Reinforcing the integrity, stability and transparency of South Africa’s financial system
FROM THE DIRECTOR’S OVERVIEW

The FIC’s role in protecting the financial system’s stability and integrity

South Africa’s framework for anti-money laundering and countering the financing of terrorism is designed to assist in making the financial system intolerant to being abused by criminals. These fundamentals underpin the integrity and stability of the financial sector and in turn, contribute to the safety and security of all South Africans. A stable and secure financial system promotes confidence, helping to attract investment from here and abroad. Such investment helps to build the economy, creates jobs and boosts living standards for the people of South Africa. A strong financial intelligence system is a major contributor in the fight against crime and corruption.

Aligning legislation with global standards

As with other components of the international financial regulatory framework, strong standards have been developed for anti-money laundering, and to counter the financing of terrorism (AML/CFT) and the proliferation of weapons of mass destruction. These standards, developed and overseen by the Financial Action Task Force (FATF) are subscribed to by 187 countries and are endorsed by the United Nations, the Organisation for Economic Co-operation and Development, the International Monetary Fund and other international institutions.

Failure by countries to implement the agreed international standards for AML/CFT exposes them to the threat of increased monitoring by the FATF and others, which as a consequence, raises questions about the stability of countries’ financial systems and increases their risk profile. In extreme cases this has led to some countries being subjected to various forms of exclusion from the global financial system, while their domestic financial institutions face the prospect of significant penalties and reputational damage.

Various amendments to the Financial Intelligence Centre Act, 2001 (38 of 2001) were adopted by Parliament shortly after the reporting period. These amendments will ensure South Africa’s financial system is aligned with global standards and international best practice to combat money laundering and the financing of terrorism. Moreover, the amendments are in keeping with South Africa’s modernisation of its financial regulatory framework, thereby enhancing the integrity and resilience of the financial system, while seeking to improve consumer protection and market conduct in financial services.

FIC STRATEGIC OUTCOMES FOR 2015/16

- Improving the collection of information and the enforcement of compliance with the FIC Act
- Better utilisation of financial intelligence
- Promoting national interest in maintaining the integrity of South Africa’s financial system
- Ensuring a safe, secure, compliant and efficient operating environment.

VISION

The FIC strives for a safer future for all South Africans in which the financial system has integrity and transparency to support economic growth and social development.

MISSION

The FIC promotes increasing levels of compliance with the FIC Act in an efficient and cost-effective manner, enabling it to provide high-quality, timely financial intelligence for use in the fight against crime and the protection of national security.
These changes have two practical and immediate consequences for average South Africans. Firstly, consumers will be better protected, and secondly, they will begin to experience a reduced administrative burden in their financial sector interactions. The amendments are aligned to the global standards derived from the Recommendations of the FATF and various relevant United Nations Conventions and special resolutions.

The FIC Act amendments seek to:

- Address regulatory gaps and enable compliance with best practice
- Strengthen customer due diligence measures, particularly relating to beneficial ownership and persons in prominent positions
- Introduce a flexible risk-based approach to identifying and verifying customers thus reducing the burden on customers
- Improved sharing of information among designated entities and enhancing co-ordination and crime-fighting capabilities.

The international standards make risk awareness and its management the cornerstone of an effective system to combat money laundering and terror financing.

Amendments bring South Africa in line with global best practice

The FIC Act amendments are designed to introduce innovative provisions to improve the transparency and integrity of South Africa’s financial system in line with global best practice.

A risk-based approach

An important change to the FIC Act gives financial institutions the flexibility to assess and manage the risks in their businesses, depending on the category of customer. Institutions will take responsibility for how they understand and manage their risks.

The institutions will seek to understand their customers and scrutinise the way they use their products or services, making it easier to recognise inconsistent behaviour. This means going beyond basic know-your-customer requirements to establish and verify their clients’ identities.

Risk-based due diligence will require institutions to vary their approach depending on factors such as the type of customer, business relationship, product and geographic location. This will allow for increased flexibility in decision-making. The level of due diligence applied will depend on what level of money laundering or terror financing risk the institution has assigned to the customer.

This should help reduce the administrative burden for most customers as institutions take a differentiated approach, rather than applying onerous requirements across the board.

