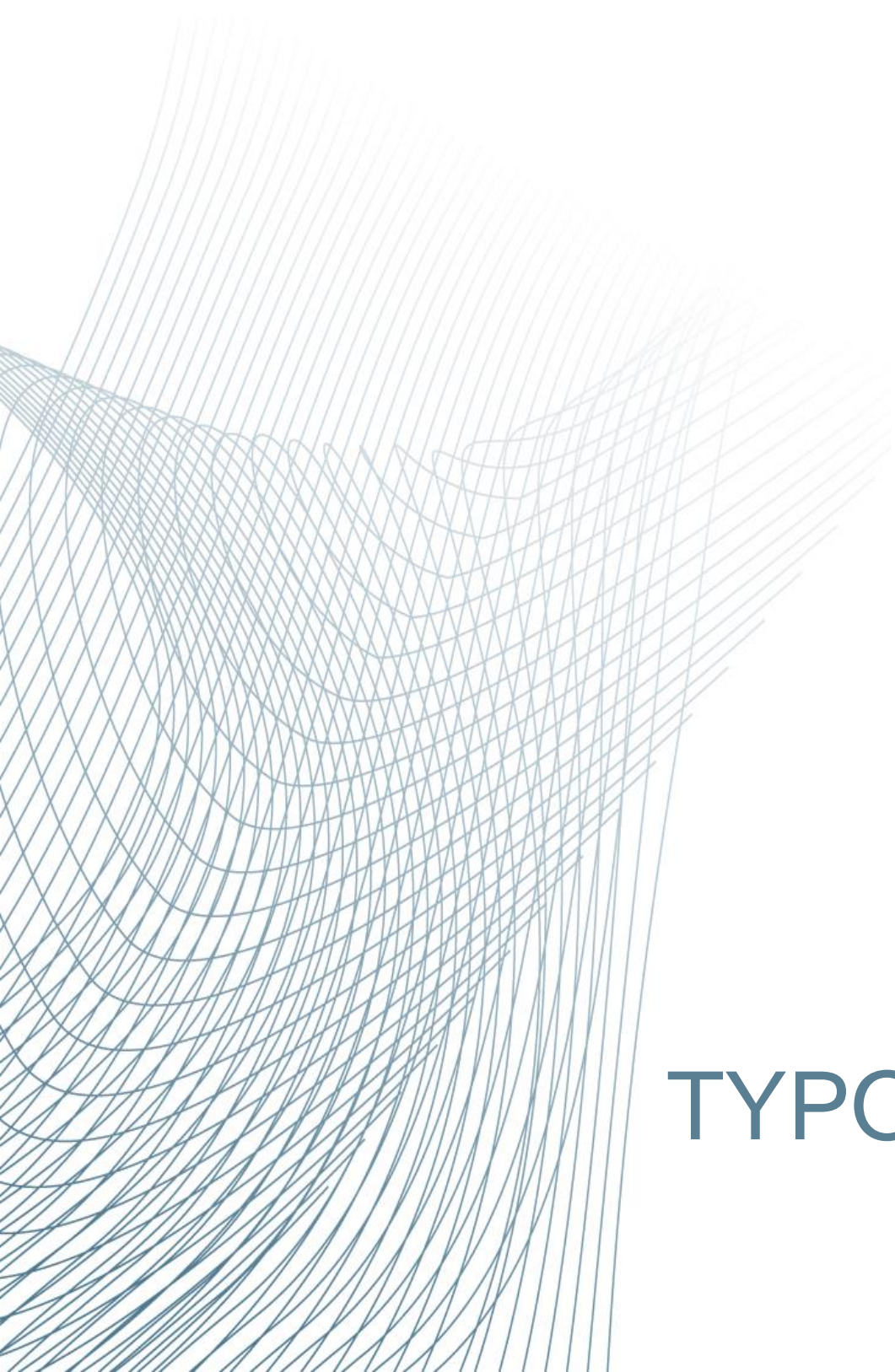




Financial  
Intelligence Centre



# TYOLOGIES

ISSUED MAY 2018

# CONTENTS

INTRODUCTION .....	2
UTILISATION OF THIRD PARTY ACCOUNTS....	3
CHANGING OF BANK DETAILS FRAUD .....	4
PROCEEDS LAUNDERED THROUGH CASINOS .....	5
CORRUPTION .....	6
NARCOTICS .....	7
CYBERCRIME.....	8
PONZI SCHEME .....	9
TAX EVASION.....	10
ENVIRONMENTAL CRIMES .....	11

