Financial
Intelligence Centre

CASE STUDIES AND INDICATORS

2017–2022 COLLECTION

VISION

To be a highly capable public entity that produces financial intelligence for making South Africa's financial system intolerant to abuse.

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, timeous 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 who are committed to the highest standards of excellence and professional service delivery in the fulfilment of their responsibilities.

THIS PUBLICATION

This publication is a compilation of case studies and indicators produced by the Financial Intelligence Centre (FIC) between 2017 and 2022. The case studies are arranged according to crime type. The indicators are by no means an exhaustive list but, are included to assist in identifying criminal activity.

It is important to note that provisions in the Financial Intelligence Centre Act, 2001 (Act 38 of 2001), oblige the FIC to keep confidential information at its disposal. The FIC may only disclose information or intelligence under certain circumstances to mandated entities, and stakeholders. For this reason, all case studies in this publication have been sanitised.

Central to the production of the case studies has been the regulatory reports submitted by accountable and reporting institutions, and other business and the collaboration between the FIC and its competent authority partners. Regulatory reports are the basis upon which the FIC produces its financial intelligence reports.

CONTENTS

THIS PUBLICATION 2

GLOSSARY 5

INTRODUCTION 8

THE FIC'S ROLE AND FUNCTION 10

REGULATORY REPORTING TYPES 11

THE SIGNIFICANCE OF REGULATORY REPORTS 12

THE VALUE OF CASE STUDIES, TYPOLOGIES AND INDICATORS 13

WHAT IS MONEY LAUNDERING? 14

MONEY LAUNDERING INDICATORS 15

CASE STUDIES AND INDICATORS 17

CORRUPTION 17

- Foreign assistance for information 17
- State-owned enterprises procurement fraud 18

COVID-19 corruption and money laundering 18

CYBERCRIME 19

- Exchange control contraventions using crypto assets 19
- Online pyramid scheme collapses 20

ENVIRONMENTAL CRIME 25

THE ZAMA ZAMAS 27

FRAUD 28

- Cracking a cryptocurrency Ponzi scheme 28
- Forex investment Ponzi scheme 28
- Ponzi scheme uncovered in coal logistics investment scheme 29

Building on a pyramid (scheme) 29
Thousands conned 29
VAT fraudster caught 30
E-mail fraud scams US company 31
Working with Denmark to track stolen funds 31
Tax fraud 32
Road Accident Fund fraud 32
Employer defrauded of R10 million 32
Stolen school sanitation funds recovered 33
Business e-mail compromise using crypto asset service providers 33
Fraudulent workman's compensation fund claims 34
Unemployment insurance fraud 35
Business e-mail compromise scam 35
Politically exposed person benefiting from government contracts 35
Personal protection equipment fraud 36
Load shedding offloads fraudulent funds 37
ILLEGAL NARCOTICS 43
Uncovering hydroponic cannabis syndicates 43
Crunch time for illegal drug and steroid dealers 44
KIDNAPPING 46
Kidnap victim goes home 46
MODERN SLAVERY AND HUMAN TRAFFICKING 46
Trafficking Thai women 46
Human trafficking and money laundering 47
ROBBERY 47
Cash in transit money found 47

GLOSSARY

Accountable institutions	Financial and non-financial institutions and sectors, as listed in Schedule 1 in the FIC Act, identified as vulnerable to being used for money laundering purposes. Note: Since 2022 changes were implemented in the FIC Act Schedules. There are no longer items listed in Schedule 3 to the FIC Act.
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 countering the financing of terrorism
ATM	Automatic teller machine
Competent authorities	Includes authorities such as the National Prosecuting Authority (NPA), South African Police Service (SAPS), Asset Forfeiture Unit (AFU), Special Investigating Unit (SIU), Independent Police Investigative Directorate (IPID), Office of the Public Protector (OPP), intelligence services and supervisory bodies. Also includes foreign partner financial intelligence units.
Crypto arbitrage	The simultaneous buying and selling of securities, currency, or commodities in different markets or in derivative forms to take advantage of differing prices for the same asset. Crypto asset service provider – A person who carries on the business of one or more of the following activities or operations for or on behalf of a client: • Exchanging a crypto asset for a fiat currency or vice versa • Exchanging one form of crypto asset for another • Conducting a transaction that moves a crypto asset from one crypto asset address or account to another • Safekeeping or administration of a crypto asset or an instrument enabling control over a crypto asset

	• Participation in and provision of financial services related to an issuer's offer or sale of a crypto asset.
CTR	Cash threshold report on transactions of R24 999.99 and above. Note: With effect from 14 November 2022, the threshold was increased to R49 999.99. Case studies in this publication pertaining to CTRs, are based on the threshold as applied prior to November 2022.
FATF	Financial Action Task Force
Indicators	Methods used by criminals in executing their crimes
ML/TF	Money laundering and terrorist financing
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.
Peel chain	A technique to launder a large amount of crypto currency through a lengthy series of minor transactions. A small portion is 'peeled' from the subject's address in a low-value transfer. These incremental outputs are often directed to exchanges where they can be converted to fiat currency or other assets. The subject's remaining, unspent transaction output (UTXO) passes to a new change address and the process is repeated. Due to the small amounts of each individual transfer, outputs from the peel chain are less likely to raise red flags for AML compliance at virtual asset exchanges or trigger mandatory reporting to tax and regulatory authorities.
Ponzi scheme	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.
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.
Pyramid scheme	A scheme where individuals are recruited to participate. Return on investment is dependent upon the subsequent recruitment of investors. Pay outs to early investors make it seem like to be a worthwhile initiative.
Regulatory reports to the FIC	Reports required to be submitted to the FIC by accountable institutions. These include cash threshold, suspicious and unusual transaction and terrorist property reports. All businesses, including accountable institutions are required to submit reports on suspicious and unusual transactions. New reporting streams came into effect post 2022.
SAMLIT	South African Anti-Money Laundering Integrated Task Force
SAPS	South African Police Service
SARB	South African Reserve Bank
Section 27	A section in the FIC Act which authorises 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	A section in the FIC Act which allows the FIC to instruct an institution, an accountable institution 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 necessary inquiries concerning the transaction and, where necessary, to inform and advise an investigating authority or the National Director of Public Prosecutions.
STR	Suspicious and unusual transaction report
Tax evasion	Illegal, non-payment or under-payment of tax

INTRODUCTION

The FIC produces typologies and indicators on existing, identified and emerging methods criminals use to launder their money through the financial system, or to raise funds for the financing of terrorism and related activities.

The selection of case studies, typologies and indicators in this publication illustrates the significance of the collaborative relationship between the FIC and its partners, and their use of the financial intelligence produced by the FIC. The case studies also provide insight on financial crimes uncovered during the five years covered in this publication.

The banking sector is at the coalface of the transactional environment and is by far the largest contributor of suspicious and unusual transaction reports (STRs) to the FIC.

These and other regulatory reports, and the wealth of information they contain, are the building blocks for the interpretation and analysis the FIC conducts to produce financial intelligence. In turn, this financial intelligence is used by law enforcement and other competent authorities for their investigations, prosecutions, applications for forfeiture and restraint of criminal assets.

The establishment of a public-private partnership, the South African Anti-Money Laundering Integrated Task Force (SAMLIT), between the banking sector and regulatory authorities in December 2019 has helped augment understanding the transaction environment in criminal activity.

SAMLIT identifies specific types of behaviours and activities associated with different types of crimes through the establishment of expert working groups (EWGs) . Tactical operations group (TOGs) address specific financial crime investigations by gathering and supplying information timeously to law enforcement and prosecutorial authorities via the Fusion Centre.

