s bank statements revealed funds paid to **an insurance company in large monthly instalments** and, at times, frequent payments during the month too. It was established that the premiums were paid with the stolen proceeds of crime.

- The FIC issued a **directive in terms of Section 34 of the FIC Act** to prevent the subject from accessing these investment products which represented the proceeds of crime, to the value of about R21 million. The subject was subsequently arrested and the Asset Forfeiture Unit proceeded to attach or preserve several assets worth millions under the Prevention of Organised Crime Act.
4) Foreign nationals drug bust

• The FIC assisted a law enforcement agency in a significant narcotics seizure to the value of about R500 million. Financial intelligence established that the foreign nationals under investigation had significant interests in several business entities in South Africa. Some of these entities owned a number of motor vehicles used for a car hire business, while another owned and sold motor cycles.

• The FIC established that these foreign nationals were using their personal and business entity accounts to facilitate the smuggling of drugs out of South Africa. Their accounts showed significant transactional activity that indicated the co-mingling of money derived from lawful activities with funds derived from unlawful activities (known as money laundering).
5) Cracking a cryptocurrency - Ponzi scheme

• The FIC identified what appeared to be an alleged Ponzi scheme run by an individual marketing a “new cryptocurrency”. This product was marketed as Africa’s first cryptocurrency and investors were promised huge returns on their investments.

• The FIC’s analysis of the individual’s bank statements revealed that there was **no cryptocurrency** and that this was indeed a Ponzi scheme.

• A restraining order was issued for more than R2.8 million in proceeds from the alleged scheme, and the FIC assisted the Asset Forfeiture Unit in obtaining a preservation order relating to **fixed property and vehicles worth more than R4 million** that was bought using the proceeds of the scheme.
6) Cyber fraud – crypto currency

- The FIC received an alert from a **neighbouring jurisdiction** that a person was defrauded of a large amount of money that was transferred to a South Africa financial institution. Some funds were transferred to a cryptocurrency exchange and converted into a **basket of cryptocurrencies**, including Bitcoin. Some funds were irrecoverable because they were transferred to other cryptocurrency exchanges in foreign jurisdictions.

- The FIC froze some of the **virtual currency** (Bitcoin, Bitcoin Cash and Ripple) held with the cryptocurrency exchange using a Section 34 directive. It also provided an affidavit that led to the Asset Forfeiture Unit obtaining a preservation order from the High Court in Johannesburg.

- To note:
  - Both addresses traced to BITTREX – exchange based in USA, Las Vegas
  - In 24 hours – R500,000.00 moved through 3 countries!
7) Fraud and money laundering

The Centre assisted the Asset Forfeiture Unit to trace the flow of funds and assets linked to the financial officer of a construction company who defrauded her employer to the value of R4 million.

Outcome

Through analysis we identified the investment accounts that held the proceeds of crime and we issued section 34 interventions blocking R384,854.70. In addition 6 vehicles including a caravan with an aggregate value of R1,899,487.39 were identified.

The Centre issued an affidavit to support a section 38 POCA Preservation order obtained by the AFU.

The suspect was arrested for fraud and ML.
8) Cash-In-Transit heist

• The FIC assisted law enforcement in an **armed robbery** matter with the analysis of financial information and the possible identification of proceeds of illegal activities. The intelligence gathered from the various banks and the provision of related account opening documents, copies of proof of employment and bank records for a six (6) month period prior to the robbery directly contributed to the analyses and the identification of the proceeds of illegal activities being deposited into the bank accounts.

• The analysis revealed that:
  • Accounts belonging to the syndicate, their family members and girlfriends were reflecting very low balances before the date of the robbery.
  • On the day of the robbery and the days shortly thereafter the accounts suddenly started reflecting unusual cash deposits by means of ATM deposits and in branch teller deposits.
  • The purchase of a vehicle in the name of one of the suspect’s parents.

• The FIC was able to authorise five (5) different section 34 interventions, and provided the necessary support which led to the successful granting of preservation orders against the funds in bank accounts and the motor vehicle.

• Cash was recovered from the proceeds of the armed robbery and the **vehicle** which was purchased.
1. High end **vehicle purchases** that are seemingly not in line with the expected income of the customer.

2. Concealment/misuse within **Business** structures

3. Illogical business **activity** - why do multiple transfers at a higher charge

4. Multiple **transactions** in a short time period with no underlying business rationale

5. Use of **False** Identities and documents / **Missing** documentation normally to be expected from a legitimate business

6. Purchasing of property in **family** members’ names.

7. Purchasing of valuable **commodities** / **extreme luxury goods**, normally associated with extremely wealthy persons (Brand Name Boutique Clothing, expensive watches and expensive electronic goods etc.)

8. Gambling activities - significant year on year **increase** in turnover / not in line with the expected income of the customer.