---

## ABBREVIATIONS/ACRONYMS

<b>AFU</b>	Asset Forfeiture Unit
<b>DPCI</b>	Directorate of Priority Crime Investigation
<b>DEA</b>	Department of Environmental Affairs
<b>FIC</b>	Financial Intelligence Centre
<b>LEA</b>	Law Enforcement Authorities
<b>NPA</b>	National Prosecuting Authority
<b>SAPS</b>	South African Police Service
<b>SARS</b>	South African Revenue Service

## INTRODUCTION

### ABOUT THE FIC

The FIC was established in 2003 as South Africa's National Centre for the gathering and analysis of financial data.

The FIC's primary role is to contribute to safeguarding the integrity of South Africa's financial system and its institutions.

Its mandate is the identification of funds generated from crime and combating money laundering and terrorist financing.

### ABOUT THIS BOOKLET

This booklet gives insight on some of the methods criminals use to abuse the financial system.

The nine case studies illustrate different types of criminal activities and demonstrate how the FIC's financial intelligence reports are pivotal in helping to solve a crime or secure a prosecution.

# UTILISATION OF THIRD PARTY ACCOUNTS

## WHAT IS IT?

It is the use of an account belonging to a third party (spouse, minor or associate) to disguise the ownership of funds in order to hide its criminal origin.

## HOW IT WORKS

The money can either be of a legal origin or the proceeds of criminal activity. If the funds are of legal origin, the purpose could potentially be to avoid a tax obligation. The proceeds of criminal activity would be placed in an account of a third party to disguise the real ownership of the funds.

## CASE STUDY

### UTILISATION OF SPOUSE'S ACCOUNTS

The FIC received a request to assist local LEAs with an investigation into an individual suspected of defrauded his employer of more than R20 million. The FIC obtained and analysed bank statements of the employer and the suspected individual. This revealed that the suspect transferred the funds from his account into that of his spouse. The FIC issued freezing orders on the accounts of

both the suspect and his spouse. The FIC assisted the AFU in obtaining preservation orders against the couple's vehicles, fixed property and accounts, including funds the couple paid to the trust account of their attorney.



## INDICATORS

- ☑ Multiple monthly deposits beyond the scope of salary payments from an employer
- ☑ Unexplained deposits into the bank account of an unemployed spouse or minor
- ☑ Purchase assets in the name of third parties (siblings, spouse and minors)
- ☑ Attorneys' trust accounts receiving numerous unexplained payments from clients.

# CHANGING OF BANK DETAILS FRAUD

## WHAT IS IT?

Fraudulent changing of a supplier's banking details resulting in funds being paid to a criminal third party's accounts.

## HOW IT WORKS

---

Before payments are effected by entities they are informed by a criminal syndicate of a change in bank details and requested a payment to be made into the syndicate's bank accounts.

## CASE STUDY

---

### CHANGE OF BANK DETAILS FRAUD

LEAs identified a syndicate perpetrating a fraudulent scheme on numerous companies and approached the FIC for assistance. The *modus operandi* involved notifying targeted companies of a change in bank account details of a supplier. This resulted in the company unwittingly making payments to a criminal syndicate's account.

After having obtained and analysing the bank statements of the victim, the FIC identified the accounts of the perpetrator and issued an order to freeze the account. The efforts of the FIC enabled the authorities to secure funds in excess of R1.7 million from being dissipated by the criminals.



## INDICATORS

---

- ☑ Change of banking details of an established business
- ☑ Changing of banking details mid-contract or when payments are expected should be treated as suspicious
- ☑ Business accounts receiving funds without showing corresponding commercial activity
- ☑ Newly opened accounts receiving large credits followed by immediate withdrawal.

# PROCEEDS LAUNDERED THROUGH CASINOS

## WHAT IS IT?

Trading in smuggled or illegally obtained precious metals and then laundering the proceeds by purchasing casino chips for future trading.

## HOW IT WORKS

---

Use of casino chips as a medium of exchange for the illegitimate sale of precious metals.