Some of the case studies featured are indicative of the impact of the public-private partnership working in concert with the FIC-led Fusion Centre. The

latter is a public-public collaboration bringing together public law enforcement, intelligence and criminal justice investigative bodies.

The purpose of this collection of case studies, typologies and indicators to help government, relevant business sectors and other stakeholders better understand and identify the risks they face and to assist with developing effective strategies to address those threats.

In addition, typologies assist the FIC in implementing effective strategies to provide law enforcement agencies with information they can use for their investigations and prosecutions in money laundering (ML) and terrorist financing (TF) cases, as well as design and implement effective preventive measures.

These indicators are intended to assist with identifying instances of suspicious and unusual transactions and activity. It is hoped that the featured case studies and indicators will raise levels of risk awareness and assist business in adopting mitigation measures such as implementing a risk-based approach and stimulate the submission of detailed suspicious and unusual transaction and other regulatory reports to the FIC.

THE FIC'S ROLE AND FUNCTION

As South Africa's financial intelligence unit, the FIC is the only government entity authorised to receive transaction and related data from financial and non-financial institutions.

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, and assist in combating money laundering and terrorist financing (ML and TF) and related activities.

The FIC Act obliges certain financial and non-financial institutions – listed in the Act as accountable institutions – to submit regulatory reports to the FIC. Before regulatory reports can be submitted to the FIC, however, accountable institutions must first register with the FIC. All business, not only accountable institutions, is required to submit reports on transactions known or thought to be suspicious or unusual.

In addition, the FIC has the power to block or freeze funds that are suspected to be the proceeds of crime. It can use a section 34 directive to instruct an institution not to proceed with a transaction for a period of 10 days.

A section 34 request provides the FIC with a mechanism to make the necessary enquiries concerning transactions and, where necessary, to inform and advise an investigating authority or the National Director of Public Prosecutions. This allows law enforcement time to conduct further investigations and helps prevents criminals from dissipating funds.

The FIC also shares financial intelligence with the AFU, which can seize and take control of the funds if necessary. As part of its role in administering the FIC Act, the FIC provides guidance and oversight on the FIC Act to accountable institutions and supervisory bodies. This is to ensure optimal awareness and compliance with the requirements of the FIC Act.

REGULATORY REPORTING TYPES

Information in regulatory reports can be indicators of illicit funds being generated, and they can help enrich the content of the FIC's financial intelligence reports.

The regulatory reporting streams include:

Suspicious and unusual transaction reports, on transactions which seem unusual and suspect.

Cash threshold reports on inbound and outgoing cash transactions of R50 000 and more.

Terrorist property reports on transactions which may be linked to terrorist activity or terrorist organisations.

Recently, reporting on cross-border electronic funds transfers, IFTRs (international funds transfer reports) was added as a new regulatory reporting stream for institutions authorised to conduct such incoming and outbound transactions. Case studies and indicators related to IFTRs are not included in this publication.

Regulatory reports are essential to South Africa's system for combating money laundering and countering the financing of terrorism and proliferation.

SIGNIFICANCE OF REGULATORY REPORTS

Using information in regulatory reports and other available data, the FIC applies the follow the money principle to identify and trace possible proceeds of crime or illicit transactions, and to develop financial intelligence reports.

The FIC interprets and analyses this information and data to develop strategic intelligence products that it shares upon request or proactively with domestic and foreign law enforcement and investigative agencies. These authorities are able to use the intelligence products for their investigations, prosecutions applications for asset forfeiture, and other follow up actions in pursuit of combating financial crime. Through their follow up work, they are able to convert the intelligence into evidence and bring to justice those who commit crime. The FIC does not itself conduct investigations or prosecutions.

With regulatory reports being the cornerstone upon which financial intelligence is produced, by extension the institutions and businesses that file regulatory reports with the FIC are intrinsic to assisting in the fight against financial crime. For this reason, registration and reporting by accountable institutions and other business is critical in the fight against financial crime.

Each case study in this publication, is indicative of how the FIC has shared its financial intelligence, proactively or upon request, with one or more of the agencies and institutions listed below:

Asset Forfeiture Unit (AFU)	Special Investigating Unit (SIU)
Department of Forestry, Fisheries and the Environment (DFFE)	South African Police Service (SAPS)
Directorate for Priority Crime Investigation (DPCI)	South African Reserve Bank (SARB)
Financial Sector Conduct Authority (FSCA)	South African Revenue Service (SARS)
Office of the Public Protector (OPP)	National Prosecuting Authority (NPA)

SIGNIFICANCE OF CASE STUDIES, TYPOLOGIES, AND INDICATORS

The case studies illustrate the value of timeous regulatory reporting in depriving criminals of the profits from illicit activities.

The regulatory reports are central to the FIC's analysis and the resulting financial intelligence supports law enforcement and other government authorities in their investigations involving a range of different types of financial crime.

Over the past five years, as shown below, most proactive and reactive reports produced have been related to fraud, followed by tax-related crime, narcotics, money laundering and corruption.

The FIC's analysis and reports revealed that the complexities involved in such crimes are constantly evolving as criminals find new ways to conduct their unlawful activities. It is therefore important that AML and CFT compliance officers, business, sectors, and supervisory bodies stay abreast of the latest typologies and indicators that are relevant to them.

Intelligence reports produced on specific crime types	2017/18		2018/19		2019/20		2020/21		2021/22		Total
	P	R	P	R	P	R	P	R	P	R	
Fraud	403	670	183	372	247	477	271	685	124	633	4 065
Tax crimes	621	295	330	203	139	176	317	95	73	69	2 317
Bribery and corruption	23	216	122	363	84	285	105	253	48	369	1 868
Narcotics	39	302	22	245	6	270	11	210	7	155	1 267
Money laundering	149	164	122	63	105	92	191	88	387	213	1 574

P: Proactive | **R**: Reactive

WHAT IS MONEY LAUNDERING?

The primary intention of money laundering activities is to transform illicit monies into legitimate funds. This is done by introducing criminal assets into the financial system – changing money from 'dirty' to 'clean'. Where money is laundered successfully, criminals can have full control over their proceeds in the financial system. To acquire their proceeds, criminals may conduct a wide range of offences from petty to more serious crimes.

Once the proceeds are in the possession of the criminal, to launder their money they integrate it into the financial system through, among other methods:

- The purchasing of high-end goods such as property or motor vehicles
- Establishing shell companies
- Moving the money transnationally.

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

THREE STAGES OF MONEY LAUNDERING

Ways criminals make their money

❶ PLACEMENT STAGE

MOVE DIRTY MONEY INTO THE FINANCIAL SYSTEM

The intention is to use legal and illegal activities to convert proceeds into usable products.
E.g. Move via financial instruments such as bank accounts or insurance products.

❷ LAYERING STAGE

CREATE DISTANCE BETWEEN SELF AND ILLICIT PROCEEDS

To create anonymity – the source (criminal activity) of illicit proceeds cannot be linked to self.
E.g. Criminals create complex layers of transactions making it difficult to trace or to link money back to the original criminal activity.

❸ INTEGRATION STAGE

MOVE DIRTY MONEY INTO THE FINANCIAL SYSTEM

The intention is to use legal and illegal activities to convert proceeds into usable products
E.g. Move via financial instruments such as bank accounts or insurance products.

