Financial
Intelligence Centre

CASE STUDIES AND INDICATORS COLLECTION

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.

VALUES

The FIC seeks to achieve its mandate through the employment of highly capable staff members who are committed to the highest standards of excellence and professional service delivery in the fulfilment of their responsibilities.

CONTENTS

THIS PUBLICATION

The featured case studies have been published over a period of time in the FIC's annual reports. The case studies are arranged by crime type and some indicators – not an exhaustive list – are included to assist in identifying criminal activity.

Core to the case study successes has been the collaboration between the FIC and its competent authority partners, as well as the regulatory reports submitted by accountable and reporting institutions, and other business. Regulatory reports form the foundation of the financial intelligence reports that the FIC produces.

INTRODUCTION

The Financial Intelligence Centre (FIC) is South Africa's national centre for gathering and analysing transactional and related information, for the purpose of producing financial intelligence reports.

The FIC was started in early 2003 following the signing into law of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001). The FIC's primary purpose is to protect the integrity of South Africa's financial system and to contribute to the administration of justice. It does this by fulfilling its mandate, which is to identify the proceeds of crime, combat money laundering and the financing of terrorism (ML/FT) and related activities.

The FIC Act obliges certain financial and non-financial institutions to submit regulatory reports to the FIC. Before submitting reports, these institutions are required to register with the FIC.

IDENTIFY PROCEEDS OF UNLAWFUL ACTIVITIES

COMBAT MONEY LAUNDERING

COMBAT TERRORIST FINANCING

COLLABORATE AND SHARE INFORMATION WITH:

- NPA
- LEA's
- Supervisory bodies
- Intelligence services
- SARS
- Other international agencies

SUPERVISE AND ENFORCE compliance with the FIC Act

FIC has no investigative powers but collects analyses

FIC'S ROLE AND FUNCTION

As part of its role in administering the FIC Act, the FIC provides identified industry sectors (accountable and reporting institutions) and supervisory bodies guidance and oversight on the Act. This is to ensure optimal awareness and compliance with the requirements of the FIC Act.

For accountable institutions, these compliance requirements include: registration with the FIC, identifying and verifying clients; maintaining records of clients; submitting regulatory reports to the FIC, appointing a compliance officer, to develop, document, maintain and implement a risk management and compliance programme, and training staff on their internal FIC Act compliance rules. Reporting institutions are required to register with the FIC and to file cash threshold reports on transactions of R24 999.99 and above.

All business, whether accountable or reporting institutions, or any other type of business, is required to submit reports on transactions known or thought to be suspicious or unusual. Information in regulatory reports can be indicators of funds being generated illicitly, and they can help enrich the content of FIC's financial intelligence reports.

The FIC is legally bound to protect the confidentiality of the source and content of all regulatory reports it receives and to ensure that no person's rights are unlawfully and unfairly prejudiced through unlawful access. This confidentiality clause relates those who submit regulatory reports, the reported person or entity, and/or any third parties mentioned.

CONDUCTING ANALYSIS

The FIC Act assigns myriad powers upon the FIC including the ability to: instruct a financial or non-financial institution, an accountable or reporting institution or any person not to proceed with a transaction or a proposed transaction for 10 working days; obtain a monitoring order which is signed by a judge in chambers, ordering an accountable institution to report on transactions of a client and request further information on a client.

Fulfilment of regulatory reporting obligations is one of the most important ways in which businesses contribute to their own long-term efficacy and integrity, as well as to that of the broader South African economy and financial system.

Using information in the regulatory reports, as well as publicly and non-publicly available databases, the FIC conducts its analysis enabling it to follow the money to identify and trace possible proceeds of crime and/or illicit transactions, and to develop financial intelligence reports. These reports assist FIC's domestic and foreign partners in their investigations, prosecutions and other follow up actions in the pursuit of combating crime. The FIC disseminates financial intelligence reports to its partners in law enforcement, intelligence services, supervisory bodies and other competent authorities. Such information is also exchanged between the FIC and its foreign counterparts. The FIC does not itself conduct investigations or prosecutions.

WHAT IS MONEY LAUNDERING

Te primary intention of money laundering is to transform illicit monies into legitimate funds. This is done by introducing it into the financial system – changing money from 'dirty' to 'clean'.

Where money is laundered successfully, criminals are able to have full control over their money in the financial system.

To acquire their proceeds, criminals may conduct a wide range of offences from petty to more serious crimes.

TRANSFORM
ILLICIT
MONEY
into
LEGITIMATE
money

Once the proceeds are in the possession of the criminal, the money may be integrated into the financial system through:

- The purchasing of high-end goods like property or motor vehicles
- The establishment of shell companies
- By moving the money transnationally and so on.

Criminals may use legitimate business for their purchases so that true ownership becomes hidden, requiring extra vigilance from authorities and institutions.

FINANCING OF TERRORISM

The objective with financing of terrorism is to fund individuals and/or organisations involved in terrorism or terrorist activities.

A notable difference between money laundering and terrorist financing is that while money laundering seeks to legitimise money from illegal sources, funds for terrorist financing may be sourced from both legitimate and illegal sources. Furthermore, terrorist financing transactions may not always raise suspicion, as the underlying transactions may not necessarily be large or complex.

THREE STATES OF MONEY LAUNDERING

IT ALL STARTS WITH A CRIMINAL ACTIVITY

E.g. A criminal sells drugs. The proceeds are then laundered through the three stages

STAGE 1 PLACEMENT

OBJECTIVE

To **move** dirty money **into** the financial system.

CHARACTERISTICS

The intention is to use legal and illegal activities to convert proceeds into **usable products**.

HOW?

- Usually via financial instruments such as bank accounts or insurance products, which will place the money into the financial system.
- Some techniques may include gambling, purchase of high-end goods with payment being done by cheque, electronic or bank transfers or mixing legal deposits of cash with illicit monies.
- An option criminal may also use is to break up large amounts of illicit cash and deposit these in smaller amounts over time, into one or various bank accounts.

STAGE 2 LAYERING

OBJECTIVE

Criminals need to **create distance** between themselves and the illicit proceeds.

CHARACTERISTICS

The intention is to create anonymity.

They need to ensure that the source (the criminal activity) of illicit proceeds **cannot be linked to them**.

HOW?

- Criminals will create complex layers of transactions. This makes it difficult to trace transactions or to link back to the original criminal activity.
- The idea is to blur the understanding of ownership – confusion is key.
- Audit trails may be complicated further by proceeds being moved to foreign countries via shell companies, property purchases, moving money between accounts, transferring funds into various monetary instruments etc.