## CASE STUDY

---

### PRECIOUS METALS AND GAMBLING

A suspect was arrested at a roadblock and precious metals and a large amount of cash were found in his possession. The FIC was requested to perform analysis on the subject's financial profile. Enquiries by the FIC to the gambling industry revealed that the suspect made regular visits to a number of casinos where he bought gambling chips and used them as currency to pay syndicate members supplying him with illegal precious metals. Relevant accounts were monitored by the FIC, revealing further beneficiaries of the scheme for the SAPS to investigate.



## INDICATORS

---

- Individuals cashing out gambling chips without gambling
- Holders of casino loyalty cards who frequently gamble without having bought any gambling chips
- Use of third parties to gamble proceeds through casinos.

# CORRUPTION

## WHAT IS IT?

Corruption, although extensively explained in South African legislation, deals with dishonest or fraudulent conduct by those in power, typically involving bribery for some type of gain.

## HOW IT WORKS

---

Corruption usually involves two parties, where one is in a position of power and able to ensure a gain for the other party in return for a benefit.

## CASE STUDY

---

### **CORRUPT PUBLIC SECTOR OFFICIALS IN LEAGUE WITH A PROPERTY SYNDICATE**

The DPCI investigated a syndicate suspected for its involvement in a scheme to defraud a government department into paying more than R40 million for the rental of properties never occupied by the department. Analysis of financial statements by the FIC revealed gratification payments by the syndicate to officials working in the department that awarded the tender. These payments were used to buy movable and immovable assets for the suspects and their family members. This information assisted the SAPS and resulted in the successful prosecution of the officials for corruption.



## INDICATORS

---

- Accounts of salaried employees credited outside of normal salary scope
- Utilisation of accounts belonging to family members to launder funds
- Purchasing of high value assets outside the scope of the income of normal salaried employees.

# NARCOTICS

## WHAT IS IT?

Narcotics refer to the manufacturing, distribution and selling of prohibited substances with addictive properties, also commonly known as drugs.

## HOW IT WORKS

---

Criminal syndicates illegally manufactures, distributes and sells psychotropic substances for financial benefit. These proceeds of crime require money laundering in order to be integrated into the formal financial sector.

## CASE STUDY

---

### **UNCOVERING A NARCOTICS SYNDICATE IN RURAL TOWNS**

Through financial analysis of financial statements belonging to suspected members of a criminal syndicate the FIC assisted LEAs to identify drug dealers operating in rural areas. The FIC's financial analysis identified individuals who were receiving large cash deposits into their accounts from various sources in different provinces. The drug

syndicate's operations were uncovered using information the FIC received from accountable institutions. While cash deposits were made in rural areas, the proceeds were spent on high value movable and immovable property by syndicate members in larger metropolitan areas.



## INDICATORS

---

- ☑ Geographic disjunction between source of funds and dissipation
- ☑ Proceeds used to purchase high value property
- ☑ Large/frequent cash deposits into accounts
- ☑ Transactions inconsistent with clients' financial profile.

# CYBERCRIME

## WHAT IS IT?

Cybercrime is the utilisation of technology to commit crime.

## HOW IT WORKS

---

Cyber criminals steal credit card details, online banking passwords and any other data that can comprise entities or individuals' accounts allowing unauthorised funds transfers to occur.

## CASE STUDY

---

### **CYBERCRIME PERPETRATED AGAINST THE CENTRAL BANK OF A NEIGHBOURING COUNTRY**

A neighbouring country's central bank's credit card was skimmed and cloned using sophisticated technology. 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's analysis identified the accounts used by the suspects, as well as certain high value items purchased with the proceeds of the crime. The FIC froze the funds in four accounts and based on intelligence reports prepared by the FIC, the AFU successfully obtained preservation orders in terms of the Prevention of Organised Crime Act.



## INDICATORS

---

- ☑ Transactions involving institutional credit cards should be subjected to enhanced scrutiny
- ☑ High value purchases on institutional credit cards should be subjected to additional internal controls
- ☑ Suspicious cross-border transfers inconsistent with the client's financial profile.



# PONZI SCHEME

## WHAT IS IT?

This is a form of fraud in which investors are encouraged to recruit other investors. It is based on recruiting people rather than selling products.

## HOW IT WORKS

---

The originator of the scheme usually makes an initial payment and thereafter others need to be recruited. The continued growth of the scheme is dependent on the recruitment of subsequent investors. The scheme resembles a pyramid-like structure with those on top benefitting the most.