MONEY LAUNDERING INDICATORS

- Acquisition of high-value assets (expensive property and/or motor vehicles) via third parties
- Dormant accounts receiving sudden huge deposits and rapid withdrawals being made.
- Concealment within company structures or with relatives (family members) – using business ventures as a front
- Structuring funds into accounts by making cash deposits at different branches of banks so as to avoid raising suspicions
- Use of third parties' accounts to hide proceeds of crime (e.g. spouses' accounts)
- Large cash deposits into accounts and rapid withdrawals
- Change of account behaviour without explanation
- Early settlement of ABF (asset-based finance) accounts
- Transacting pattern inconsistent with client's profile
- Rapid movement of funds through multiple accounts

- Cross-border and national financial flows through couriers
- Cash purchases of high-value properties or motor vehicles
- Frequent cross-border travel
- Regular travel to high-risk countries (tax or financial secrecy havens or countries known to support terrorist activities)
- Regular cash deposits below the FIC Act CTR threshold to the same person or different individuals
- Cash deposits below FIC Act reporting threshold to the individual's different bank accounts
- Regular third-party cash payments into accounts and money quickly withdrawn by the recipient
- Formal networks of money transfer services for cross-border transactions such as Hello Paisa, MoneyGram, Western Union, Mukuru, or informal networks such as Hawala, a system based on trust to transfer and receive transactions etc.
- Regular cash deposits via retailers' money market till points
- Widespread use of cash in the informal sector
- Small, medium and micro enterprises registered or unregistered with the Companies and Intellectual Property Commission (CIPC) and in the informal transport industry
- Properties, second-hand and/or new motor vehicles paid for in cash through agents and dealerships that are non-compliant with FIC Act obligations. The focus being on sales and commission versus FIC Act reporting obligations.
- Investments in livestock, which is largely a cash transaction business.

CASE STUDIES AND INDICATORS

CORRUPTION

Crime in neighbouring country

Collaborating to uncover corruption

The FIC received a request from a neighbouring country's financial intelligence unit for information regarding the alleged misappropriation of funds from a state-owned entity in that country. The funds were believed to have been transferred to South Africa and to involve politically exposed or prominent influential individuals.

The FIC established that the subjects had purchased various moveable assets in South Africa to the value of about R20 million, as well as a number of properties. The FIC subsequently met with the financial intelligence unit to present the results of the analysis and to ask for further details on the matter. The AFU asked the FIC to support a mutual legal assistance process between South Africa and that country to recover the proceeds.

Foreign assistance for information

Associated crime type | **BRIBERY**

A foreign financial intelligence unit requested the FIC's assistance regarding the matter of the former head of an asset management company and his friend and accomplice, a former cabinet minister. Both suspects were accused of corruption related to kickbacks for the award of fishing rights in that country.

The FIC identified two properties in Cape Town and three bank accounts with funds linked to the two individuals. This, as well as requirements for the freezing of funds to be followed by possible preservation, was communicated to the foreign financial intelligence unit.

The FIC provided a financial intelligence report to that financial intelligence unit, and the matter was subsequently closed. The foreign country's police made arrests.

State owned enterprises procurement fraud

Associated crime type | **PROCUREMENT FRAUD**

Working with the SIU, the FIC identified an account that was alleged to have received payments, possibly because of procurement fraud at Eskom.

The FIC issued an intervention on the subject's bank account securing R10.1 million and an affidavit in support of the SIU Special Tribunal order. The Special Tribunal has ordered that more than R10 million held in the bank account be forfeited to the state.

COVID-19 corruption and money laundering

Associated crime type | **TENDER FRAUD AND MONEY LAUNDERING**

Contractors and professional service providers were irregularly appointed during the acquisition and refurbishment of a hospital by the Gauteng Department of Health and the Gauteng Department of Infrastructure Development.

The emergency procurement process was permitted due to the COVID-19 pandemic. However, proper procurement processes had not been followed.

The FIC's analysis of the bank accounts of the identified persons and entities revealed they had received R58.6 million between connected accounts via electronic transfers.

There was possible concealment of funds – probable disguise and dilution of funds between accounts – where funds were spent quickly after receipt.

Personal transactions, high-end goods shopping, large cash withdrawals and deposits were noted. A section 34 FIC Act intervention was issued against two bank accounts, which led to the recovery of R7.9 million. The FIC issued certificate under section 39 of the FIC Act in support of the SIU application at the Special Tribunal issued for a Preservation Order.

Cyber theft in the US

Associated crime type: **THEFT**

The FIC received intelligence from its counterpart in the United States, the Financial Crimes Enforcement Network, indicating that four subjects with links to South Africa may have been implicated in an international cyber theft scheme that had operated between 2014 and 2018.

The scheme involved phishing, spear phishing, hacking and intrusion tactics to gain access to victims' e-mail accounts and funds. The subjects then engaged "mules" in the United States to transfer illicit funds to overseas bank accounts. About US$2 million was identified, but according to the Federal Bureau of Investigation, between US$5 million and US$10 million may have been transferred to various destinations. Intelligence indicated that the subjects may have had several individuals in South Africa assisting with the scheme.

The FIC identified various local bank accounts linked to the subjects and the information was subsequently referred to DPCI.

Exchange control contraventions using crypto assets

Associated crime type: **EXCHANGE CONTROL CONTRAVENTIONS**

The FIC was informed by local crypto asset service providers (CASPs) that various accounts were possibly being used to launder funds.

The FIC subsequently analysed FIAT accounts and crypto assets wallet accounts. The analysis showed that Chinese nationals involved had purchased approximately R460 million worth of crypto assets within a period of six months. The crypto assets were mostly sent to crypto addresses held with foreign CASPs operating in South Africa.

Based on the intelligence provided by the FIC, the SARB was able to block approximately R9 million worth of FIAT currency and about 7.3881012 Bitcoins.

Online pyramid scheme collapses

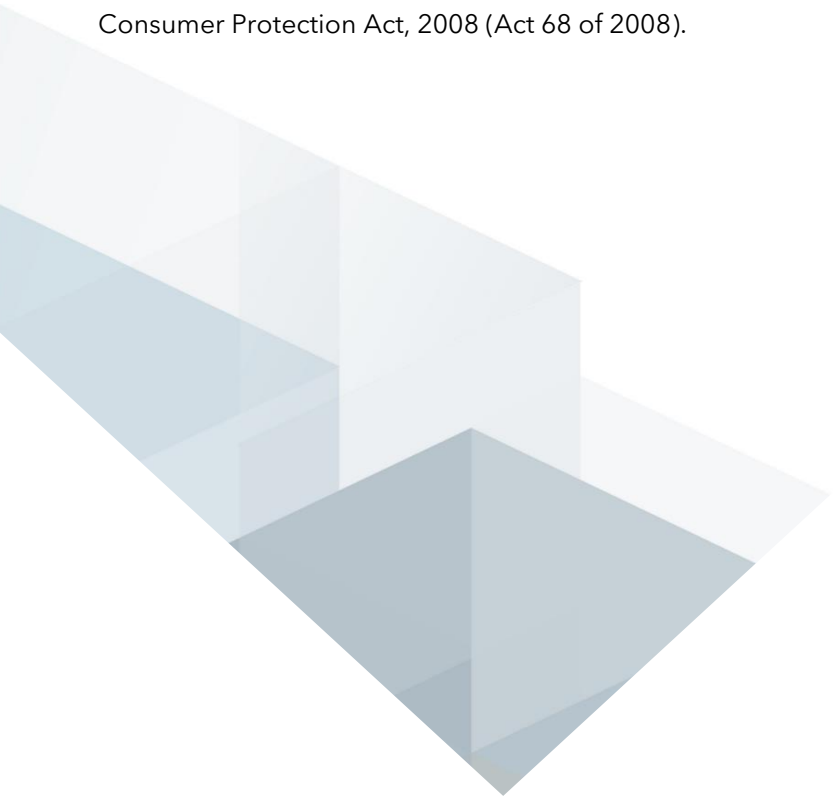
Associated crime type | **PYRAMID SCHEME**

Thanks to regulatory reports filed by financial institutions, negative media coverage, and a request for information from a law enforcement agency, the FIC became aware of a pyramid scheme. Financial intelligence revealed that 21 individuals and one entity were allegedly transacting with the crime proceeds linked to the scheme.