9. Declared Source of Income **not aligning** to activity of the customer /exceeds the expected deposits for the customer.
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)

Referrals of information to Law Enforcement Agencies (2014-2018)
Suspected proceeds of crime frozen 2014-2018

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>Millions in Rands</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2014/2015</td>
<td>2296.7</td>
</tr>
<tr>
<td>FY 2015/2016</td>
<td>477.6</td>
</tr>
<tr>
<td>FY 2016/2017</td>
<td>443.9</td>
</tr>
<tr>
<td>FY 2017/2018</td>
<td>3027.9</td>
</tr>
</tbody>
</table>

Section 34 freezing of accounts

Proceeds of crime recovered using FinInt
Conclusion

- Institutions have made an unprecedented level of investment in both people and IT. They now have significant and largely untapped expertise and financial intelligence of huge value in money laundering and terrorist financing investigations.

- Sharing of analytical information and skills (Artificial Intelligence) around clients/accounts.

- Crypto assets – By recognising that innovative financial technologies, products and services may offer significant economic opportunities but also present a risk of being misused, including for terrorist financing.

- Focus on quality referrals to agencies and for feedback on matters to measure impact.

- Stakeholders (LEAs) will be kept accountable – for feedback on matters (Impact of the FIC)
THANK YOU
Risk-based approach and the risk management and compliance programme
Risk-based approach

- What is risk
- What is required of an accountable institution in terms of the risk-based approach?

Unpacking the risk management and compliance programme
Risk-based approach

- Amendments to FIC Act resulted in paradigm shift

<table>
<thead>
<tr>
<th>Rules based</th>
<th>Risk based</th>
</tr>
</thead>
<tbody>
<tr>
<td>“old”</td>
<td>“new”</td>
</tr>
<tr>
<td>• Prescriptive</td>
<td>• Risk to AI is fundamental in application</td>
</tr>
<tr>
<td>• Narrow/strict interpretation of requirements</td>
<td>• Ownership in understanding AML risk</td>
</tr>
<tr>
<td>• Minimal ownership of AML understanding by AIs</td>
<td>• Focus on higher risk areas</td>
</tr>
<tr>
<td>• Tick box approach applied</td>
<td>• Compliance requirements met more efficiently and cost effectively</td>
</tr>
</tbody>
</table>
What is risk?

- Likelihood and impact of uncertain events on set objectives.

  *International best practice rating methodology*

- Uncertainty is a function of
  
  - Threats – potential to cause harm
  - Vulnerability – things that can be exploited by threats
  - Consequence – impact of threat/exploitation
Which risks are we talking about?

Money Laundering risk

Money Laundering

- Proceeds of crime
- Placement, layering, integration
- Proceeds no longer associated with underlying criminal activity
- Proceeds appear legitimate
### Terrorist Financing

- Solicitation, collection and providing funds and assets with intention to be used to support terrorist acts, terrorist organisations and individual terrorists
- Illegal and legal sources
- Goal – to conceal financing and nature of activity being financed
Unpacking money laundering and terror financing risks

- These are threats and vulnerabilities which put accountable institutions at risk of being abused in order to facilitate money laundering and terror financing activities
- Potential that clients may use products and services offered by the accountable institution for money laundering and terror financing purposes
  - Launder proceeds
  - Blur detection, investigation or prosecution of money laundering
- Applying a risk-based approach ensures that AIs are able to ensure that measures to prevent money laundering and terror financing are in proportion with the risks identified
Risk-based approach – risk management

- Identification of risk
- Assess the risk
- Methods to manage the risk
Factors to take into account when identifying risks

### Risk-based approach

- **Identification of risk**

### Products and services
- Third party payments
- Cash / EFT
- Cross border flow of money
- Duration of relationship/transaction
- Same name payments?

### Delivery Channels
- Direct relationship
- Working through intermediary
- Face to face or non-face to face

### Geographic location
- SA / foreign jurisdiction
- High risk countries
- Client confidentiality in foreign jurisdiction
- Week regulatory oversight

### Clients
- Natural / Legal person
- Complex structures
- PEP / PIP
- Adverse information
- ML findings
- Transactional pattern

### Other factors
- ML approach
- Strategy of entity
- Regulatory fines in similar industries
- Learnings / typologies
• Assessment of risk

- Review of the identified risk, applicable indicators and the interaction with different types of clients
- Understand the impact of the indicators
• Assessment of risk

• Risk rating, by assigning categories to different levels of risk
  o High/Medium/Low risk

• No “one size fits all” approach

• Risk rating may change, re-evaluation of risk rating is critical

• Smaller AI’s – simplistic risk scale

• Complex structures with multiple indicators – more sophisticated risk scale
Risk-based approach