## CASE STUDY

---

### FOREIGN EXCHANGE PONZI SCHEME

The FIC analysed suspicious and unusual transaction reports to identify a forex trader scheme that promised a return on investment of 48 percent per year on smaller investments and 84 percent per year on larger investments. The unrealistic high yields promised by the operators of the scheme lead the FIC to conclude that the trader was in fact operating a Ponzi scheme. The FIC, through analysis of all accounts linked to the scheme and its operator, determined that the scheme

owner used large amounts of investor funds to finance two high value properties, luxury vehicles, shopping expenses and employee salaries.

The FIC reported this scheme to the relevant supervisory bodies and LEAs. The FIC also blocked accounts held by the scheme to the value of R87 million and assisted the AFU in its applications for a preservation order.



## INDICATORS

---

- ✓ Rapid cash deposits of a similar amount into a single account
- ✓ Transactions inconsistent with the client's financial profile
- ✓ High volume of deposits within a short period
- ✓ Large amount of cash from unexplained sources
- ✓ Large volume of cash deposits into bank accounts on a regular basis
- ✓ Purchasing of high value assets
- ✓ Multiple individuals sending funds to one beneficiary

# TAX EVASION

## WHAT IS IT?

When entities or individuals do not discharge their tax obligations.

## HOW IT WORKS

---

Individuals or entities can fraudulently under report their taxable income in order to reduce their tax obligation to the fiscus.

## CASE STUDY

---

### COMPANY CAR TAX REFUNDED

An employee tax consultant firm markets itself as an accounting firm that specialises in tax returns for employees receiving company vehicles benefits.

The *modus operandi* relating to the case was to target employees working in the motor vehicle industry. The prospective targets had to be the recipients of a fringe benefit from their employer (motor vehicle dealership), driving the dealership's vehicle. As such a company vehicle fringe benefit is included as part of their remuneration package and is tax deductible.

An easy way to increase SARS refund is to adjust the kilometres travelled for business purposes and by overstating this, a higher tax refund can be expected.

In this instance, the consultant firm overstated the business kilometres travelled by their clients and submitted the overstated (fraudulent) returns to SARS. The overstated submission to SARS was done unknowingly to the taxpayer whom in return thought the accounting firm practiced excellent tax administration. The consulting firm negotiated an incentive payment of 10 percent of any tax refund the taxpayer were to receive from SARS.

In terms of the South African Income Tax Act, fringe benefits are deemed as income and must be quantified in accordance with the regulations of Schedule 7 of the Act.

The FIC assisted both SARS and the AFU to identify all bank accounts held by the individuals and involved entities, all material assets including the identification of cross border financial activity and investments held.



## INDICATORS

---

- ✓ Actual claim amount below the claim instituted
- ✓ Large frequent claims which do not seem appropriate given the amount due
- ✓ Use of tax consulting firm to conduct fraud.

# ENVIRONMENTAL CRIMES

## WHAT IS IT?

Environmental crimes involve the illicit harvesting of fauna and flora by criminal elements resulting in severe damage to South Africa's biodiversity and tourism industry.

## HOW IT WORKS

---

Specific plants and wildlife animals are targeted by criminals poaching these plants and animals from their natural environment, before processing and smuggling them for monetary value.

## CASE STUDY

---

### RHINO POACHERS

The FIC was part of a multi-agency task team comprising of SAPS, the NPA, and the DEA which led to the arrest of 10 suspected rhino poachers for allegedly killing 22 rhinos and being in possession of 84 horns.

The FIC analysed financial intelligence relating to syndicate members involved in the illegal rhino horn trade. The FIC identified the methods being used to launder the proceeds

of rhino horn trade, which included the use of cash deposits, international funds transfers and electronic transfers, often through the accounts of syndicate members or third parties. The FIC assisted the AFU in preserving R190 000 held in the bank accounts of the syndicate.

The intelligence report produced by the FIC exposed a criminal network, including an attorney, a pilot and a corrupt law enforcement official believed to be involved in the illegal rhino horn trade. In addition, it also established that the syndicate used the illicit proceeds to purchase high value assets.



## INDICATORS

---

- ☑ Unexplained large deposits into accounts
- ☑ High value property and vehicle purchases
- ☑ Financial activity inconsistent with the client's profile.

***Making South Africa's  
Financial System Intolerant to Abuse***

T +27(0)12 641 6000

F +27(0)12 641 6215

[www.fic.gov.za](http://www.fic.gov.za)