STAGE 3 INTEGRATION

OBJECTIVE

At this stage the criminal must **legitimise** the illicit proceeds.

CHARACTERISTICS

Depending on the success of the placement and layering phase, the illicit proceeds are **indistinguishable** from legitimate funds in the financial system.

HOW?

- Criminals are now free to spend their illicit monies.
- They claim they have earned their money from legitimate business dealings.
- They deepen the spread of criminal money into the financial system via the purchase of high-end goods, businesses and other items.
- Others continue to use the proceeds to fund more criminal activities.
- Funds are also used to fund terrorism and the proliferation of weapons of mass destruction.

GLOSSARY OF TERMS AND ABBREVIATIONS

Accountable and reporting institutions	Identified financial and non-financial institutions and sectors that may be used for money laundering purposes. Accountable and reporting institutions are listed in Section 1 and 3 of the FIC Act respectively.
Advance fee fraud	Requests or demands for advance payment for services or other elements to cover administration fees, processing or completion of a deal or many deals
AFU	Asset Forfeiture Unit in the National Department of Public Prosecutions
AML/CFT	Anti-money laundering and combating the financing of terrorism.
ATM	Automatic teller machine
CTR	Cash transaction report on transactions of R24 999.99 and above
Competent authorities	Includes authorities such as the National Prosecuting Authority (NPA), the South African Police Service (SAPS), the Asset Forfeiture Unit (AFU), the Special Investigating Unit (SIU), the Independent Police Investigative Directorate (IPID), the Public Protector (PP), intelligence services and supervisory bodies. Also includes foreign, partner financial intelligence units
FATF	Financial Action Task Force
Indicators	Methods used by criminals in executing their crimes
Money laundering	Money laundering is the process of disguising the source and/or ownership and disposal of money derived from criminal activity to make it appear as if it has stemmed from legitimate sources
ML/TF	Money laundering and terrorist financing
Tax evasion	Illegal, non-payment or under-payment of tax
Tax avoidance	Arranging financial affairs so as to minimise tax liability within the law
Ponzi	A fraudulent scheme in which participants invest in an enterprise which offers quick and unusually high returns. The scheme is unsustainable as funds are not invested but used to support the illusion of an investment scheme.
Pyramid scheme	Scheme where individuals are recruited to participate. Return on investment is dependent upon the subsequent recruitment of investors. Payouts to early investors make it seem like it is a worthwhile initiative.

Preservation orders and forfeiture orders	Where it is believed that property (money, fixed property, motor vehicles and so on) is related to the instrumentality of an offence, or it is the proceeds of unlawful activities, the Asset Forfeiture Unit can apply to a court for a preservation order on the property, preventing any person from dealing in any manner with the property. Where there is a preservation order in place, the National Director of Public Prosecutions can apply to a high court for forfeiture of that property.
Regulatory reports to the FIC	Reports required to be submitted to the FIC by: Accountable institutions: cash threshold, suspicious and unusual transaction and terrorist property reports Reporting institutions: cash threshold reports All businesses, including accountable and reporting institutions: are required to submit reports on suspicious and unusual transactions.
SAPS	South African Police Service
SARB	South African Reserve Bank
STR	Suspicious and unusual transaction report
Section 27	Section in the FIC Act which authorises representatives of the FIC to request information from an accountable institution on whether a specified person is acting or has acted on behalf of any client of the accountable institution or whether a client of the accountable institution is acting or has acted for a specified person
Section 34	Section in the FIC Act which allows the FIC to instruct an institution, accountable and reporting institutions and persons not to proceed with a transaction, a proposed transaction or any other transaction related to that proposed transaction for a period of not more than 10 working days. This allows the FIC to make the necessary inquiries concerning the transaction and, where necessary, to inform and advise an investigating authority or the National Director of Public Prosecutions
Section 35	Section in the FIC Act which allows the FIC to approach a judge in chambers to obtain permission, to order an accountable institution to report to the FIC on transactions of clients suspected of money laundering or terrorist financing. This is to expedite access to information by the FIC on suspected proceeds of crime, money laundering or terrorist financing

CASE STUDIES AND INDICATORS

PYRAMID SCHEMES

Explanation: Stokvel abuse

Stokvels can be used as a cover for pyramid schemes. It is important to know that people involved in the types of social clubs known as stokvels, must have a constitution which states, among other aspects, the number of members and contributions to be made by each member, and the frequency of their contributions. Stokvels that promise returns greater than those offered by commercial banks should be treated with caution.

MAIN CRIME TYPE	PYRAMID SCHEME

FIC helps uncover illegal stokvel

Alerted by 13 000 cash deposits into one account in one day, the FIC worked with the AFU and the SAPS'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 growth in membership.

FIC banks accounts containing R26 million were frozen, preservation orders against the main accounts were obtained. According to the AFU, this was the fastest it had ever identified and acted on a pyramid scheme.

MAIN CRIME TYPE	PYRAMID SCHEME

Uncovering a pyramid scheme

The FIC referred two STRs to the SAPS based on suspicions that a community-based pyramid scheme was drawing on the investments of poor people using false promises. The Bellville commercial crime branch in Cape Town opened an investigation.

On visiting the subject's residence, the police observed a long queue of people who explained that they were investing money that would deliver huge dividends by the end of the week. Further investigation confirmed the subject's involvement in pyramid scheme activities. Important evidence was seized from the residence.

After conferring with the police, the banks froze the relevant accounts. The subject approached the court to overturn the hold on his accounts. Meanwhile, the AFU requested the FIC to place a section 34 hold on the relevant accounts, and the FIC identified two additional accounts.

INDICATORS | Pyramid Scheme

- The promise of unrealistically high, quick returns for nominal investment.
- High and fast returns may suggest that commissions are being paid out of money received from new recruits.
- Prospective members required to deposit money (joining fee) and attend a seminar on travel arrangements and investing.
- Not much business training offered to potential business partners.
- Recruited persons have to qualify for certain levels of bonuses, which require various levels of product purchases and other associated costs.
- Like all pyramid schemes, illegal stokvels rely on continuous membership growth and recruitment of new participants encouraged.
- The business model is vague or overly complex, and difficult for members of the public to understand.
- A complex commission structure in place for the stokvel or pyramid scheme.
- Investment schemes that rely on recruited persons bringing in more participants in order to generate a return, is a classic trait of both pyramid and Ponzi schemes.

PONZI SCHEMES

Explanation: A Ponzi scheme is a fraudulent investment scheme. It offers investors unusually high or unrealistic returns on investment based on elaborate business models. They require a constant stream of new investors to bring money into the scheme, as pay-outs do not come from actual profits. When this stream slows down, the scheme collapses because regular payments to investors cannot be made.