A SAMLIT tactical operations group (TOG) was created to meet and share financial intelligence on the case. The FIC issued directives to secure some R8 million held across 54 bank accounts, which was also subject to two preservation orders by the AFU.

Financial analysis uncovered that multiple credit payments had been received from members of the public and that the funds had been transferred using the subjects' own bank accounts – often among each other.

The scheme was found to be in contravention of section 37(1) of the Consumer Protection Act, 2008 (Act 68 of 2008).



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 transfers of funds followed by immediate withdrawals at ATMs.
- Transactional activity or funds in bank accounts not matching the profile of the client.
- Sudden activity such as large deposits and rapid withdrawals on previously dormant accounts.
- An increase in daily transactions followed by sudden, large withdrawals or transfers.
- Duplication of cards 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.

Crypto assets

- Registering of businesses promoting crypto offerings to the public through websites and social media sites. These businesses close within a short space of time (maximum of two years), claiming their services were compromised. Criminals disappear with the crypto assets and victims are left destitute without recourse.
- Regulatory reports relating to crypto arbitrage are common. The reports highlight clients of a bank who use corporate cash management accounts as a platform to lure potential investors into fictitious offshore investments. To participate in this investment, the client must first acquire a tax clearance certificate in respect of their foreign investment allowance. Once this document is obtained, the client transfers funds of R1 million to the corporate cash management account. The portfolio manager uses the consolidated funds to purchase crypto assets locally at a favourable rate.

Thereafter the assets are arbitraged offshore as an entity investment for the benefit of the portfolio manager. Once the invested funds and profits are returned to South Africa, the portfolio manager returns only the original investment to the client without any interest or profits. The modus operandi of the credit agreements is used by the portfolio manager to bypass SARS tax clearance processes and, to circumvent exchange control regulations to facilitate the flow of money offshore through crypto arbitrage.

- Money launderers can place low outcome bets at online casinos that accept crypto assets. These users will not win large amounts, but they will ultimately obtain legitimate money.
- Prepaid crypto cards also create opportunities for money laundering as they allow criminals to convert "dirty" crypto assets into fiat.
- The use of "peel chain" techniques to launder large amounts of crypto assets through a lengthy series of minor transactions.
- Smurf techniques for splitting funds and depositing those into many bank accounts with funds, which are finally used for buying crypto assets from private sellers who reside in different countries.
- The use of crypto asset ATMs to launder money, especially where those have been installed temporarily, such as in a pop-up store or were combined with events such as sports matches or festivals.
- Payments using crypto assets on websites with known links to illegal activities.
- Participation in an initial coin offering (ICO), which is the equivalent in the crypto currency industry of an initial public offering. Due to their unregulated status and the anonymous nature of the transactions involved, ICOs are attractive for the laundering of money acquired in a criminal manner.
- The use of fake verified accounts where con artists steal crypto, taking advantage of the trust signals on social media platforms, such as blue checkmarks on Twitter. Scammers will create profile pictures that include a blue checkmark or cleverly use the wallpaper to incorporate a blue check placed appropriately for it to appear authentic. Hackers will also use these verified accounts to reply to other high-profile accounts or viral tweets to gain more exposure.
- With a YouTube live scam, fraudsters create a live video (often using stolen content), portraying themselves as some form of authority in crypto asset trading. They would post a link to a "giveaway" in the video's

description, where potential victims will be persuaded to send crypto assets. By using the 'live' feature, the fraudsters avoid YouTube's content review process until the video is over.

- Affiliate scams are incentive programmes where companies pay an affiliate to drive traffic or new subscribers to their site.
- Catfishing: Where a person who sets up a false personal profile on a social networking site for fraudulent or deceptive purposes involving crypto assets.
- Misleading or fake news involving crypto assets. For example, high-profile government officials were used in a phishing and clickbait scam in 2020.
- Crypto currency fraudsters are known to use complex financial instruments to disguise the nature of their transactions to aid in the money laundering process.
- Advertisements using "Bot technology" that provides unrealistic returns on crypto investment proposals, creating an appeal or to lure new users to the crypto asset industry.
- Purportedly using artificial intelligence in trading with unrealistic returns or level of profits every month.
- Potential victims' lack of knowledge on crypto assets make them vulnerable to being scammed.
- The use of trading platforms and accounts, and various trading facilities such as contract for differences and forex derivatives to subvert regulators and regulations across jurisdictions.
- Minimal to no reliance on banks or bank accounts may be used in the placement stage of money laundering, in terms of contributions in FIAT currency.
- Large electronic credit transfers and cash deposits into various accounts linked to the subject, which are rapidly disposed of.
- Large international transfers made to crypto related entities.
- The cross jurisdictional nature of crypto assets makes it vulnerable and harder for law enforcement to rapidly detect, trace and address.
- Inconsistent account turnover.
- Payments made to betting agencies.
- The use of online gambling facilities or networks assist in the layering process.
- Transactional activity involving excessive Bitcoin trading.
- The pooling of investors' crypto assets, obfuscating the origin, nature and purpose of the transactions.

- Conversion of crypto currencies to FIAT currencies and vice versa to add to the layering process and to further disguise the nature and origin of the crypto assets.
- The use of multiple CASPs across the globe, to purchase, place and trade crypto currency.
- Adverse media coverage.
- The use of social media, promotional videos and websites to lure potential victims and to appear legitimate.
- Entity receives crypto currency funds and 'co-spending' with most funds being sent to an online casino.

Rhino horn trafficker busted

Associated crime type | **RHINO HORN TRAFFICKING**

An investigating team asked the FIC to provide information on individuals allegedly involved in illegal trading of rhino horn. The FIC had received several regulatory reports on these individuals.

The subjects, all based in Mpumalanga, were dealing with large amounts of cash, mainly used to recruit people to poach or procure rhino horns. The subjects were later linked to several rhino killings in the Kruger National Park and other national parks. Based on the FIC's financial intelligence, the investigating team conducted surveillance which led to the arrest of the subjects.

Abalone poaching syndicate

Associated crime type | **ABALONE POACHING**

The FIC assisted a law enforcement agency, the NPA and the AFU with an urgent matter relating to investigations into certain officials in a government department. It was alleged that these officials were involved in assisting an abalone poaching syndicate.

The FIC's financial intelligence was used to trace assets, bank accounts and relevant financial information of the implicated officials and syndicate members. As a result, a number of officials were arrested and charged with racketeering, theft, defeating the ends of justice and corruption.

Illegally dealing in cycads

Associated crime type | **CYCAD DEALING**

The DFFE requested the FIC to analyse the accounts of a person who was illegally dealing in cycads. The FIC's analysis showed that the illegal sale of cycads was a trend in the Krugersdorp area in Gauteng. It also revealed that the subject was involved in international trade via financial transactions received into his account from abroad.

Cycads are the oldest living seed plants on the planet with a lineage going back some 340 million years and, according to the International Union for the Conservation of Nature, the world's most threatened living organisms.