Beneficial ownership

Requiring institutions to know the people behind their companies – those who benefit financially – will bring greater transparency to the financial system. For corporate clients, this means that institutions will take reasonable measures to determine the identity of beneficial owners.

It is important to know the people behind company structures, so that financial institutions are able to understand their customers better and apply the appropriate level of risk-mitigating controls. This will also help authorities detect, investigate and prosecute instances where corporate structures have been used to cover illicit financial dealings.

This requirement brings South Africa in line with current global standards.

Prominent influential persons

According to global standards, financial institutions should pay close attention to their politically exposed customers – people in prominent positions in the public sector. The FIC Act amendments have adopted this measure and broadened its scope to include people in the private sector who do business with government (those in senior positions responsible for high-value procurement contracts).

Financial institutions will have different approaches to domestic and foreign influential persons. They will always apply additional customer due diligence to foreign influential persons, but will only do so for domestic influential persons if they assess that there are specific risks that they need to manage.

This does not presume that people in prominent positions (domestic or foreign) are assumed to be involved in financial crime. Institutions will maintain relationships with these customers, while ensuring they manage potential risks.

The FIC Act Amendment Bill will require financial institutions to identify new clients who may be prominent and influential persons in South Africa or from abroad.

Freezing of assets

The Amendment Bill establishes a legal framework for applying and administering financial sanctions emanating from UN Security Council Resolutions. The provision aims to fulfil South Africa’s obligations as a UN member state and bring its legislation in line with international standards.
Improving reporting and compliance

Fundamental to the FIC’s effectiveness and impact is that business and identified sectors comply with requirements and obligations of the FIC Act. Their compliance brings greater accountability, transparency and stability in the financial system.

The FIC Act identifies categories of business deemed vulnerable to money laundering and terror financing and lists these sectors as schedule 1 and 3 in the Act. The requirements and obligations of schedule 1 and 3 institutions in terms of the FIC Act are as follows:

**Schedule 1**
- Identify and verify clients
- Keep records of clients
- File statutory reports - cash threshold and terror property reports
- Appoint compliance officers
- Train employees on how to comply
- Register with the FIC
- Reflect compliance structures in the organisation

**Schedule 3**
- Identify and verify clients
- Register with the FIC
- File statutory reports - cash threshold reports

All businesses, including those listed in schedules 1 and 3, must also report suspicious and unusual transactions to the FIC.

The statutory reports submitted by business and institutions are critical to the work of the FIC and form the basis of the financial intelligence the FIC produces. And, as the quality of the data captured and submitted by institutions has improved over the years, so too has the ability of the FIC to produce quality financial intelligence.

Over the past six years, the number of institutions registered with the FIC has grown to 34 255.

Institutions submitted close to 9.5 million reports in total (cash threshold, suspicious and unusual transaction and terror property reports) to the FIC in the 2015/16 financial year. However, of the 34 255 institutions registered with the FIC, only 3 531 institutions (about 10 percent) were contributors or filers of these reports.

Institutions required to register with the FIC

The FIC Act requires all accountable and reporting institutions to register with the FIC within the prescribed period and in the prescribed manner. An accountable or reporting institution is an individual or an institution that, by virtue of the business it conducts, falls within the ambit of schedule 1 or 3 of the FIC Act. Accountable institutions differ from reporting institutions in terms of their client base, size, operations and the risks to which they are exposed. Their use of branches, divisions and franchises within the same legal entity is also a distinguishing feature.

In some instances, a group of companies or a legal entity may contain more than one accountable or reporting institution, for example, different entities in a financial conglomerate or divisions in a legal entity.

Of the total number of reports received, 9.3 million of these reports were cash threshold reports (CTRs), up from 6.6 million for the same period last year. CTRs are reports on cash transactions (notes, coins and travellers’ cheques) of R25 000 or more.

The top three sectors to contribute CTRs to the FIC were:
- Banks as the largest contributor of CTRs – more than 8.3 million
- The gambling industry – more than 600 000
- The foreign exchange sector – close to 160 000.

This financial year the FIC received 180 363 suspicious transaction reports. In the 2016/17 financial year, an area of focus for the FIC will be institutions’ timeous delivery of STRs.