MAIN CRIME TYPE	PONZI SCHEME
ASSOCIATED CRIME TYPE	SCAM

Inter-agency co-operation brings Ponzi scheme to a halt

The FIC co-ordinated an inter-agency task team that tackled the largest Ponzi scheme yet to operate in South Africa. The estimated value for the South African leg of the scheme was over R12 billion.

The scheme drew in several hundred "investors" who contributed substantial funds to import antiretroviral drugs, based on the promise of large percentage pay outs. As the economic recession hit home globally, the funds to pay out investors at the promised rates dried up and the scheme was revealed.

A task team was formed, made up of agencies in the departments of Justice and the National Treasury. The FIC provided the financial intelligence that helped with co-ordination of a targeted investigation and to identify information which was used as evidence for eventual prosecution.

Perpetrator's accounts were frozen and some assets were confiscated. The task team also developed a list of all scheme investors, facilitators and administrators. The investigation was supported by the FIC's partnerships with financial intelligence units in several other countries. International co-operation helped the FIC to establish the cash flow pattern, the accounts involved and the method use to launder money. This information was given to other agencies which also helped give direction for the investigation.

MAIN CRIME TYPE	PONZI SCHEME
ASSOCIATED CRIME TYPE	CRYPTO CURRENCY OR BITCOIN

Cracking a crypto currency Ponzi scheme

The FIC identified what appeared to be an alleged Ponzi scheme run by an individual marketing a "new crypto currency". This product was marketed as Africa's first crypto currency and investors were promised huge returns on their investments.

The FIC's analysis of the individual's bank statements revealed that there was no crypto currency 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. In addition, the FIC assisted the AFU in obtaining a preservation order relating to fixed property worth more than R4 million that was bought using the proceeds of the scheme.

MAIN CRIME TYPE	PONZI SCHEME
ASSOCIATED CRIME TYPE	FRAUDULENT INVESTMENT ACCOUNT

Ponzi scheme uncovered

Through its analysis of STRs, the FIC identified two business accounts with activities indicative of a Ponzi scheme.

Both investment companies promised a 100 percent return on investment within one to five days. Working with the South African Reserve Bank, the SAPS and the then Financial Services Board (now known as the FSCA – Financial Sector Conduct Authority), the FIC shared its analysis for judicial action to recover the proceeds of the scheme.

MAIN CRIME TYPE	PONZI SCHEME
ASSOCIATED CRIME TYPE	FRAUD

Foreign exchange Ponzi scheme

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 to the value of R87 million held by the scheme. The AFU obtained a preservation order for R12 million in blocked funds and properties.

MAIN CRIME TYPE	PONZI SCHEME
ASSOCIATED CRIME TYPE	UNREGISTERED FINANCIAL SERVICE PROVIDER

Uncovering an investment scheme

The FIC became aware of a R50 million Ponzi scheme and referred the information to the relevant supervisory body and the AFU. The supervisory body's investigation revealed that the company concerned was conducting the business of a financial service provider without being registered to do so. FIC analysis revealed that several accounts were being used by the scheme.

Information collected by the FIC helped the AFU obtain preservation orders on these accounts. The recovered money was paid into the Criminal Asset Recovery Account.

INDICATORS | PONZI SCHEME

- Offer of high investment returns with seemingly little or no risk. Every investment carries some degree of risk, and investments yielding higher returns typically involve more risk.
- Overly consistent returns. Ordinarily, investment values and returns tend to go up and down over time. In general, Ponzi schemes generate regular, positive returns regardless of prevailing market conditions.
- Unregistered investments. Ponzi schemes typically involve investments that have not been registered with regulators.
- Unlicensed sellers. Stock exchange laws require investment professionals and their firms to be licensed or registered. Most Ponzi schemes involve unlicensed individuals or unregistered firms.
- Investors are encouraged to source new investors.
- Purchase of high-value assets.
- Similar transacting patterns involving cash and electronic funds transfers across different accounts.
- Unexplained source of money. Perpetrators often explain an elusive, unclear and sophisticated plot to generate huge profits. For example, they say that because investment involves many businesses, the development work and the flow of money investment cannot be explained in detail.
- The business model is vague or overly complex and difficult for a lay person to understand.

419 SCAMS

Explanation: 419 scams or advance fee fraud

Measured by monetary losses, the 419 "advance-fee" fraud is the world's most prevalent scam. It originated in the early 1980s in Nigeria, and is named after a section of that country's criminal code. This scam is no longer confined to Nigeria – 419 fraudsters are arrested throughout South Africa and around the world.

Commonly, 419 scams begin with an e-mail, a message via cell phone, or any other means of communication, with the aim of persuading the recipient to advance money to the sender, with the promise of a large future pay out. Messages sent by scamsters often contain letterheads or references to companies, government departments and international organisations in a bid to persuade recipients.

The author often claims to be royalty, fabulously wealthy or being on the verge of receiving a huge inheritance payout. They promise large amounts of money if the recipient of the communication pays a sum of money to 'release' the payouts, or if they forward their bank details. Perpetrators advance a range of claims to explain why they need the recipient's help: funds are said to be trapped in central banks due to political unrest; massive inheritances are hard to access because they exiled, because of government restrictions or taxes; and so on.

Remember: If an offer sounds too good to be true, it probably is. See e-mail snippet below.

MAIN CRIME TYPE	419 SCAM
ASSOCIATED CRIME TYPE	INVESTMENT SCAM

Advance fee fraud: E-mail excerpt

419 scam *(Spelling as in original)*

You may be surprise to receive this message from me since you don't know me in person, but for the purpose of introduction, I am Mr (NAME REMOVED).

Before the death of my father, he took me to SOUTH AFRICA to deposit the sum of $25.5 million with a security and finance company as if he knew the looming danger in Angola.

I, my mother and my family … have decided to transfer this money to a foreign country where we can invest it…. The South African monetary policy/law does not allow such investment hence I am seeking for an asylum or refugee. I must let you know that this business is 100% risk free and the nature of your business does not necessary matter.

So if you are willing to assist us, we have agreed to give you 20% of the total money, 40% will be for a joint business venture I will be doing with you and another 35% will be for me and my family which we shall also invest in your country and the remaining 5% will be mapped out for all expenses we may Incurred during the transaction.

Therefore, if you are willing and interested to render the needed assistance, endeavour to reply through my email address or the above Tel number. I also need your private phone and fax number for easy communication.

Remember that this is highly confidential and the success of this business depends on how secret it is kept.