• Methods to manage risk

Treating the risk

• Risk mitigation – entails control measures, systems and minimising the money laundering and terror financing risk
• Align money laundering and terror financing controls (measures) accordingly
• Systems and controls to accommodate:
  o Higher risk- enhanced controls required
  o Lower risk- lighter controls required.
Mechanisms to manage risk

- Systems, policies and procedures
- Awareness training
- Reporting
- Client and transaction analytics
- Process to exit high risk relationships
- Approval for high risk transactions and relationships
- Screening tools
Risk-based approach

Inherent Risk

Risk mitigation - treatment of risk

- Treatment of risk = systems and controls developed to manage the identified money laundering and terror financing risks i.e. clients and products

- Risk will be adequately treated = level of residual risk is acceptable & within the risk appetite of the accountable institution

Practical treatment:

- Apply RBA when carrying out customer due diligence measures in respect identified money laundering and terror financing risks

- Higher money laundering/terror financing risk – more stringent due diligence

- Lower money laundering/terror financing risk – “lighter touch”
Risk management and compliance programme

**WHO**
- All Accountable Institutions
- Approved by, and responsible party are the board of directors

**WHAT**
- Policy, procedures, systems and controls for money laundering risk-based approach

**WHEN**
- Current, and ongoing reviews

**WHERE**
- All subsidiaries within the AI space
- International application as the minimum standard

**WHY**
- To understand money laundering and terror financing risk facing the entity, and to allocate the appropriate time and resources
Unpacking the RMCP

Risk management and compliance programme

Risk identification
Customer Due Diligence
Transactional monitoring
Record keeping
Reporting to the FIC
Extended registration model of entity
Implementation of RMCP
The risks that the products or services may involve or facilitate money laundering must be:

- Identified
- Accessed
- Monitored
- Mitigated
- Managed
Customer Due Diligence

- Identification if prospective client, or client who has established a relationship / once-off transaction
- Provisions relating to not dealing with anonymous and fictitious clients – section 20A
- Establishment and verification of client identification (CDD / KYC / “FICA”) – section 21
- Additional due diligence for legal persons, trusts and partnerships
- Ongoing due diligence
- Process when there are doubts about information or documentation received (veracity)
- Process to exit a relationship when customer due diligence cannot be conducted
Risk management and compliance programme

- How to determine if a client is a foreign prominent public official or domestic prominent influential person (politically exposed person or politically influential person)
- Process for enhanced due diligence for high risk clients
- Evidence how customer due diligence is linked to risk (low risk application vs high risk application)
Manner in which future transactions will be consistent with knowledge of client

Examination and records of

- Complex/unusually large transactions
- Unusual patterns that have no apparent business or lawful process
Customer due diligence and transactional information obtained – how and where will these records be kept?

- Who will have access to these records
- Measures in place to safeguard the records
- 3rd party storage?
- Electronic vs manual record keeping
- How long will the records be kept (i.e. 5 years)
Reporting to the FIC

- When is a transaction or activity reportable to the FIC
  - Suspicious or unusual transactions (STR)
  - Cash Threshold (CTR)
  - Terrorist Property and Target Financial Sanctions (TPR)
  - International Fund Transfer (IFTR)
- Timing of reporting (to tie in with provisions of FIC Act)
- Manner of reporting (i.e. goAML, user access etc.)
When an entity has branches, subsidiaries or other operations in foreign countries

Does the host country of the foreign branch permits FIC Act obligations or measures

Advise the FIC accordingly

South African requirements remain the minimum requirement (i.e. if in another country and if they have a lower standard than South Africa)
Implementation of RMCP

- Process for implementing the risk management and compliance programme
  - Role definition in terms of application
  - Clear approval by senior management/board
  - Process to review and update risk management and compliance programme
  - Training on risk management and compliance programme.
THANK YOU
Customer due diligence and enhanced due diligence
Customer due diligence measures

- Risk-based approach
- FIC Amendment Act
- Record keeping

Customer due diligence measures

- Natural persons
- Legal persons - beneficial ownership
- Foreign prominent public officials
- Domestic prominent influential persons
Customer due diligence measures

Customer due diligence

• Customer due diligence process assists AI to:
  o Know who they are doing business with
  o Know who benefits from the business it does with the client
  o Understand the nature of the business it does with a client

• Determine when a transaction during that business relationship is considered suspicious or unusual

• Customer due diligence expands client identification and verification

• Risk-based approach allows for more flexibility to exercise judgement in determining the extent and nature of the information required for customer due diligence

• The findings of the risk assessment will determine the level and type of customer due diligence that will be applied
Anonymous clients and single transaction threshold

No anonymous clients

- AIs may not do business with an anonymous client or a client with apparent false or fictitious name

Single transaction threshold

- Value of the transaction is determined by the Minister
- No requirement to carry out full customer due diligence
- Should obtain and record some information about the client
Establishing the identity of the client