**SUMMARY OF STATISTICS**

<table>
<thead>
<tr>
<th>Item</th>
<th>2015/16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of reports received</td>
<td>9 494 717</td>
</tr>
<tr>
<td>Suspicious transaction reports received</td>
<td>180 363</td>
</tr>
<tr>
<td>Cash threshold reports received</td>
<td>9 314 339</td>
</tr>
<tr>
<td>Approximate rand value of cash threshold reports received (9.314 million reports X R25 000)</td>
<td>R233 billion</td>
</tr>
<tr>
<td>Cash threshold reports submitted by banks</td>
<td>8.3 million</td>
</tr>
<tr>
<td>Judicial actions contributed to</td>
<td>26</td>
</tr>
<tr>
<td>Number of institutions registered with the FIC</td>
<td>34 255</td>
</tr>
<tr>
<td>Number of FIC Act compliance inspections conducted by supervisory bodies and by the FIC</td>
<td>1 396</td>
</tr>
<tr>
<td>Value of funds blocked as proceeds of crime – majority went into Criminal Asset Recovery Fund</td>
<td>R184.6 million</td>
</tr>
<tr>
<td>Requests for information from national and international law enforcement agencies</td>
<td>1 979</td>
</tr>
</tbody>
</table>
Improvements in the quality of reports received, has enabled an improvement to the quality of the financial intelligence the FIC is able to produce.

During the reporting period, the FIC implemented a new reporting and registration information and technology communications solution, which has improved its ability to process data.

**FIC modernises its reporting system**

Following several years of preparation, the FIC implemented its new registration and reporting system in 2015/16. The system went live shortly after the end of the reporting period.

The solution, called goAML, is an integrated software solution developed by the UN Office on Drugs and Crime specifically for FIUs. The FIC is the first to implement the full enterprise version of the solution. It is designed to meet the FIC’s data collection, management, analytical, document management, workflow and statistical needs.

The system improves the FIC’s capacity to:

- Register accountable and reporting institutions
- Receive large reporting volumes from business and other data
  - Analyse reports and other available data
  - Provide intelligence products to law enforcement and supervisory bodies in a seamless and secure way.

The new registration and reporting system will help the FIC ensure that the South African financial system stays relevant, effective and aligned with best practice in the global fight against money laundering and terror financing. It will also improve collaboration with reporting institutions and other stakeholders, and standardise and streamline reporting requirements.

Several institutions participated in the pilot phase to test various aspects of the system.

**The significance of partnerships – domestic and international**

Partnerships and collaboration are crucial to the work of the FIC and has been at the crux of its delivery approach since its inception in 2003.

The FIC Act assigns certain roles, responsibilities and powers to supervisory bodies to support the objectives of combating money laundering and preventing the financing of terrorist and related activities.

FIC’s quarterly meetings with supervisory bodies are opportunities to increase awareness on the FIC Act; to share experiences and to reinforce knowledge on updates and developments in the regulatory environment and compliance arena. Training and development is also conducted to harmonise approaches to supervision and enforcement of the FIC Act across different sectors.

**What is an FIC Act compliance inspection?**

An FIC Act compliance inspection is conducted in terms of section 45B of the FIC Act by an inspector appointed by the Director or head of a supervisory body in terms of section 45A of the Act. The FIC is responsible for conducting inspections on entities listed in schedules 1 and 3 of the FIC Act that are not supervised or regulated by a supervisory body. It may also support inspections conducted by supervisory bodies.

Where appropriate, an inspector may inspect the premises of an accountable or reporting institution. Inspections determine the level of compliance with the provisions of the FIC Act, or with any order, determination or directive made in terms of the Act. Inspectors have the legal power to question managers and staff; order any person to produce a document; access any computer system or equipment; or examine, make copies of or seize any document. The inspector samples client files to ensure compliance with record-keeping, client identification and verification, and reporting obligations.

The FIC and supervisory bodies cannot use their inspection powers to investigate criminal conduct. If the FIC or supervisory body suspects that a criminal offence has or is being committed by the person who is the subject of the search, or if the premises are a private residence, an inspector may only conduct the inspection after a magistrate or judge has issued a warrant, or if the FIC has obtained permission from the institution to be inspected.