MAIN CRIME TYPE	419 SCAM
ASSOCIATED CRIME TYPE	ACCOMMODATION SCAM

Accommodation Scam

The FIC helped competent authorities in the investigation of accommodation scams targeting foreign visitors during the 2010 FIFA World Cup. Syndicates advertised bogus bookings over the internet, and demanded large deposits to "secure" reservations. Unsuspecting tourists were lured to deposit funds. The booking agents would subsequently disappear and no longer be contactable.

In one such instance, an individual was asked to deposit R18 000 into the account of a third party. The victim made an electronic transfer, and only realised that she had been the victim of a scam when the guest lodge said it had no room reservation confirmed for her.

The FIC discovered that the account into which the funds had been deposited was owned by a South African who had previously been reported for suspicious overseas remittances. Furthermore, the account was linked to 419 scams; it was held in a third country under a different name.

INDICATORS | 419 SCAM

- Small investment with promise of high return.
- The details of the business, or reasons for payment request, are often are confidential or secretive.
- Unknown sources of money and unrealistic value of funds are presented.
- Unsolicited offers for the opportunity to invest in an exclusive deal.
- Request for assistance to remove funds from a high risk jurisdiction.
- Suspicious overseas remittances.
- Request for large deposits or advance payments to reserve services, unlock access to funds or to cover administrative processing expenses to complete the deal.
- "Risk-free" transactions in which confidentiality is emphasised.
- Variety of paperwork offered as 'proof' of authenticity, including blank company letterheads that are signed, blank invoices and company details, letters written under government department and other organisation's logos.
- Requests for bank account information. These are commonly used to obtain further information and siphon monies from the accounts of targeted individuals and firms. The funds are then transferred into an account under the control of the criminal syndicate.

CYBER CRIME

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	FRAUD

Computer hacking, cloning of bank accounts

The FIC was part of a multi-agency investigation team after cyber attackers gained access to the bank accounts of two financial institutions and transferred large sums of money to several beneficiary accounts. The FIC traced and identified these multiple bank accounts, and tracked the flow of funds to block the accounts.

In the first attack, R72.2 million was illegally transferred into 1 433 different accounts, and was immediately dissipated. These beneficiary accounts – mainly dormant accounts – were accessed with legitimate login credentials stolen by loggers and/or spyware. A complicit bank employee created duplicate cards to access these accounts.

In a second incident, with inside help, a syndicate hacked into a bank's computer systems and transferred R42 million to a large number of beneficiary accounts. These amounts were immediately withdrawn using ATM cards with increased daily limits. Analysis determined that two of the financial institution's computer workstations had been cloned to enable the fraudulent transfers.

The FIC created profiles on the beneficiaries of these transactions and identified various suspects, related bank accounts and investment portfolios. Cell phone data supplied by investigating authorities was analysed and links between suspects were identified. As a result of the joint operation, several suspects were arrested. The FIC created a database that was used to successfully oppose bail. Information supplied by the FIC was used to support preservation orders on immovable and movable property, such as expensive houses and vehicles.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	CARD SKIMMING

Central bank of a neighbouring country

A neighbouring country's central bank's credit card was skimmed and cloned using sophisticated cyber aids. The bank was defrauded of R7 million and the stolen funds were paid into four different South African bank accounts, held by individuals who did not have any business dealings with the central bank.

The FIC froze the four accounts in terms of section 34 of the FIC Act. The FIC's analysis uncovered that the proceeds were used to buy high-value items. Based on intelligence reports and affidavits prepared by the FIC, the AFU successfully obtained preservation orders in terms of the Prevention of Organised Crime Act.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	FRAUD

Pay point machines

A former employee of a company responsible for maintaining the pay point machines of prominent retail outlets started approaching these retail outlets in rural and smaller towns, allegedly to service their machines. He used this false cover to debit funds from the accounts of various customers and diverted the proceeds to his personal account.

The FIC was approached to assist in tracking the funds. It froze more than R165 000 in the employee's account.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	SCAM

Online romance scam

The FIC, operating in a task team, identified an individual who used an online dating website to extort funds from his victims. The funds were paid into an entity bank account. The FIC was able to identify the signatory on the entity's bank account as being a Nigerian national with South African citizenship.

The subject had been running this scam for more than seven years, making about R13 million in Europe and North America. The latest victim, from North America, reported him after losing R1.8 million. The subject laundered the proceeds by using the money to renovate his house, buy expensive clothing and electronic equipment, and pay school fees.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	PHISHING

Catching phish

The FIC worked with the AFU, SARS, the SAPS, 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 cards used at the ATMs are discarded. 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 were sentenced to between 15 and 20 years in prison.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	CYBER FRAUD, CRYPTO CURRENCY SCHEME

Cyber fraud

The FIC received an alert when a person in a neighbouring jurisdiction was defrauded of a large amount of money that had been transferred to a South African financial institution.

Some funds were transferred to a crypto currency exchange and subsequently converted into a basket of crypto currencies, including Bitcoin. Some funds were irrecoverable because they were transferred to another crypto currency exchange in a foreign jurisdiction.

The FIC froze the account held with the crypto currency exchange using a section 34 directive. It also provided an affidavit that led to the AFU obtaining a preservation order from the High Court in Johannesburg.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	CRYPTO CURRENCY SCHEME

Bitcoin investment scheme

An entity was hosting meetings and seminars at prominent hotels and casinos throughout South Africa. Participants were charged seminar fees and encouraged to buy Bitcoin to increase their wealth quickly. The currency seemingly promised a 50 percent return on investment when sold.

The FIC's analysis revealed that the entity's account was not used for formal business activity but as a front to lure investors into contributing towards an unknown investment goal. Funds in the account were being depleted rapidly and were not being replenished by new contributors.

Working with the SARB, the SAPS and then Financial Services Board (now known as the Financial Sector Conduct Authority), the FIC shared its transactional analysis for judicial action to recover the proceeds of the scheme.

MAIN CRIME TYPE	CYBER CRIME
ASSOCIATED CRIME TYPE	CHILD PORNOGRAPHY

Guesthouse owner arrested for child pornography

The FIC assisted the Family Violence, Child Protection and Sexual Offences Unit of SAPS 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 via 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.

INDICATORS | CYBER CRIME

- The use of crypto currency.
- The use of institutions in foreign jurisdictions or cross-border transactions.
- The use of mobile banking applications.
- Large transfer of funds followed by immediate ATM withdrawals.
- Transactional activity or funds in bank accounts does not match the profile of the client.
- Sudden activity such as large deposits ad rapid withdrawals on previously dormant accounts.
- An increase in daily transactions followed by sudden, large withdrawals or transfers.
- Duplication of cards in order to access accounts.
- Use of cloned ATM cards with increased daily withdrawal limits.
- Structuring of funds into multiple accounts.
- Purchase of high value assets to hide the proceeds of crime.
- Funds that do not match the profile of the client.