- Customer due diligence begins with an AI knowing the identity of its client.
- Establishing the client’s identity requires obtaining a range of information about the client.
- Obtained from the client during the take on stage or part of the client engagement process.
- Verification of the client’s identity is the corroboration of the information by comparing it against the original source or reliable third party.
- 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 risk management and compliance programme.
- Verification must occur during the course of conducting the single transaction/business relationship but must complete the verification before it concludes a transaction.
## Establishing the identity of clients - natural persons

<table>
<thead>
<tr>
<th>IDENTIFICATION</th>
<th>VERIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic level</strong></td>
<td>• Verification methods may vary</td>
</tr>
<tr>
<td>• Full names</td>
<td>• Verification with information obtained from a reliable and independent third party source</td>
</tr>
<tr>
<td>• Date of birth</td>
<td>• As far as possible the original source of the information</td>
</tr>
<tr>
<td>• Identifying number issued by government</td>
<td></td>
</tr>
</tbody>
</table>

**Supplementary information**  
• Biometric information  
• Place of employment or business  
• Residential address  
• Contact particulars  
• Tax number
Establishing the identity of clients - natural persons

Examples of government issued or controlled sources of information:

- South African identity documents including smart card identity documents
- Valid driver’s licence
- Foreign identity documents
- Passports
- Asylum seeker or refugee permits
- Work permits
- Visitor's visas
Understanding the business relationship

• Accountable institutions are required to obtain additional information at the customer due diligence stage of the business relationship including:
  o Purpose and intended nature of the business relationship
  o Source of funds to be used in business relationship
• The information should be sufficient to understand the client and the business relationship
Ongoing due diligence

- Scrutiny of transactions undertaken throughout the business relationship
- Ensure transactions are consistent with knowledge of the client and client’s business and risk profile
- Pay attention to unusual patterns of transactions or unusually large or complex transactions
- Ensure client information is accurate and relevant
- Frequency and intensity of ongoing due diligence based on money laundering or terror financing risks associated with business relationship with client
- Ongoing due diligence processes detailed in risk management and compliance programme
Doubts about veracity of previously obtained information

- AIs are required to take certain measures
  - If there are doubts about the veracity of previously obtained customer due diligence information
  - Suspects an activity is suspicious and unusual

- Risk management and compliance programme must set out the manner and process to confirm the customer due diligence information when it has doubts about veracity of previously obtained information
Inability to conduct due diligence

- Prohibits AI from entering into or maintaining business relationship or concluding single transaction if it cannot perform customer due diligence
- If circumstances that prevents customer due diligence are suspicious or unusual – consider report in terms of section 29
- Risk management and compliance programme should indicate the sequence of attempts to obtain the required information as well as when verification must be completed and at which point the conclusion is reached that the information is not forthcoming and is therefore unable to conduct customer due diligence
- Risk management and compliance programme should also provide for the manner in which it will terminate an existing business relationship when unable to complete customer due diligence requirements
Foreign and domestic prominent persons

- AI must know who their clients are and understand their client’s business.
- Business with foreign prominent public officials must always be considered high risk.
- Business with domestic prominent influential persons are not inherently high risk.
- Being a prominent person does not create a presumption of being guilty of any crime and does not mean that an AI cannot transact with such a person.
- AIs will have to include the management of business relations with person in prominent positions in their risk management and compliance programme.
Domestic prominent influential persons includes:

- 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, FSB, NGB, EAAB, etc.
- Judges
- Senior officials of companies who receive certain tenders from government

Includes family members and known close associates
Foreign prominent persons

Foreign prominent public officials includes:

- 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
Foreign and domestic prominent persons

Where relationship with domestic prominent person poses a high risk OR dealing with a foreign prominent public official:

• AIs must do the following:
  
  o Obtain senior management approval
  
  o Establish source of wealth and source of funds
  
  o Monitor the business relationship

• Monitoring the relationship means that close attention is paid to the manner in which the client uses the institution’s services and products
Corporate vehicles identification and verification - additional due diligence measures applied

- Nature of client’s business
- Ownership and control structure
- Beneficial ownership

Corporate vehicles
Legal persons
Trusts
Partnerships
Legal persons, partnerships and trusts

In addition to verifying the identities of the clients which are not natural persons, AI’s need to:

• Understand the nature of its business
• Understand its ownership and control structure
• Know who the natural persons are
• Who ultimately owns or control their clients
Legal persons

Definition

A legal person is defined in the FIC Act as any person, other than a natural person that establishes a business relationship or enters into a single transaction with an AI table institution and includes:

• A person incorporated as a company
• Close corporation
• Foreign company
• Or any other form of corporate arrangement or association but excludes a trust, partnership or sole proprietor.
### Legal persons

#### Characteristics which describes identity of legal person

- Name and trading name
- Form
- Registration number
- Address of registered office/business address if different
- Powers
- directors
- Senior management
- Tax numbers

#### Verification

- AI to decide on degree and methods of verification based on money laundering or terror financing risk
- Methods may vary
- Verification with information obtained from a reliable and independent third-party source
- As far as possible the original source of the information
Beneficial ownership

Beneficial ownership requirements

• AIs are required to establish who the beneficial owner of the legal person is and take reasonable steps to verify the beneficial owner’s identity.