The FIC and the supervisory bodies conduct inspections using a risk-based approach. This means that inspectors focus on the inherent and residual risks in an institution’s business structure, customer profiles, internal controls, and products and services.
During the course of the 2015/16 financial year, supervisory bodies and the FIC conducted 1,396 FIC Act compliance inspections. Sixty-six of these were conducted jointly, while 1,251 inspections were conducted by the supervisory bodies individually.

The FIC has signed memoranda of understanding (MoUs) with the supervisory bodies which govern how they will relate to the FIC, and how supervisory bodies engage with the entities that report to them in terms of compliance with the requirements of the FIC Act.

Financial intelligence produced by the FIC is important for law enforcement, revenue agencies, police and others to support their investigations and forfeiture processes.

Demand for FIC’s financial intelligence products increased in 2015/16, increasing to 1,979 requests from 1,799 in the previous year.

FIC also contributed to 26 judicial actions – a court’s action or decision after a hearing – by providing affidavits on matters presented during court proceedings. The FIC blocked R184.6 million as suspected proceeds of crime during 2015/16.
These are some examples of instances where, thanks to the reports submitted by institutions, together with additional data, the FIC has been able to produce financial intelligence which has assisted law enforcement and prosecutorial authorities and other partners in solving crime.

**SOUTH AFRICA LINKED TO GLOBAL INTERNET SCAM**

The FIC helped identify fraudsters in South Africa who were members of a global syndicate. The syndicate scammed hundreds of internet users outside of South Africa out of millions of dollars.

The fraudsters used fake profiles on dating sites and hundreds of fake e-mail accounts to convince people to ship electronic goods or wire money to bank accounts in Gauteng.

Analysis by the FIC revealed that the syndicate used the proceeds of their scams to buy properties and vehicles. The FIC was also able to identify their domestic bank accounts and froze three accounts belonging to the syndicate’s kingpin. Preservation and forfeiture orders were issued for assets valued at R2.4 million.

**MILLIONS SEIZED ON MOZAMBIQUE BORDER**

On Christmas Day 2015, more than R78 million in cash and a Toyota Hilux were seized following the arrest of two Mozambican nationals at the Lebombo Border Post.

Mpumalanga’s Asset Forfeiture Unit, which used several FIC financial intelligence reports during its investigation, apprehended the subjects with US dollars and euros hidden in various custom-made compartments in the vehicle. The Asset Forfeiture Unit obtained preservation orders for this cash.

**STOLEN STUDENT LOANS**

The FIC received a suspicious transaction report regarding an employee working in the finance department of a university. The employee was diverting tuition payments from student loans into his personal bank account after advising the donor of a change in the university’s banking details.

The FIC established that the subject made payments into various bank accounts, including his family members’ accounts, and purchased luxury vehicles. This information was shared with law enforcement agencies in a detailed report, substantiated with a flow of funds analysis.

The FIC issued intervention directives on various bank accounts, securing more than R4.6 million, and the matter was referred to law enforcement agencies. The organisation’s financial intelligence helped the Asset Forfeiture Unit obtain a preservation order for funds in the subject’s bank account and movable as well as immovable property.

**CATCHING PHISH**

The FIC worked with the Asset Forfeiture Unit, SARS, the South African Police Service, the South African Banking Risk Information Centre and various banking institutions to uncover a phishing scam.

Phishers clone bank accounts using sophisticated devices. After the phishers have identified a potential phishing victim, they contact SIM swappers to block the owner’s cell phone number so that account holders do not receive transaction notifications. This allows the phishers to log into the victim’s account and transfer money out of it. The money is then immediately withdrawn from different ATMs, after which the ATM cards are discarded. The mobile service provider employees are paid for assisting with the SIM swap, while the rest of the money is deposited into the accounts of the main phishers.

With the FIC’s assistance, law enforcement arrested some of the subjects and seized laptops and cell phones. Three of the perpetrators have been sentenced to between 15 and 20 years in prison.
FRAUD AGAINST THE NATIONAL LOTTERY

Employees of a non-profit organisation submitted an application to the National Lottery for project funding of about R1.2 million, without their organisation’s authorisation. One of the employees fraudulently opened a bank account using the organisation’s name and the National Lottery paid project funds into this account.