Illicit wildlife trade

- The use of cash is still highly prevalent in the trafficking of wildlife and wildlife products.
- High volume of cash transactions – frequent cash deposits made over a short period.
- Methods of payment and laundering become more sophisticated higher up in the supply chain whereas basic cash or barter tends to occur at the lower levels.
- The use of front companies and enablers; many of these businesses appear to be legitimate, but analysis of their transactions point to large incoming flows and show few legitimate business expenses.
- The use of money mules.
- Money flows associated with illegal wildlife trade is often linked to other crimes such as fraudulent documentation or paperwork, trade-based money laundering including over- or under-invoicing or fictitious invoicing, as well as corruption to facilitate the flow of funds into South Africa.
- Financial transactions not consistent with the account or client profile.
- Funds leaving South Africa are predominantly in US or Canadian dollars, Euros or Thai Baht, and are moved out of the country through suspected cash smuggling and money transfer systems.
- Some of the criminals linked to investigations have high volumes of casino transactions.
- Unusual cash deposits and EFTs into the accounts of park rangers and other informers, and unusual cash spending on flashy or expensive items such as cars and houses (or boats in the case of abalone poachers).
- Purchase of investment and/or insurance products.
- The use of the legal wildlife industry to mask illegal trade.
- Cash-in-transit and transport industries feature heavily in illegal wildlife trade.
- EFTs are primarily associated with actors involved higher up in the supply chain.

- The use of gift and payment cards to make payments to level two or three intermediaries.
- Mobile money payments are prominent in the lower levels of the value chain.
- The suspected use of attorney trust accounts – the purchase of properties either through cash or the attorney trust account has been noted.
- The use of casino chips as payment, particularly to intermediaries.

The Zama Zamas

Associated crime type: **ILLEGAL MINING**

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

The FIC conducted analysis and confirmed that the subjects made small regular payments to various people in the Free State to pay the low-level operators or "runners" in the syndicate, 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. The subjects were sentenced to five years imprisonment.

PRECIOUS METALS AND STONES

- Use of attorneys to launder proceeds of crime through purchase of high-end goods.
- Attorneys' trust accounts that receive funds from clients and purchasing high-value assets for clients.
- Use of third-party accounts such as that of a spouse to hide proceeds of crime.
- Suspect withdrawals and deposits of large sums of money into accounts.
- Opening of offshore accounts in tax or financial secrecy havens.
- Flow of funds from accounts to offshore destinations.
- Use of personal accounts to move funds generated from business transactions.

- Transfers of funds between business accounts and personal accounts that are not business related.
- Transacting pattern inconsistent with client's profile.
- Inter-provincial cash deposits.

FRAUD

Cracking a crypto currency Ponzi scheme

Associated crime: **PONZI SCHEME**

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

Forex investment Ponzi scheme

Associated crime: **PONZI SCHEME**

Vulnerable individuals from middle class communities were targeted by an individual who was offering forex investment packages with the promise of returns of up to 700 percent within a three-month period.

Analysis of the entity's bank account transactions reflected a possible Ponzi scheme with approximately R36 million worth of suspicious and unusual transactions. Neither the entity nor the individual was licensed to conduct financial services or receive deposits from the public.

The matter was reported to various authorities including the Financial Sector Conduct Authority (FSCA), DPCI, AFU, SARS and SARB. The AFU secured a preservation order R16 532 944.40.

Ponzi scheme uncovered in coal logistics investment scheme

Associated crime: **PONZI SCHEME**

A logistics company advertised opportunities for investments in the coal logistics business on the internet. The company offered unrealistic returns for investments starting from R65 000 upwards. Investigations revealed that investments to the value of R21 930 110 were deposited in the account, most of which was then transferred to the account of the company's only director.

In terms of a preservation order obtained by the AFU, close to R10 million was frozen and the director was arrested.

Building on a pyramid (scheme)

Associated crime: **PYRAMID SCHEME**

The FIC received a request from the National Consumer Commission and the AFU regarding an entity marketed on social media as a 'building scheme'. The FIC's analysis process, however, deemed it to be a pyramid scheme.

Regulatory reports filed with the FIC identified the subjects and the bank accounts linked to them and the business entity. Analysis revealed that the accounts received multiple payments via numerous debit payments and referenced with the names of individuals.

Balances adding up to R669 246.40, held in seven bank accounts were secured by the FIC issuing directives to block the accounts, and a subsequent request from a public agency led to an additional R714 484.54 being secured. The AFU obtained a forfeiture order during November 2022 and the funds were successfully confiscated.

Thousands conned

Associated crime: **PYRAMID SCHEME**

The FIC was able to identify a pyramid scheme after it received a report that between 4 May and 2 July 2020, a gold business bank account opened on 10 February 2020 had had a total turnover of more than R42 million. Nearly

R40 million of this amount had been deposited through 221 976 individual payments of R180 each.

The sole director also made several payments to another business entity account linked to the sole director. This account was used at various motor vehicle dealerships for the purchase of luxury vehicles. Payment of more than R12 million was made to a major retailer.

Based on its analysis, the FIC supplied the AFU with a confirmatory affidavit setting out its findings that the entity was operating a pyramid scheme in contravention of section 43(2)(b) of the Consumer Protection Act, 2008 (Act 68 of 2008). It also found that a bank account of the director was used to receive and launder the fraud proceeds.

Using section 27A of the FIC Act, the FIC requested bank statements for all the entities and individuals involved in running the scheme. After receiving all the bank documents, the FIC analysed the transactions. It also requested an affidavit from FSCA, which confirmed that the main entity was not authorised to operate as a financial services provider.

The AFU obtained preservation orders against the entity, the director and affected bank accounts. A criminal case was opened.

VAT fraudster caught

Associated crime: **TAX CRIMES**

The FIC assisted the AFU in a case where an employee of a company had defrauded her employer of more than R15 million by colluding with a legitimate supplier of transport services for the company.

Employed as a creditor's clerk, the subject told her company's transport service provider that the employer was purposefully manipulating its invoices to escape input tax liability and save money. She said she would ensure that the value added tax (VAT) was correctly calculated and paid into the supplier's account. However, since the employee was doing this without the employer's knowledge or authority, she asked the service provider to transfer half of the "VAT" amount into her personal account as her share for helping the transport provider retrieve the "VAT" that was due to it. This continued

for several months. By the time the employee was caught she had stolen more than R15 million.

The FIC analysed the employee's accounts and traced assets that had been bought with the funds. Through this process, a large amount of money left in the employee's account was blocked. After the FIC identified several assets that were purchased using the stolen funds, the AFU obtained a restraint order. The assets included immovable property, motor vehicles and other household contents.

E-mail fraud scams United States company

Associated crime | **BUSINESS E-MAIL COMPROMISE**

The FIC received a request for information and assistance in a case involving the defrauding of a company registered in the US.

A company employee received a fraudulent e-mail from an address similar to that of a colleague, instructing him to transfer funds to a bank account for the purchase of a vehicle. The employee transferred R607 000 before realising that the e-mail was fraudulent.

The FIC discovered that part of the funds had already been used and the rest had been transferred to another bank account. After verifying the facts and obtaining the necessary documentation from investigators, the FIC issued an instruction directing the bank not to proceed with any transactions on the two identified accounts, which at the time had a cumulative balance in excess of R500 000. The AFU was granted a preservation order allowing it to seize the funds in these two accounts.

Working with Denmark to track stolen funds

Associated crime | **THEFT**

Denmark's financial intelligence unit, the Money Laundering Secretariat, asked the FIC to provide information on four Danish nationals (a mother and her three adult children). The main subject (the mother) was suspected of defrauding her former employer, the Danish National Board of Social Services. She had been dismissed by that employer and had subsequently fled to South Africa. Through its analysis the FIC identified cash and assets linked to the subject.

Based on the AFU's request, the FIC froze R6.7 million. The unit seized and returned the funds to the Danish government.

Tax fraud

Associated crime | **TAX CRIME**

The FIC was requested to assist SARS with a case relating to a senior manager at a state-owned enterprise. The individual had not declared all his income.

The FIC provided SARS with analysis of the flow of funds from a supplier of the state-owned enterprise to the bank accounts of the senior manager. The senior manager appeared in court during March 2020 on a R30 million tax fraud charge.