Beneficial ownership?

• Beneficial ownership refers to the natural person(s) who owns or exercises effective control over the legal person

Application

• Beneficial ownership applies to legal persons, partnerships and trusts.
Beneficial ownership

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:
  o The identity of known or suspected criminals
  o The true purpose of an account or property held by the legal entity
  o The source or use of funds or property associated with the legal entity

• The establishment of beneficial ownership is important for two reasons:
  o Understand the customer profile to properly assess the money laundering or terror financing risks associated with the business relationship
  o Take appropriate steps to mitigate the risks
Beneficial ownership

Ownership and control structure – who is the beneficial owner?

Beneficial Owner

- Natural person (warm body)
- Owns/exercises effective control of the legal person
- Independently or together with another person

Verification of beneficial owner

- Methods may vary
- Verification with information obtained from a reliable and independent third-party source
- As far as possible the original source of the information
- Process detailed in risk management and compliance programme
Beneficial owner elimination process – legal person

Step 1: Who is the main shareholder or voter
- The percentage of shareholding with voting rights = good indicator
- Ownership of 25% or more of shares/voting rights = good indicator

Step 2: Who is natural person who exercises control through other means
- e.g. through voting rights attaching to classes of shares or through shareholder

Step 3: If no natural person can be identified - management
- AI must determine who = natural person who exercises control over the management of the legal person
Partnerships

**Identification**
- Name – how partnership is known
- Partners

**Executive control - partnership**
- Section 21B(3)
- Identity of such a person
- Identity of each natural person authorized to enter into single transaction or business relationship on behalf of partnership

**Verification**
- Reasonable steps
- Based on money laundering or terror financing risk
- Partnership agreement
- Verification measures documented in RMCP

**Verification**
- Reasonable steps to verify
- Based on money laundering or terror financing risk
- Verification measures documented in risk management and compliance programme
Trusts

Identification
- Name – unique name or description
- Registered with Master of High Court – unique reference number and address where trust registered

Beneficial Owner – Trust
- Section 21B(4)
- Identity of founder
- Identity of trustee and each natural person authorised to enter into single transaction or business relationship on behalf of trust
- Identity of named beneficiaries
- Particulars of how beneficiaries are determined

Verification
- Reasonable steps to verify
- Based on money laundering or terror financing risk
- Trust deed
- Verification measures documented in risk management and compliance programme
THANK YOU
Questions and discussion
TEA BREAK

30 minutes
Registration and Reporting Feedback
AGENDA

• Registration – updating entity/user details
• Reporting to the FIC – reports that can be submitted
• Updated business rules and the regulations
• Access to regulatory reporting information by SBs
• Supervisory bodies and their schedule items
• What can go wrong
• General reporting feedback and recommendations
• General feedback relating to the completeness of regulatory reports
• Background and reference documents
Updating Entity Details (Directive 1 & Directive 4)

- The compliance officer/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 or unusual transaction report (STR)**
  - Section 29
    - Suspicious or 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)
    - AIs only
Updated business rules and regulations

• The Money Laundering and Terrorist Financing Control Regulations (the 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)

• The FIC has published updated reporting user guides along with tutorial videos (see YouTube) and all AI/RIs are encouraged to utilise these materials during **staff training** and **awareness sessions**
Updated business rules and regulations

The following amendments were made to the goAML business rules in December 2017

- When reporting your client the client’s identification 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)
- 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”
- AI/RIs need to complete the reporting form with all readily available information. Avoid only completing system mandatory fields or selecting “Not Obtained” when information is known, or should be known
- The reporting forms allows for the selection of “Not Obtained” in certain client information fields (e.g. Address and Telephone Number). This allows for the successful submission of reports with all mandatory fields completed in the case where a customer was deemed to be low risk and such information was not obtained
- In the event that a mandatory field does not have a list with “Not Obtained” pre-populated, the AI/RI will have to insert “Not Obtained” when applicable
Access to regulatory reporting information by SBs

- Amendments to the FIC Act section 45B(2A) allow supervisory bodies (SBs) to request and view information directly from their supervised industry whilst they are conducting a FIC Act inspection.
- This includes facts and information relating to regulatory reports submitted to the FIC i.t.o. sections 28, 28A and 29 of the FIC Act (previously only sections 28 and 28A reports could be viewed).
- The FIC will independently verify information industry provides to their SBs in order to provide assurance and/or confirmation that the information or content disclosed, corresponds with that reported to the FIC.
- AI/RIs are advised to have adequate record management processes in place. The FIC recommends that AI/RIs keep copies of all submitted regulatory reports, messages (report receipts and request for information) on their internal systems to enable them to provide such information timeously to the SBs.
What can go wrong?