TAX EVASION – TAX HAVENS

Explanation: Tax havens

The FIC has identified several areas of concern related to electronic fund transfers to offshore investment tax havens.

Investment-related transactions to tax friendly foreign jurisdictions were of interest because the transaction category selected to process the payment appeared to be abused. Reports have shown that individuals exceed the set threshold of R10 million in foreign currency transactions per individual per year.

Individuals may legitimately invest in other countries in the hope of obtaining favourable tax benefits. If not adequately regulated, however, such investments can provide avenues to hide the proceeds of crime or to evade the payment of tax.

FIC intelligence shows that tax havens have featured prominently as destination countries for outward transactions and various reports have been routed to the SARS for evaluation. Trends and patterns have also given rise to the identification of various individuals and entities that warranted investigation by supervisory authorities and law enforcement agencies.

The analysis established that:

- One of the jurisdictions was preferred for both individuals and entities.
- Most offshore investment transfers to one of the jurisdictions were to non-resident individuals (rather than entities).
- Most investment transfers to one of the countries involved bonds and equities.

MAIN CRIME TYPE	TAX EVASION, TAX HAVENS
ASSOCIATED CRIME TYPE	TRUST ACCOUNTS

Abuse of attorney's trust account

The FIC received several STRs about an attorney who appeared to be abusing his attorney trust facility, which must be regulated in terms of section 78(1) of the Attorneys Act (1979).

The suspicious and unusual transactions in the reports pointed out the following:

- Multiple large sums of money were being deposited into the trust account by different persons and companies over a period exceeding two years.
- These funds were used to make payments to other depositors in South Africa and abroad.

- Funds from this account were being remitted to foreign jurisdictions deemed to be tax havens.
- Some monies were transferred to the attorney's personal credit card; his practice expenses were also paid directly from the trust account.

INDICATORS | TAX EVASION AND TAX HAVENS

- The use of off-shore tax havens for the purpose of criminally evading income tax payments.
- The use of complex financial transactions between fictitious entities.
- Use of common address and bank accounts by several persons and corporate entities.
- The location of the business is not the same jurisdiction in which the account holder lives.
- Large, unusual claims and deductions, or similar claims all made in the same manner.
- Large and/or frequent foreign currency transactions or cross-border transactions.
- Use of nominees.
- Excessive loans granted to individuals.
- Personal expenses paid with corporate funds.
- Double payment of bills.
- A sudden and unexplained spike in turnover of the trust account.
- Servicing of practice expenses via the trust account, for example, fees or commission paid to the attorney from the account.
- Servicing of personal expenses from the trust account. Transfers to a personal credit card to buy luxury items.
- No business trust account servicing the practice.

FRAUD AND CORRUPTION

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	TRUST ACCOUNTS

Front companies

The FIC formed part of a multi-agency investigation into a case of corruption and fraud involving several officials at a government department responsible for the administration of a R100 million social and economic development fund. The FIC collected financial intelligence on the subjects and their related entities.

Initial analysis revealed that funds were being diverted to projects benefitting former senior employees of the department who had been responsible for allocating grants for qualifying projects.

Financial intelligence revealed front companies, through which these former employees' relatives had set up projects or entities to receive grants from the fund. The proceeds of these illegal grants were used to buy properties and vehicles. Some of the proceeds were laundered through the attorney's trust accounts.

Financial intelligence enabled the identification and issuing of subpoenas for more than 100 bank accounts, which allowed the forensic auditors to compile a detailed cash flow analysis of the scheme.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	COMPANY HIJACKING

Fraudulent company scam

The FIC assisted a law enforcement agency with an investigation concerning fraudulent companies that were being used as vehicles to commit financial crimes. The modus operandi of this syndicate involved the following:

- The syndicate registered legal entities with the then Companies and Intellectual Property Registration Office (now the Companies and Intellectual Property Commission – CIPC) using names that were confusingly similar to those of legitimate, existing businesses in South Africa
- Using these details and employing false identity documents, the syndicate opened several bank accounts for the "duplicated" companies and began making multiple changes to account information
- The syndicate then successfully changed the banking details of the aforementioned legitimate companies, and channelled the money of these firms into the accounts opened with false identity documents.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	MONEY LAUNDERING VIA CASINOS

Gambling chips

At a roadblock in Gauteng, the SAPS discovered precious metals and a large amount of cash in a vehicle.

FIC analysis shed light on the financial profile of the individual arrested, including regular visits to casinos, where he bought chips that were used and later exchanged to pay syndicate members supplying him with these commodities. Relevant accounts were monitored, revealing other beneficiaries of the scheme for the SAPS to investigate.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	ELECTRICITY FRAUD

Electricity voucher fraud

As part of a task team, the FIC helped the Hawks and a state utility to investigate the theft of equipment which was used in producing fraudulent prepaid electricity vouchers.

FIC analysis of various bank accounts and cash deposits identified the beneficiaries of this scheme. A person was arrested on 597 charges of fraud and money laundering.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	PROCUREMENT FRAUD AND DUPLICATE PAYMENTS

Municipal theft and fraud

A financial clerk working at a municipality responsible for executing payments to service providers, was a person of interest in a FIC investigation.

It was alleged that the subject made duplicate payments to the municipality's service providers. The municipal manager picked up on a payment discrepancy and reported the suspected unlawful activity. The SAPS and the AFU asked the FIC to conduct a financial investigation.

The FIC analysed the municipal account to identify the duplicate payments and beneficiaries. It was discovered that duplicate payments were routed to the subject's bank accounts. The accounts were analysed to determine how the proceeds were being used. In the process, various other beneficiary accounts were identified. The FIC identified cash withdrawals, lifestyle spending, funds transferred to a car dealership and to an attorney's account to purchase a property.

The FIC issued a directive to seize R1 268 000 and the AFU obtained a preservation order for the money in the blocked accounts, a residential property to the value of R1 795 000 and a vehicle as well as furniture worth about R620 000.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	FEE MISAPPROPRIATION

Student fees stolen – university employee

The FIC received an STR regarding an employee 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 had 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 FIC's financial intelligence helped the AFU obtain a preservation order for funds in the subject's bank account and movable as well as immovable property.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	SCAMS

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 US 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 sufficient intelligence to issue four additional intervention directives and identified three vehicles bought with some of the criminal proceeds.