Road Accident Fund fraud

The FIC was approached by a law enforcement agency to look into the financial affairs of a lawyer in the Western Cape. The lawyer was being investigated for defrauding clients of third-party claims from the Road Accident Fund (RAF).

Through analysis, it was found that the lawyer had a gambling problem, spending up to R18 million at a single gambling establishment. Bank statements and financial flow analyses showed that he would gamble shortly after RAF payments were made into his trust account. He would also travel throughout South Africa to visit various gambling establishments. His defrauded clients were left out of pocket, with the majority of them receiving no financial benefits at all.

The FIC's intelligence contributed to a successful investigation by the DPCI's Serious Commercial Crime investigation team. The lawyer was subsequently arrested.

Employer defrauded of R10 million

Associate crime | **THEFT**

The FIC received an urgent request for assistance in a matter where it was alleged that the subject had defrauded his employer of more than R10 million. After being confronted about it, the employee absconded from work, and went into hiding.

The FIC analysed eight bank accounts to trace the crime proceeds, leading to five FIC Act intervention orders towards securing a total of R9 502 133.07.

Analysis of the bank records also revealed the subject's hiding spot – an hotel in Gauteng close to the airport. When the subject's hotel room was searched, he was discovered to be deceased. The proceeds of the unlawful activity were recovered by the AFU from bank accounts of the deceased. The funds were forfeited and paid back to the company.

Stolen school sanitation funds recovered

Associated crime | **CORRUPTION**

Acting as a member of the Fusion Centre, the FIC carried out urgent analysis of findings by the SIU on COVID-19 procurement irregularities relating to the sanitisation of schools.

The matter involved an amount of R64 647 635.91 that was irregularly awarded to seven companies for school sanitation, that had never occurred.

During the analysis process, the FIC requested information in terms of the FIC Act and analysed the bank records in conjunction with the allegations made by the SIU and their client.

The resultant financial flow analysis led to tracing the proceeds of the unlawful activity through 15 bank accounts held by identified entities and individuals, prompting the FIC to issue 10 intervention directives to the value of R38 776 335.56.

Flow analyses also noted the purchase of five motor vehicles with a combined value of R4 517 782.40, registered in the names of family members and associates of the perpetrators, meaning that a total value of R43 294 117.96 in unlawful proceeds was recovered by the work of the FIC in conjunction with the other Fusion Centre members.

Business e-mail compromise using crypto asset service providers

Associated crime | **BUSINESS E-MAIL COMPROMISE**

The FIC assisted the AFU with an intervention on alleged proceeds of illegal activities. An e-mail received by an employee of a national government

department was intercepted and a different bank account number was inserted, thus replacing the original bank account number.

The funds were originally intended to pay an entity that was conducting renovations on behalf of the national government department.

Further analysis by the FIC established that the newly provided bank account was in the name of a crypto asset service provider (CASP).

The FIC analysed bank statements and confirmed that the amount was credited to the account. An enquiry, in terms of section 34 of the FIC Act, was issued regarding the destination account. The financial institution confirmed that the amount was credited to the CASP account.

The FIC then contacted the CASP who advised that the amount was transferred to their suspense account due to an incorrect reference used and the funds could not be allocated.

The FIC issued a section 34 intervention against the CASP's account and, in addition, deposed an affidavit in support of a Prevention of Organised Crime Act, 1998 (Act 121 of 1998) (POC Act) preservation order. A preservation order was granted for the full amount.

Fraudulent workman's compensation fund claims

The FIC embarked on a comprehensive and complex analysis of transactions involving Compensation Fund claims over a period of seven years.

SAMLIT members were approached to assist with requests on more than 77 identified accounts. The resulting analysis identified more than 757 beneficiary accounts to which funds have been dispersed, pointing to beneficiaries of the proceeds of the illegal activity. Within this process of analysis SAMLIT members were able to identify funds that were still held in some of the accounts directly linked to the initial fraudulent claims. These transactions took place between 2015 to 2022.

Assistance from SAMLIT members resulted in three successful POC Act preservations being obtained against 15 accounts amounting to R3 398 939.84.

Unemployment insurance fraud

Collaborating in the Fusion Centre, the FIC assisted the AFU in a Department of Labour matter related to fraudulent claims of Unemployment Insurance Fund (UIF) Temporary Employment Relief Scheme (TERS), which was processed and paid to 65 different accounts of recipients in the Eastern Cape amounting to R220 million.

Following the payments, the funds were immediately dispersed to various other accounts. The FIC, with the support of Fusion Centre and SAMLIT members, conducted financial flow analyses, which highlighted the rapid transfer and withdrawal of funds.

The FIC issued 21 section 34 interventions on which preservation orders were obtained to the value of R26 522 265.07.

Complainant defrauded

The FIC received information dated 6 June 2022 relating to an incident that occurred on 11 May 2022, in Jeffreys Bay in the Eastern Cape, whereby a complainant was defrauded of R92 713.75.

The information further indicated that the complainant received an e-mail indicating that he should pay that amount relating to a business transaction into a certain bank account. He had completed that transaction on 10 May.

The complainant later discovered that the account provided to him in an e-mail was not the correct account number of the intended business account. The FIC's enquiries to the bank confirmed that the account received the electronic transfer, and a section 34 directive was issued on an amount of R20 158 which formed part of the proceeds of crime.

Politically exposed person benefiting from government contracts

At the outset of this matter, there were media reports about a politically exposed person benefiting from government tenders related to COVID-19 relief efforts.

Based upon regulatory reports and comprehensive analytical products received from SAMLIT members the FIC, as part of its operational work in the Fusion Centre, assisted the SIU in an alleged irregular communication contract which had been exposed in the media.

Total payments over a nine-month period from the government department to the service provider, linked to a politically influential person, amounted to R150 million.

The FIC conducted financial flow analyses which identified 163 beneficiary bank accounts and payments towards three credit cards from the service provider.

Through this complex analysis process the FIC issued section 34 directives to financial institutions securing R22 million. Using some of the financial flow analysis, the FIC deposed an affidavit in support of a SIU Special Tribunal Order which identified 12 respondents and preserved R22 million. The SIU instituted review proceedings with the aim of recovering the full R150 million.

The FIC traced the funds from the government department to the supplier through 163 second level beneficiary accounts and three credit cards. Forty-four accounts were further analysed to level three, identifying a further 200 third-level beneficiary accounts through 1 422 transactions.

Assisting the AFU, the FIC identified additional assets that were purchased to the value of approximately R6 million through multiple layers of transactions.

Personal protection equipment fraud

SAMLIT and the Fusion Centre worked on a criminal investigation regarding fraud and corruption committed in the awarding of a contract to two companies for the procurement of personal protection equipment.

Analysis of the financial information received, indicated that all payments made by a government department were deemed unlawful and represented the proceeds of unlawful activities.

In collaboration with the Fusion Centre the FIC conducted financial flow analysis, tracing the proceeds of the illegal activity.

The SIU recovered R26.5 million in cash based on the financial information shared through SAMLIT.

Government buildings not sanitised

In a matter of fraudulent allocation of tenders and lack of provision of services related to COVID-19 sanitation of government buildings, the FIC supported the SIU by analysing various interlinked groups of company accounts and identified the proceeds of the crime.

The analysis consisted of four groups, consisting of 46 companies, and more than 500 accounts. The companies were found to be interlinked and shared the proceeds of the tenders among the entities, individuals, and family members.

The analysis and subsequent interventions and AFU Special Tribunal Order obtained resulted in 26 accounts being frozen securing R65 million.

Analysis also showed that eight vehicles had been purchased with the proceeds of crime. to the value of R6 million, which was also secured with the Special Tribunal Order.