A review of the Directive 3 (failure to report) issues reported for 2017/2018 financial year found that reporting failures are normally attributed to the following root causes:

<table>
<thead>
<tr>
<th>Missed products lines and services</th>
<th>Incorrect or incomplete capturing of regulatory reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect aggregation and detection of cash threshold transactions in terms of section 28 of the FIC Act</td>
<td>Deficiencies in compliance governance</td>
</tr>
</tbody>
</table>
Pre-validation and post submission quality reviews

- The FIC notes multiple instances or re-occurrences whereby regulatory reports are submitted that fail the schema specifications and business rules, or do not adhere to the regulations.

- Pre-validation should include a multi-disciplinary team, including users from the ICT, business and compliance units.

- Such pre-validation reviews should cover both (a.) the technical system / reporting requirements (when reporting is automated), along with reviews pertaining to (b.) the completeness / correctness of client information and transactions data as specified in the regulations.

- Post submission quality reviews should be conducted on an ongoing basis to ensure that the AI/RI has assurance that (a.) submitted reports have indeed been processed/accepted, and the client information and transactional data reported (b.) meets the requirements outlined in the regulations, and (c.) indeed correlates with the information held by the AI/RI.
General reporting feedback and recommendations

• 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)

• AI/RIs should revisit their transaction scenarios as FIC notes that many reports list the client (e.g. person or entity) on both the sender/payer and receiver/beneficiary side of a transaction. Normal scenarios for AI/RIs would require that the client (i.e. person or entity) be on one side and the AI/RI or its account (i.e. entity or account) on the other. When funds are transferred between accounts the scenario should reflect account to account

• AI/RIs are submitting multiple notices relating to incorrect and over/under reporting of transactions to the FIC. It is the FIC’s expectation that AI/RIs apply adequate internal controls and address these internal deficiencies to avoid multiple reoccurrence of the same reporting failures.
General feedback relating to the completeness of regulatory reports

• AI/RIs need to ensure that the regulations are understood by all users and that the information or data is available to end users to capture on the applicable reporting forms

• Client information that needs to be captured on the reporting forms directly relates to the client identification and verification information obtained (in terms of section 21 of the FIC Act) and would therefore be different for natural persons, companies (includes director information) etc.

• AI/RIs are reminded that client information and transactional data must be captured in a uniform manner - this will be best achieved by setting up defined processes, reporting scenarios and master templates (e.g. for CTRs, CTRAs, STRs & SARs)

• AI/RIs must avoid practices whereby transactions or a series of transactions are summarised. The applicable transactions must be listed separately on the reporting forms to avoid creating a skewed, inaccurate and/or incomplete view of what has indeed transpired.
Accountable Institutions need to note the following:

- AIs need to conduct **ongoing screening** of clients against **UN1267 = i.e. client onboarding and existing clients**

- **Client screening** should be concluded **before accepting funds** into the entity’s account, and/or concluding a transaction with a prospective client

- AIs need to screen clients at **set / predefined intervals** which should be documented in the RMCP

- FIC has **provided a link** to the UN1267 list on the FIC’s website ([www.fic.gov.za](http://www.fic.gov.za))

- The list is available in PDF, XML and HTML format (note that this list is **updated** and must be monitored on an **ongoing basis**)

- Alternatively the AI may utilise the services of a third party system for its sanction and watch list screening of clients (normally offered as paid subscription services and software)
General recommendations when filing a report i.t.o. 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 (i.e. when an inspection is conducted)
- 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 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 filling = why do you feel uneasy or find it unusual?)
- What (what caused you to submit the report = what was the indicators/ 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/ 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:**

- Always ensure that you provide a detailed narrative that outlines the above in a **chronological order** - do not summarise information (i.e. transactions or involved parties) or use acronyms that are not commonly used.
- When reporting an account = provide the **balance of the account** and clearly indicate whether the account is still **open and active**?
- When reporting an asset = provide a **description** of the asset and advise who is in control thereof?
- Attach all available **supporting documents** with the original report = this enables the FIC to see the entire picture from the onset.
- In the event that a report i.t.o. section 29 of the FIC Act was identified but ultimately not reported- the decision and all documentation relating thereto must be kept by the AI/RI.
## Activity Reports