The NPA and the AFU obtained preservation orders against nine accounts and three motor vehicles. Co-operation between all stakeholders resulted in the recovery of 93 percent of the stolen funds.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	MARKET VALUE MANIPULATION

Property value manipulation

The FIC was part of a task team with the SAPS to investigate individuals who fraudulently adjusted the market value of properties to the benefit of development companies, resulting in a loss of millions of rands in revenue to local municipalities.

Through its analysis, the FIC identified payments made into municipal employees' personal bank accounts originating from property development companies and other entities. These proceeds were then spent on expensive vehicles and properties.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	TRADE-BASED MONEY LAUNDERING

Import/export corruption ring exposed

Through its analysis of financial information, the FIC helped identify a corruption ring involving public officials colluding with an import/export company operating at ports of entry into South Africa. This syndicate was manipulating import/export documentation for containers arriving at the border from various international jurisdictions.

The FIC's analysis of financial records enabled law enforcement to identify public officials and the export businesses. The FIC also identified the bank accounts being used to receive the proceeds of crime and determined how the money was laundered.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	PROCUREMENT FRAUD

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 the husband's bank account. The funds were then used to buy luxury vehicles and several properties. The money was also used to fund gambling activities and family holidays, and given 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 as well. 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 AFU proceeded to attach or preserve several assets worth millions of rands under the Prevention of Organised Crime Act.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	BANK DETAIL FRAUD

Manipulating bank details

The authorities identified a syndicate and approached the FIC for assistance. The syndicate targeted companies in a neighbouring country that had head offices in South Africa.

The modus operandi was to send targeted companies notifications to inform them of a change in bank account details. Two companies subsequently paid amounts to the new account.

When questioned about outstanding payments, the companies realised that they had been defrauded. The FIC froze the bank accounts, conducted analysis and contributed to statements in support of preservation orders obtained against the funds in the accounts.

In a similar instance, a company that was owed funds by a neighbouring country's post office for the transport of post within South Africa was defrauded when its beneficiary's bank details were changed using a fraudulent letter. Two amounts of R1.45 million and R1.3 million were paid to a fraudulent bank account.

The FIC worked with the foreign law enforcement agency and identified the withdrawal and transfer of the stolen funds. Funds in excess of R1.7 million were secured in the above instance.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	TAX-RELATED CRIME

Undeclared funds in other countries

The FIC became aware of a high-profile South African holding substantial funds and assets in a foreign jurisdiction. The FIC's analysis of financial data revealed that he had failed to declare these funds and assets to the SARS. He was also believed to be holding undeclared assets in a second offshore jurisdiction.

The FIC shared its findings with SARS for further investigation.

MAIN CRIME TYPE	FRAUD AND CORRUPTION
ASSOCIATED CRIME TYPE	CASH SMUGGLING

Millions seized on Mozambique border

On Christmas Day 2015, more than R78 million in cash and a pickup truck were seized following the arrest of two Mozambican nationals at the Lebombo border post.

Mpumalanga's AFU, 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 AFU obtained preservation orders for this cash.

INDICATORS | FRAUD AND CORRUPTION

Mules / Cash smugglers

- Mule networks used via a collection of linked accounts that belong to either a person or a business entity, at times even without the knowledge of the account owner, to move the proceeds of crime.
- High-end goods, assets and properties purchased via attorneys.
- Abuse of businesses and entities e.g. shell company for receipt and distribution of funds.
- Newly opened accounts, with generic shelf company names, suddenly receiving money, followed by immediate disbursing of funds.
- Use of cash and currency such as large cash withdrawals and cross-border transfers
- Dormant accounts receive sudden huge deposits and rapid withdrawals.
- Entity account transactions do not match the client profile.
- Unusual volumes of cash deposited into bank accounts.
- Large deposit of funds followed by almost immediate withdrawal of funds.
- The use of various accounts of high profile individuals.
- The utilisation of more than one bank account.
- Cross-border and foreign transactions.
- Opening of accounts with fraudulent documentation, followed by account control takeovers.
- The prevalence of "trade as" accounts to commit fraud or other financial crimes.
- International funds transfers that are not consistent with the client's business.
- The money used to fund gambling activities.
- Purchase of investment products.

Trust accounts and/or trust attorneys

- Unusual payments to an attorney's trust account.
- Transfers from the attorney's trust account into attorney's personal account.
- Routing of funds via attorneys' trust accounts to purchase high-end goods, luxury properties and vehicles.

Purchasing patterns

- The purchase of high value items and assets including vehicles and/or property.
- Purchase of investment/ insurance products.
- Duplicate account payment information and beneficiaries.
- Over-payment for services or products.
- Regular purchase and sale of gambling chips under the threshold, to prevent disclosure.
- Living expenses not matching client profile.

Tax

- Company account is new but receives tax refunds and value-added tax return payments.
- Tax fraud.

General

- Criminal activity related to fraud generates money that generally needs to be laundered, so where fraud is detected, money laundering will be present.
- Involvement in investments promising unrealistically high returns over a short period of time.
- Numerous cash deposits not followed by the agreed investment.
- Funds diverted to sham companies.
- Registration of businesses and establishment of business accounts using names similar to those of well-known trading enterprises.
- Using trademarks similar to those of another person or already existing entity.
- Shell entities with names similar to legitimate firms previously paid by government.
- Hiding of benefits via friends, family and/or close associates.
- Fronting to ensure contract awards.
- Price inflation to sponsor illicit benefit payments.
- Fraudulent payments routed close to festive periods or public holidays.

MONEY LAUNDERING

MAIN CRIME TYPE	MONEY LAUNDERING
ASSOCIATED CRIME TYPE	ENVIRONMENTAL CRIME

Park rangers in rhino poaching-related offences

Two national park rangers were arrested for offences relating to rhino poaching.

The FIC supported the operation and provided the AFU with financial intelligence to enable it to apply for preservation orders.

The FIC identified various cash deposits and electronic transfers made into the rangers' bank accounts, which often exceeded the cash threshold limit. One of the perpetrators bought various vehicles in cash using the proceeds.

MAIN CRIME TYPE	MONEY LAUNDERING
ASSOCIATED CRIME TYPE	FERROUS AND NON-FERROUS METALS CRIME

Syndicate, scrap metal dealer

Law enforcement authorities approached the FIC for assistance in their investigation of a suspected copper theft syndicate. About half a billion rand's worth of copper is stolen each year and, according to the South African Chamber of Commerce and Industry, close to R5 billion is spent each year on repairing the damage caused and replacing the stolen copper.

During the course of the investigation, the FIC discovered that a scrap metal dealer and the syndicate were transacting only in cash to avoid detection and to subvert anti-money laundering controls.