Load shedding offloads fraudulent funds

The FIC supported the SAPS and AFU in an advanced fee fraud matter (419 scam or non-delivery scam) in which a member of the public was coerced into paying a large amount for the purchase of a diesel generator.

After many enquiries by the purchaser and excuses received following non-delivery of the generator, the member of the public approached the SAPS.

The immediate response to a request from the FIC to SAMLIT members resulted in all the funds being secured with a section 34 intervention and a preservation order. Prompt assistance by a SAMLIT member helped produce the positive result. In these types of cases, the funds are often immediately withdrawn and become untraceable.

Fraud and corruption

GENERAL

- Criminal activity related to fraud generates money that usually needs to be laundered. Therefore, where fraud is detected, money laundering will most likely be present.
- Involvement in investments promising unrealistically high returns over a short period.
- Numerous cash deposits not followed by the agreed investment.
- Funds diverted to sham companies or 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 an existing entity.
- Shell entities with names similar to legitimate firms previously paid by the 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.
- Unexplained cash deposits into accounts of local prominent influential persons.
- Sudden cash deposits into newly formed or dormant accounts followed by rapid withdrawals.

MULE NETWORKS

- 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.
- Volumes of cash used outside of the formal banking system are large and blur the trail on the flow of funds.
- Dormant accounts receive sudden huge deposits and rapid withdrawals.
- Entity account transactions do not match the client profile.
- Unusually 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 use 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 "trading 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 or 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.

PYRAMID AND PONZI SCHEMES

- The promise of unrealistically high, quick returns for nominal investment.
- High and fast returns which 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 to generate a return, is a classic trait of both pyramid and Ponzi schemes.
- 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 would state that investment involves many businesses, the development work and the flow of money investment cannot be explained in detail.

TAX-RELATED CRIMES

- A company account is new but receives tax refunds and VAT return payments.
- Tax fraud.
- The use of offshore tax or financial secrecy 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 business is not located in the 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.
- Cross-border and national financial flows through couriers and Hawala.
- Frequent travel across the borders and to high-risk countries (tax or financial secrecy havens or countries known to support terrorist activities).
- Regular cash deposits to the same person or different individuals below the FIC Act threshold on for reporting cash transactions i.e. below R50 000 and/or via retailers' money market till points.
- Regular third-party cash payments into accounts and money quickly withdrawn by the recipient.
- Formal networks of money transfer services (MTS) for cross-border transactions such as Hello Paisa, MoneyGram, Western Union, and Mukuru.
- Widespread use of cash in the informal sector, SMME's registered or unregistered with the CIPC and in the taxi industry.

- Properties, second-hand or new motor vehicles paid for in cash through agents and dealerships that are not FIC Act compliant. The focus is on sales and commission versus reporting requirements.
- Investments in livestock, which is largely a cash transaction business and a challenge to monitor role players such as auctioneers.

STATE PROCUREMENT

- Individuals with multiple directorships.
- Companies under the same directors with multiple identical or similar names.
- Companies with no online presence or physical address (or the address for a company contracted for millions of rands worth of work is operating from a residential address, with no business premises).
- Companies with directors who are closely associated with or related to senior government representatives.
- Companies with no track record of similar work to that contracted by state.
- Companies with very recent incorporation dates or those who have recently seen changes in directors, or sudden changes to dormant companies, which have failed to submit annual returns and risk deregistration by CIPC.
- Government employees, especially those who have responsibilities related to procurement processes including supply chain management, bid adjudication, contracts and payments, who appear to be living beyond their means.
- Tenders awarded at inflated prices, relative to reference price registry, or historical pricing for similar goods and services.
- Non-compliance with procurement processes and regulations i.e. advertising tenders, consideration of bids, minimum number of quotes, cancellation and reissue of tenders.
- Nominee arrangements – where a nominee appears to be the director or shareholder of a company, whereas in fact the actual owner remains unknown and exercises control.

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. 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 KwaZulu-Natal province. 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. The subjects have since been convicted of dealing in narcotics and money laundering.

Crunch time for illegal drug and steroid dealers

Financial intelligence obtained identified financial profiles and bank accounts linked to two subjects who were under investigation for alleged dealing in illegal drugs and steroids.

During the investigation, DPCI conducted a search and seizure operation. The FIC provided financial and other data, such as entity names linked to the subjects.

Cash threshold reports filed by the financial institutions indicated the movement of large amounts of cash and identified various bank accounts linked to the subjects. Financial analysis also detected sizable cash transactions and cross-border flows of money linked to the subjects under investigation.

Two arrests were made on charges of dealing and manufacturing scheduled substances, as per the Medicines and Related Substance Act, 1965 (Act 101 of 1965) and Drug Trafficking Act, 1992 (Act 140 of 1992).

Drug 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 of the 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.

KIDNAPPING

Kidnap victim goes home

The FIC assisted with the rescue of a kidnap victim as well as the identification and arrest of three alleged kidnappers.

Starting with enquiries at financial institutions, the FIC ascertained that financial activity had taken place on the victim's bank account after the kidnapping had occurred. The FIC requested further information on the transaction details for further analysis.

The transactions turned out to be ATM cash withdrawals from a town close to the victim's home address. After providing relevant information to DPCI, the suspects were identified and tracked down.

At the point of arrest, the suspects were leaving a shopping mall with the victim in a vehicle.

The owner of the vehicle was also identified. A search of the owner's address led to the seizure of two other vehicles believed to have been used in the commission of other kidnappings, as well as 16 mobile phones thought to belong to kidnap victims.

The suspects were charged with kidnapping, extortion, armed robbery, and possession of stolen goods.

MODERN SLAVERY AND HUMAN TRAFFICKING

Trafficking Thai women

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

Human trafficking and money laundering

Law enforcement approached the FIC for assistance with a human trafficking investigation. The subject of the enquiry was suspected of using an agency as a front for engaging in prostitution and money laundering. The subject allegedly directed her workers to provide illegal services from hired premises and extorted money from clients through threats of exposure.

Through bank statement analysis, the FIC discovered links between the main subject and multiple depositors. Contra details to these transactions was also included, thus identifying possible victims and customers linked to the illegal activities. It was also established that the main subject received numerous cash deposits.

The FIC provided valuable new information and insights into the financial operations of the subject that enabled law enforcement to pursue the case.

ROBBERY

Cash in transit money found

SAPS requested assistance from the FIC regarding a case involving a cash in transit security officer who was robbed of cash amounting to R2.6 million.

Proceeds amounting to R92 701.48 from the crime were identified through financial intelligence and blocked in bank accounts through directives issued by the FIC. The AFU then obtained a preservation order to prevent the dissipation of the money. The enquiry focused on the alleged involvement of various subjects suspected of using their bank accounts to receive deposits and disbursement of funds linked to the incident.

Bank statement analysis by the FIC on corresponding accounts revealed that items had been purchased with the proceeds of the crime. After being pointed to the relevant credit providers, SAPS confiscated the items.

Furthermore, the analysis indicated that two of the alleged perpetrators received cash deposits prior to the commission of the offence, suggesting that they were the architects behind the cash in transit robbery.

INDICATORS RELATING TO SECTORS

Red flags associated with ESTATE AGENT SECTOR

Possible concealment of real beneficiary owner

- Customers making unusual requests.
- The customer is a foreign national who refuses to cooperate or provide the required information, data, and documents.
- The customer makes unusual requests related to the estate agency, brokerage, or its employees.
- The risk of money laundering becomes higher if the customer is either a politically exposed person or is connected with a person who is politically exposed.