### Activity Report Structure:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Report Type</strong></td>
<td>The type of report (i.e. SAR, TFAR or TPR)</td>
</tr>
<tr>
<td><strong>2. Reporting Person</strong></td>
<td>Linked to the logged in user details, this is the person <strong>uploading</strong> the regulatory report</td>
</tr>
<tr>
<td><strong>3. Location</strong></td>
<td>Describes the actual geographical area / branch where the proposed, cancelled or attempted transaction or series of transaction or suspicious and unusual activity occurred (when reporting <strong>SAR &amp; TFAR</strong>) <strong>OR</strong> Describes the actual geographical area / branch where the transaction or series of transactions occurred (<strong>TPR</strong>)</td>
</tr>
<tr>
<td><strong>4. Indicators</strong></td>
<td>In relation to SAR/TFAR indicators are used to specify the nature or type of suspicious or unusual activity that the institution is reporting to the FIC. <strong>OR</strong> An indicator in relation to TPR means the type of report submission</td>
</tr>
</tbody>
</table>
| **5. Activity** | • **Report Parties** = Person / Entity / Account  
• **Goods and Services** = this information is required to further describe the physical assets that are linked to the report submitted |
Activity Reports

Report Layout

1. Report Type
2. Reason for Reporting - NB for SAR, TFAR & TPR (applies to transaction reports as well)
3. Action - NB for SAR & TFAR
4. Reporting Person
5. Location
6. Indicators
7. Activity
Activity Reports

Report Layout (Continued)

7. Activity
   a) Report Parties
   b) Goods and Services

<table>
<thead>
<tr>
<th>Report Parties *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person / Account / Entity</td>
</tr>
<tr>
<td>Person</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Goods and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item Type</td>
</tr>
<tr>
<td>Property</td>
</tr>
</tbody>
</table>
### Transaction Report Structure:

<table>
<thead>
<tr>
<th>1. Report Type</th>
<th>The type of report (i.e. CTR, CTRA, STR &amp; TFTR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Reporting Person</td>
<td>Linked to the logged in user details, this is the person uploading the regulatory report</td>
</tr>
<tr>
<td>3. Location</td>
<td>Describes the actual geographical area / branch where the transaction, series of transactions or reportable event occurred</td>
</tr>
<tr>
<td>4. Indicators</td>
<td>An indicator in relation to CTR/CTRA means the type of report submission. OR In relation to STR/TFTR indicators are used to specify the nature or type of suspicious or unusual transactions, series of transactions or reportable event that the institution is reporting to the FIC</td>
</tr>
</tbody>
</table>
| 5. Transactions | • From Type = Person / Entity / Account  
• To Type = Person / Entity / Account  
• Goods and Services = this information is required to further describe the physical assets that are linked to the report submitted |

1. Report Type
2. Reporting Person
3. Location
4. Indicators
5. Transactions:
   5.1 From Type
   5.2 To Type
   5.3 Goods and Services
### Transaction Reports

**Report Layout**

1. Report Type
2. Reporting Person
3. Location
4. Indicators
5. Transactions

<table>
<thead>
<tr>
<th>Report Type: CTR</th>
<th>ID: 3559698-0-0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entity</strong></td>
<td>ABC Estate Agents- RI/0010100001</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Cash Threshold Report (CTR)</td>
</tr>
<tr>
<td><strong>Submission Date</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Reporting Entity Branch</strong></td>
<td>Centurion</td>
</tr>
<tr>
<td><strong>Reporting Entity Reference</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FIC Ref Number</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Reporting Person**

- **First Name**: Mtumile
- **Surname/Last Name**: Ndizma
- **Birth Date**: 1990/07/26
- **RSA ID Number**: 9007263637083

**Location**

- **Address**: Homes Park Office Suite 10B, Number 25 Baker Street
- **City**: Centurion
- **Province/State**: Gauteng
- **Postal/Zip**: 0157
- **Country**: SOUTH AFRICA

**Indicators**

- **Indicator**: Cash Threshold Report (CTR) in terms of Section 26 of the FIC Act 26 of 2001 where the report contains unrelated transactions whereby each transaction on its own has exceeded the threshold and no aggregation is demonstrated

**Transactions**

<table>
<thead>
<tr>
<th>#</th>
<th>Number</th>
<th>Date</th>
<th>Local Amount</th>
<th>Transmode Code</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TRW-171112-0000001</td>
<td>2017/11/09</td>
<td>24999.99</td>
<td>Cash (received by AI/RI)</td>
<td>Complete</td>
</tr>
</tbody>
</table>
5. Transaction
   a) From Type
   b) To Type
   c) Goods and Services
goAML web reporting tips

- Clear your browsing history frequently and always open goAML from the FIC website (www.fic.gov.za) instead of saving it as a favourites or as a bookmark.

- Ensure that your internet browser allows pop-ups and that the compatibility view is enabled.

- Always ensure that web reports are saved whilst completing multiple sections/transactions and prior to submitting it on goAML Web.

- Available attachments (e.g. copy of ID or passport, contract or deposit slip) may be uploaded and submitted with the initial report submitted to the FIC.