The FIC followed the money trail through various bank accounts to one held with another financial institution, which contained just under R1 million. The FIC froze the account and law enforcement was able to recover the full amount.

FOREIGN EXCHANGE PONZI SCHEME

Ponzi schemes promise unrealistically high returns on investments based on elaborate investment business models. They require a constant stream of new investors to bring money into the scheme. When this stream slows down, the scheme collapses because regular payments to investors cannot be made.

The FIC used STRs to uncover a forex trader scheme that promised average returns of 48 percent per year on small investments and 84 percent per year on big investments. During the FIC’s analysis, it became evident that this was a Ponzi scheme. The scheme owner used large amounts of investor funds for two properties, luxury vehicles, shopping expenses and staff salaries.

The FIC shared its analysis with supervisory bodies and law enforcement agencies, which led to the blocking of accounts held by the scheme to the value of R87 million. The Asset Forfeiture Unit obtained a preservation order for R12 million in blocked funds and properties.

MONITORING BANK ACCOUNTS LEADS TO DRUG BUST

The FIC’s monitoring of bank accounts played a central role in identifying and arresting a criminal syndicate that was growing dagga in hydroponic drug laboratories. Eleven people were arrested and drugs were seized from 10 locations around Gauteng.

The FIC assisted in a large-scale investigation to identify the syndicate’s crime structure, profile the role players, and identify the assets and money laundering techniques used. This financial intelligence was used to confirm the identity of various role players in the syndicate and indicate how proceeds were laundered. The FIC exchanged this information with law enforcement agencies and assisted in building a criminal case, which resulted in the arrest of various role players associated with the syndicate.

AMERICAN PROPERTY PURCHASER SCAMMED ONLINE

When buying property in New York, an American citizen was duped into paying a portion of his purchase amount into a fraudulent account.

The fraudulent account holder intercepted e-mails between the property purchaser and his estate agent. Posing as the estate agent over e-mail, the subject convinced the purchaser to pay cash for the property into the fraudulent account. The funds were then immediately transferred to three different accounts held in South Africa.

After gathering information from its American counterparts, the FIC immediately authorised intervention directives to freeze the funds in the three accounts and tracked funds to six other accounts. The FIC gathered enough intelligence to issue an additional four intervention directives and identified three vehicles bought with some of the crime’s proceeds.

The National Prosecuting Authority and the Asset Forfeiture Unit obtained preservation orders against nine accounts and three motor vehicles. The co-operation between all stakeholders involved resulted in the recovery of 93 percent of the stolen funds.
GUESTHOUSE OWNER ARRESTED FOR CHILD PORNOGRAHY

The FIC assisted the Family Violence, Child Protection and Sexual Offences Unit of the South African Police Service with a case involving a guesthouse owner based in South Africa. The man was suspected of accessing child pornography on websites from outside the country, and selling child pornography acquired in South Africa on certain websites.

The FIC was asked to identify financial transactions linked to the sale of the pornographic material. The FIC analysed transactional information and identified certain payments to support the allegations, which helped lead to the guesthouse owner’s arrest.

The FIC’s report also played a key role in the subject’s bail application, resulting in a bail amount that was acceptable to the investigation team and the community. The guesthouse owner faces possible extradition once the judicial process is completed in South Africa.

FIC HELPS UNCOVER ILLEGAL STOKVEL

Alerted by 13,000 cash deposits into one account in one day, the FIC worked with the Asset Forfeiture Unit and the South African Police Service’s Commercial Crimes Unit to identify an illegal stokvel.

The stokvel promised unrealistically high, quick returns and a lavish lifestyle of international travel in return for an investment of just R295. Prospective members were required to deposit money and attend a seminar on travel arrangements and investing. Little training was actually given at these seminars. Instead, participants were encouraged to recruit as many new members as possible into the stokvel. Like all pyramid schemes, the stokvel was heavily dependent on continuous membership growth.

The investigating team froze five bank accounts containing R26 million and obtained preservation orders against the main accounts. According to the Asset Forfeiture Unit, this is the fastest it has ever identified and acted on a pyramid scheme.