Law enforcement authorities negotiated with the scrap metal dealer, who agreed to pay the syndicate through electronic transfers to their bank accounts. This allowed the FIC to identify the flow of funds and the key people involved in the syndicate, as well as the assets they had acquired. The funds and assets were later seized and forfeited to the state.

MAIN CRIME TYPE	MONEY LAUNDERING
ASSOCIATED CRIME TYPE	PRECIOUS METALS AND STONES CRIME

Illegal diamonds

The FIC used financial information to identify role players in the illicit diamond trade.

The FIC tracked the flow of the proceeds through several bank accounts in support of applications by the AFU in terms of the Prevention of Organised Crime Act, enabling the identification of the subjects through their association in various companies.

During the operation, 29 subjects were arrested and cash to the value of R7 million was seized. Preservation and restraining orders to the value of R50 million were obtained against the subjects.

MAIN CRIME TYPE	MONEY LAUNDERING
ASSOCIATED CRIME TYPE	ENVIRONMENTAL CRIME

Rhino horn smuggling

Transnational organised crime has increasingly targeted South Africa's natural resources, including wildlife. In particular, the targeting and smuggling of rhino horns has escalated to unprecedented levels in recent years.

The FIC and law enforcement agencies have adopted a multi-agency approach in dealing with the rhino horn trade. In one instance, the FIC followed the illicit flow of funds to a key individual and identified bank accounts that were part of the operation.

Armed with this information, the FIC and law enforcement agencies obtained a directive to preserve and seize R190 000.

MAIN CRIME TYPE	MONEY LAUNDERING
ASSOCIATED CRIME TYPE	ENVIRONMENTAL CRIME

Following the money to find rhino poachers

A news network broadcast an investigative documentary where they exposed persons they believed to be involved in the illegal rhino horn trade. This led to the FIC's involvement in assisting the Hawks in its investigations.

The FIC provided financial intelligence on foreign nationals involved in the syndicate. It was able to identify the methods being used to launder the proceeds of rhino horn trade, which included the use of cash deposits, international fund transfers and electronic transfers, often through the accounts of third parties. The syndicate also used the money to buy cars and immediately changed the motor vehicle ownership.

INDICATORS | MONEY LAUNDERING

- Flow of funds between various accounts. Funds are deposited into the account at various locations in South Africa.
- Request a secondary account card to be issued, which is given to another person.
- Deposits are followed almost immediately by withdrawals overseas.
- In some instances, South Africans surrender their accounts to foreign nationals for a fee.
- Some accounts, opened in the name of a minor, are used by the guardian and their associates.
- Purchase of high value assets and lifestyle expenses.
- Financial transactions not consistent with the account or client profile.
- Account operated by someone other than the owner.
- Cash payments for funds transfers.
- Co-mingling of illicit funds with legitimate sources of income.
- Company account used for personal use.
- Frequent cash deposits made over a short period of time.
- Use of several accounts belonging to entities and individuals.
- High volume of cash transactions.
- Funds were used to buy luxury vehicles and several properties.
- Financial transactions not consistent with the account or client profile.

DRUG MANUFACTURING AND TRAFFICKING

MAIN CRIME TYPE	DRUG MANUFACTURING AND TRAFFICKING
ASSOCIATED CRIME TYPE	CROSS-BORDER TRAFFICKING

Drug manufacturing syndicate

The FIC and the SAPS conducted a joint investigation into a drug manufacturing and trafficking syndicate. The FIC collected, analysed and provided financial intelligence relating to bank accounts and transactions linked to subjects of the investigation, including cross-border transactions.

Through the use of STR information and detailed analysis of transactions, the FIC was able to identify and link additional subjects to those already under investigation. Analysis revealed that a high value property was purchased and used to manufacture Mandrax. The title holder of the property, a naturalised citizen, was virtually absent from public databases. The only reference to this individual was the initial credit check performed by the financial institution involved in financing the property deal.

Analysis of transactional records revealed regular cash deposits soon followed by withdrawals. Another identified account reflected large cash deposits, with some funds frequently being transferred to a travel agency. One of the entities investigated had a business account that did not reflect any business transaction but which showed deposits followed by immediate withdrawals and transfers to other accounts.

The subjects were convicted of drug manufacturing and distribution, as well as money laundering. Preservation and forfeiture orders were obtained and the state confiscated drugs valued at R112 million, drug manufacturing equipment worth R10 million, and properties and assets worth R3.7 million.

MAIN CRIME TYPE	TRAFFICKING
ASSOCIATED CRIME TYPE	ORGAN SMUGGLING

Foreign national nabbed for mutilation

FIC was approached by a law enforcement agency during 2015 to assist in investigating allegations of a foreign national's involvement in female genital mutilation.

The FIC identified a banking relationship between the subject and a banking institution, as well as various transactions of interest. It identified:

- Personal and business bank accounts linked to the same individuals
- Funds transferred from foreign jurisdictions
- Multiple cross-border payments via the banking institution's international banking division
- Various historical CTRs and cross-border transactions

The FIC supported the multi-agency investigation over a period of over 24 months, which culminated in the subject being sentenced in March 2018 to two life imprisonment terms for rape and conspiracy to commit murder. He was also given a fine of R5 000 or six month's imprisonment for providing false information in order to remain in South Africa.

MAIN CRIME TYPE	HUMAN TRAFFICKING
ASSOCIATED CRIME TYPE	SEX SLAVES

Trafficking Thai women

The FIC was asked to assist with an investigation involving women of Thai origin entering South Africa illegally to work in a brothel. Situated in Durban North, the brothel was allegedly disguised as a bed-and-breakfast establishment and run by a Community Policing Forum member and his wife, who was also of Thai origin. Following a tip-off, law enforcement authorities raided the property and arrested the couple and 12 Thai women.

Between 2007 and 2017, 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 that period. This information supported the allegations against the subject.

MAIN CRIME TYPE	DRUG MANUFACTURING AND TRAFFICKING
ASSOCIATED CRIME TYPE	DRUG SYNDICATES

Uncovering hydroponic cannabis syndicates

The FIC supported a law enforcement investigation between 2014 and 2017 that resulted in the successful pursuit and capture of a large syndicate on charges relating to murder, attempted murder, kidnapping, VAT fraud, and cloning of stolen motor vehicles. The SARS and the AFU 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.

During 2017/18, the FIC identified individuals running hydroponic operations in the North West, Gauteng and the Free State provinces. Four of these illicit operations were successfully disrupted and the subjects were arrested. Equipment valued at approximately R5 million was seized.

The FIC's analysis of financial data helped identify various properties purchased with the suspected proceeds of crime in the KwaZulu-Natal South Coast region. In early 2018, the FIC provided a law enforcement agency with information that 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.