- Download copies of all submitted regulatory reports (web and batch) along with the report receipts and save on the AI’s internal systems for record keeping purposes.

- Web reports must be remediated as per the defined process whereby it is reverted back to draft status, edited, fixed and resubmitted- please do not submit a new report as it creates duplicates and the original rejected report remains unresolved.

- Always report any goAML incidents/queries to the FIC immediately by means of the formal channels.
Background and reference documents

Documents are available on the FIC website (www.fic.gov.za) 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 04A (STRs/SARs/TFTRs/TFARs in terms of section 29 of the FIC Act)
- Guidance Note 05B (CTRs/CTRA in terms of section 28 of the FIC Act)
- Guidance Note 06 (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)
THANK YOU
Supervision and Enforcement
The FIC Act supervision and enforcement model

1. 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).

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

3. 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>
New tripartite supervisory model

FSCA

FIC

SARB
# New 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>• 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></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>
</tbody>
</table>
FIC supervisory model

- Enforcement
- Inspections
- Compliance Monitoring
- Public Compliance Communications & Guidance Notes
- Public Awareness & 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.
<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></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CTR</td>
<td>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>TPR</td>
<td>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>STR</td>
<td>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>
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. 1st Assessment – Notice of Intention to Sanction
3. Representations
4. Notice of Sanction
5. 2nd Assessment – Matter reconsidered in light of representations and mitigating factors
6. 3rd Assessment – Director considers matter and sanction recommendations
Administrative Sanctions

- Between 2010 and 2015, the FIC allowed industries a grace period to understand and implement the provisions of the FIC Act

- The FIC imposed the first administrative sanction in terms of the FIC Act in March 2015

- To date, the FIC has issued a total of 45 sanctions and in excess of R2.3 million

- In the 2017/18 financial year, the FIC issued 18 financial sanctions against non-compliant institutions:
  - 13 against motor vehicle dealers
  - 5 against Kruger rand dealers

- Supervisory bodies have imposed a total of 24 sanctions on accountable institutions and in excess of R224 million.
### Sanctions imposed by the FIC during 2017/18

<table>
<thead>
<tr>
<th>ENTITY</th>
<th>SANCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scoin Trading (Pty) Ltd t/a The South African Gold Coin Exchange</td>
<td>R176 060 caution, reprimand and directive to take remedial action</td>
</tr>
<tr>
<td>Henque 1881 CC t/a Henque Motors</td>
<td>R15 275 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Mr Kruger East Holdings – Moreleta Park</td>
<td>R30 531 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>3DNA Architecture and Design t/a Gold Buyers</td>
<td>R49 288 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Arthlene Ondernemings CC t/a Auto Unique</td>
<td>R68 659 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Bidvest McCarthy (Pty) Ltd t/a Chrysler Jeep Dodge - Centurion</td>
<td>R288 663 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Tom Campher Motors</td>
<td>R60 100 Caution, reprimand and directive to take remedial action</td>
</tr>
<tr>
<td>Abilia Trading t/a Gold Vault</td>
<td>R5 000 fully suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>We Buy Cars</td>
<td>R2 150 031 R1 600 031 suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>ENTITY</td>
<td>SANCTION</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Auto 1 Automotive t/a Nissan Uitenhage</td>
<td>R93 060 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Global Autohaus</td>
<td>R349 091 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Peng Investments (Pty) Ltd t/a Leo Haese</td>
<td>R415 530 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Tadocube (Pty) Ltd t/a Jaguar Land Rover Hillcrest</td>
<td>R556 723 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Gold Traders Mossel Bay</td>
<td>R13 120 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>European Automotive Imports (Pty) Ltd t/a Maserati</td>
<td>R176 000 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Mystic Cars (Pty) Ltd</td>
<td>R180 000 R120 000 suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>Nissan Mthatha</td>
<td>R60 000 50% suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
<tr>
<td>SMG Auto Cape Town (Pty) Ltd</td>
<td>R1 600 000 R1 200 000 suspended, caution, reprimand and a directive to take remedial action</td>
</tr>
</tbody>
</table>
### Sanctions imposed by SBs during 2017/18

<table>
<thead>
<tr>
<th>SUPERVISORY BODY</th>
<th>ENTITY</th>
<th>SANCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve Bank</td>
<td>Sikhona Forex</td>
<td>R130 000 reprimand and directive to take remedial action</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>China Construction Bank</td>
<td>R75 million R20 million suspended for 1 year, reprimand and directive to take remedial action</td>
</tr>
<tr>
<td>Reserve Bank</td>
<td>VBS Bank</td>
<td>R2.5 million R2 million suspended for 1 year, reprimand and directive to take remedial action</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 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.
"The only thing necessary for the triumph of evil is for good men to do nothing."

~Edmund Burke~
THANK YOU
Questions and discussion
www.fic.gov.za

Compliance Contact Centre
012 641 6000