If the customer is a legal person or made a legal arrangement

- Inability to demonstrate a history or provide evidence of real activity.
- No presence on internet or social business network platforms.
- Registered under a name that does not indicate the activity of the company.
- The registered name of the company is identical or similar to big multinational companies.
- E-mail address provided uses public or non-professional domains such as Hotmail, Gmail, Yahoo etc.
- The registered address of the company is the same as the address of many of the client's companies, indicating the use of a mailbox service.
- Unable to contact or locate directors or controlling shareholders.

Suspicious payment methods

- Payment made through cash or negotiable instruments that do not state the true payer such as cashier's cheques etc.
- The payment is divided into smaller parts with a short interval in-between.
- Vague validity of the documents submitted with loan applications.

Red flags associated with
MOTOR VEHICLE DEALERS

- Identities of clients not verified, dealers not enquiring about their customers' source of funds when cash payments are made. Customers only undergo robust customer due diligence if vehicle purchases are through loans. There is also little information about the proportion of high-risk customers.

- The vulnerability of the industry is frequently exploited by customers who purchase motor vehicles to disguise the origin of dirty money - all dealers must be alert to this risk. If they negligently fail to identify suspicious transactions, motor vehicle dealers risk being charged with money laundering.

Vulnerabilities identified in this sector include the following:

- Informal motor vehicle dealers.
- Cash-based transactions.
- Deficiencies within legislation in relation to imported second hand cars.
- Collusion of officials and illegal dealers.
- Ineffective control on bonded warehouses.

Red flags associated with GAMBLING SECTOR

- Buying casino chips for cash or on account, then redeeming value by way of a casino cheque, bank draft of money transfer and casino cheques payable in cash.
- Frequent deposits of cash or wire transfers into casino account.
- Funds withdrawn from account shortly after being deposited.
- Exchanging low denomination currency for high denomination currency.
- Casino account transactions fronted by persons other than account holder.
- Large amounts of cash deposited from unexplained sources.
- Associations with multiple accounts under multiple names.
- Transfer of funds from or to a foreign casino or bank account.
- Transfer of funds into third-party accounts.
- Multiple individuals transferring funds to a single beneficiary.
- Structuring of deposits, withdrawals, or wire transfers.
- Use third parties to undertake EFT transfers and structuring of deposits.
- Use of an intermediary to make large cash deposits.
- Use of multiple names to conduct a similar activity.
- Use of casino account as a savings account.
- Activity or income is inconsistent with the customer's profile.
- Use of false and stolen identities to open and/or operate casino accounts.
- Customer name and name of account do not match.
- The intentions of buying winning tickets from legitimate winners for more than they are worth to create the impression that the funds were derived from legitimate sources.
- Requests for casino accounts from politically exposed persons.

FATF identifies at least nine ways in which gaming and gambling companies may be particularly vulnerable to money laundering:

- Receiving the proceeds of crime.
- Accepting cash payments.
- Transfers between customers.
- Improper use of third parties.
- Casino deposit accounts.
- Prepaid cards.
- Identity fraud.
- Multiple accounts.
- Multiple operators.

Red flags associated with
KRUGER RAND DEALERS

Customer behaviour

- Established customer (including bullion dealers) dramatically increasing their purchase of gold bullion for no apparent reason.
- Foreign nationals purchasing gold bullion through multiple transactions over a short period of time.
- Bullion transferred among associates using bullion accounts (including family members) for no apparent commercial purpose.
- Occupation inconsistent with customer's financial profile. For example, the customer may list their occupation as 'student' or 'truck driver' yet transfer large values of funds to bullion accounts.
- Customer buying gold bullion and using a general post office, or private service provider mailbox as their address, without listing a corresponding box number.
- Unusual pattern of bullion transactions and the nature of the transactions are inconsistent with the customer profile.
- A previously unknown customer requesting a refiner to turn gold into bullion.

Red flags associated with
REAL ESTATE SECTOR

- Customer pays rent in advance and thereafter requests a refund.
- Customer makes a substantial down payment in cash and balance is financed by an unusual source, such as, a third party or private lender.
- Purchases carried out on behalf of any natural person who appears to lack the economic capacity to make such purchases.
- Customer is known to have a criminal background.
- Customer uses or produces identification documents with different names.
- Customer does not want to put their name on any document that would connect them to the purchase or rental.
- Customers concerned that they may be reported to the FIC.
- Customer may appear to want to finalise the purchase as a matter of urgency.
- The purchase price appears to be beyond the customer's means based on their stated or known occupation and/or income.
- Structuring cash deposits below the reporting threshold or purchasing properties with sequentially numbered checks or money orders.
- Accepting third party payments, particularly from jurisdictions with ineffective or weak money laundering controls.

Red flags associated with

LEGAL PRACTITIONERS

- The use of cash for payment of services or payment into trust accounts.
- Anonymity of clients and transactions that are complex in nature for which legal advice is provided by legal practitioners.
- New payment technologies, for example crypto currencies.
- Lack of ML and TF awareness of the legal practitioners.
- Trusts, shell companies and other legal arrangements with a potential to conceal the identity of the ultimate beneficial owners of the clients.
- International payments received from clients.
- High-risk customers and jurisdictions, such as clients linked to institutions or jurisdictions on the sanctions lists.
- Having as clients foreign prominent public officials, domestic prominent influential persons, and high net worth individuals, which are internationally regarded as high-risk clients.
- Organised crime can use legal practitioners to conceal proceeds of crime, obscure ultimate ownership through complex layers and legal entity structures, avoid paying tax, work around financial regulatory controls, create a veneer of legitimacy to criminal activity, create distance between criminal entities and their illicit income or wealth, avoid detection and confiscation of assets, and hinder law enforcement investigations.
- Clients who offer to or do pay extraordinary fees for services that would not warrant such fees.
- Payments from non-associated or unknown third parties and payments for fees in cash where this practice is not typical.
- Where legal practitioners, including those acting as financial intermediaries, physically handle the receipt and transmission of funds through accounts they control, they may be requested to transfer real estate between parties in an unusually short period, thereby hindering the know-your-client process and potentially contribute to concealing the beneficial ownership of the client or other parties to the transaction(s) from competent authorities.
- Funds are received from or sent to a foreign country when there is no apparent connection between the country and the client.
- The client is using multiple bank accounts or foreign accounts without good reason.

- Possible involvement of foreign prominent public officials and domestic prominent influential persons in instances where the entity, structure or relationships of the client make it difficult to identify its beneficial owner or controlling interests (e.g. the unexplained use of legal persons or legal arrangements).
- Instances where clients, for no apparent reasons change the way in which transactions are concluded or change their instructions to the legal practitioners on short notice or in a manner that does not make economic sense.

Red flags associated with

TRUST AND COMPANY SERVICE PROVIDERS

- Inability to conduct proper customer due diligence on multi-jurisdictional and/or complex structure of corporate entities.
- Complex legal structures that are beneficiaries of the trust or clients of the trust.
- The client of the trust or the company is a politically exposed person.
- The client of the trust or the company sets up a shell company with nominee shareholders and/or directors for conducting business with the trust or company.
- Client is known to have a criminal background or media reports may point to possible criminal activities.
- No economical or logical explanation for the transaction.
- Apparent commercial implausibility of transactions.
- Transactions appear to hide money laundering.
- The transaction does not fit the person's background or legal income.
- The interest rate used for credit transactions differs significantly from the market rate.
- Interest payments and repayments do not occur.
- Flags anonymous companies in offshore jurisdictions: Such companies play an important role in the concealment, shifting and investment of criminal proceeds as well as in the concealment of the true beneficial owners.
- Non-transparent/non-identifiable customers, creditors, or lenders.
- Deviation from usual or expected behaviour – the greater the deviation in behaviour and the more frequent the occurrence of unusual situations, the greater risk there is of money being laundered.

www.fic.gov.za

Financial
Intelligence Centre