INDICATORS | DRUG MANUFACTURING AND TRAFFICKING

- Multiple foreign, cross-border and/or domestic transactions.
- Fraudulent documentation such as visas used.
- Purchase of investment products.
- Transacting pattern inconsistent with client's profile. The purchase of high value assets and lifestyle expenses.
- High volume of transactions.
- Procurement of high value assets via attorneys.
- The use of family members' accounts.
- The use of multiple bank accounts to hide proceeds of crime.
- Structuring of the funds into bank accounts by making cash deposits at different branches
- Company account used for personal use.
- Early settlement of asset-based finance accounts.
- VAT fraud.
- Syndicates display similar indicators as those involved in money laundering.
- Money laundering is the keystone of organised crime, thus the same indicators are applicable.
- Cash payments for funds transfers.
- Co-mingling of illicit funds with legitimate sources of income.
- Co-mingling of transactions on personal and business accounts.
- Frequent cash deposits and withdrawals over a short period of time.

ENVIRONMENTAL CRIME

Explanation: Environmental crime

There has been a marked increase in the number of reports identifying environmental crimes:

- With the market value of rhino horn soaring to about $65 000 or R520 000 a kilogram, rhino horn is more expensive than gold or platinum, generating substantial amounts of ill-gotten gains that attract STRs.
- Intelligence gathered by the FIC contributed to the discovery that rhino poaching involves a range of actors, including game rangers, veterinarians, professional hunters and farmers that conspire with criminal networks.
- FIC reporting streams also suggest continued abuse of marine resources. The FIC's information and analysis has helped to reveal a complex web of interests at work in abalone poaching, including the collusion of local fishing communities, with overseas criminals.

MAIN CRIME TYPE	ENVIRONMENTAL CRIME
ASSOCIATED CRIME TYPE	RHINO POACHING

Rhino poaching

As part of a government task team, the FIC identified bank accounts, and traced assets belonging to a rhino poaching syndicate. After receiving STRs on accounts belonging to individuals linked to the rhino poaching syndicate, the FIC analysed transactional records that revealed large amounts of money being deposited into their accounts. This money was then used to purchase a high value property and vehicles.

The FIC's financial intelligence reports were forwarded to law enforcement agencies, which prepared criminal charges for possession of rhino horns and elephant tusks, as well as offences under the Convention on International Trade in Endangered Species of Wild Fauna and Flora.

The state obtained preservation and forfeiture orders for a residential property valued at more than R1.4 million, foreign currency to the value of R3 million and vehicles to the value of R950 000. Ten rhino horns and one elephant tusk, with a combined market value of R6 million, were seized and used as evidence in court.

MAIN CRIME TYPE	ENVIRONMENTAL CRIME
ASSOCIATED CRIME TYPE	RHINO POACHING

Research to boost fight against wildlife trafficking

The FIC worked with a counterpart from the United States of America to conduct research on the illegal trade in rhino horn and ivory. As a result of its research, the FIC gained a better understanding of the indicators associated with the illicit flow of proceeds related to this crime.

These indicators identified by both jurisdictions have been shared with relevant institutions that have reporting obligations. More focused reporting will ultimately help law enforcement agencies in a range of jurisdictions and boost the domestic effort to stop rhino poaching.

MAIN CRIME TYPE	ENVIRONMENTAL CRIME
ASSOCIATED CRIME TYPE	RHINO POACHING

A person under investigation for rhino poaching was arrested while in possession of R400 000 in cash and hunting equipment.

He claimed that the cash came from a policy payout. A FIC investigation showed that a policy payout had taken place but, for a considerably lower amount more than a year before the arrest. Using this information, the AFU obtained a preservation order for the monies to be seized.

INDICATORS | ENVIRONMENTAL CRIME

Environmental crime is linked to money laundering and thus similar indicators operate as follows:

- Purchase of high value assets, luxury vehicles and several properties and lifestyle expenses.
- Purchase of investment and/or insurance products.
- Financial transactions not consistent with the account or client profile.
- Account operated by someone other than the owner.
- Cash payments for funds transfers.
- Co-mingling of illicit funds with legitimate sources of income.
- Company account used for personal use.
- Frequent cash deposits made over a short period of time.
- Use of several accounts belonging to entities and individuals.
- High volume of cash transactions.
- Financial transactions not consistent with the account or client profile.

PRECIOUS METALS AND STONES

CRIME TYPE	PRECIOUS METALS AND STONES
ASSOCIATED CRIME TYPE	GOLD SMUGGLING

Illegal trade in precious metals

The FIC and the SAPS conducted an investigation into illegal gold smuggling. The suspected role players were linked to several legal entities and were all involved in the gold business. The FIC identified and traced the bank accounts of the subjects, including all their financial transactions, assets and foreign accounts.

The FIC's analysis uncovered suspicious deposits and withdrawals of large sums, including transfers from business to personal accounts belonging to syndicate members. Analysis of financial statements identified funds being transferred to attorneys, who in turn purchased high-end properties and vehicles on behalf of syndicate members. With the help of its international counterparts, the FIC determined that some of the syndicate members held offshore bank accounts and owned properties in other jurisdictions.

The FIC's financial intelligence report resulted in the arrest of syndicate members and the confiscation of assets worth about R6.8 million.

MAIN CRIME TYPE	PRECIOUS METALS AND STONES
ASSOCIATED CRIME TYPE	ZAMA ZAMAS

The Zama Zamas

The FIC helped a law enforcement agency identify several syndicate members in Virginia and Welkom in the Free State who were obtaining gold-bearing material from the Zama Zamas (illegal miners) engaged in using their own technique to process the gold. This gold was being sold to various refineries in Gauteng.

The FIC conducted analysis and confirmed that the subjects made small regular payments to various persons in the Free State to pay the low level operators in the syndicate, "runners", who acted as intermediaries between the illegal miners and the refineries.

The law enforcement investigation team located the runners and the premises they used to process the gold-bearing material. A search and seizure warrant led to the authorities confiscating equipment and two gold nuggets. Four subjects were arrested.

INDICATORS | PRECIOUS METALS AND STONES

- Use of attorneys to launder proceeds of crime through purchase of high-end goods.
- Use of third party accounts such as, for example that of a spouse, to hide proceeds of crime.
- Opening of offshore accounts in tax havens.
- Use of personal accounts to move funds generated from business transactions.
- Transacting pattern inconsistent with client's profile.
- Inter-provincial cash deposits.

NOTES:

NOTES:

Financial
Intelligence Centre

www.fic.gov.za