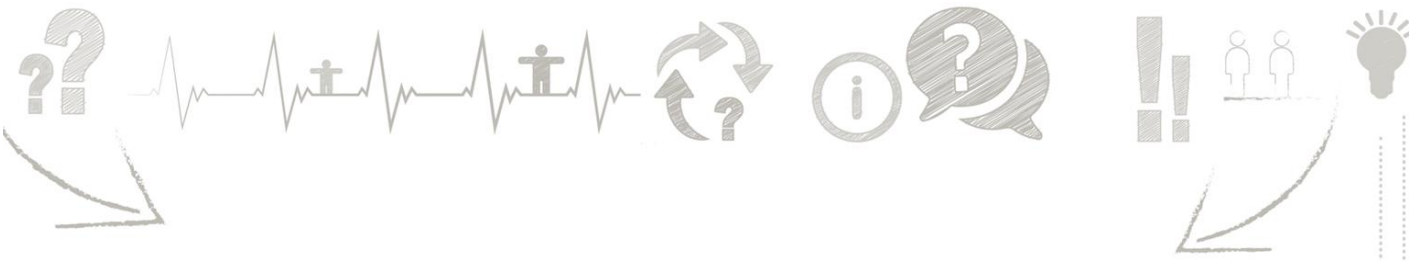
Financial
Intelligence Centre

MONEY LAUNDERING

TYPOLOGIES & INDICATORS



CONTENTS

DUPLICATE PAYMENTS.....3

FRAUDULENT COMPANY SCAMS ..4

ILLEGAL GOLD SMUGGLING.....5

ENVIRONMENTAL CRIMES.....6

CORRUPTION 7

NARCOTICS 8

CYBERCRIME.....9

PONZI SCHEME 10

STOLEN STUDENT LOANS.....11

TRUST ACCOUNT ABUSE.....12

ABOUT THE FIC 13

INTRODUCTION

The Financial Intelligence Centre (FIC) is committed to increasing the utilisation of financial intelligence using a variety of methods – including creating awareness on criminality – in an effort to enhance the intolerance of the abuse of South Africa's financial system.

This publication provides indicators developed from case studies to assist the reader in identifying potential criminal financial activity.

In this publication the FIC uses case studies to illustrate how criminal incidents can occur and how criminals operate.

DUPLICATE PAYMENTS

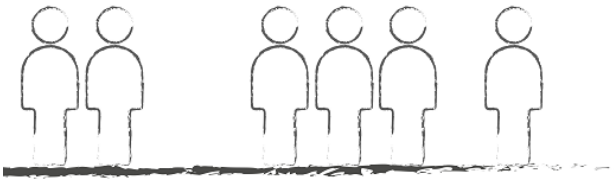
WHAT IS IT?

Duplicate payments are a form of fraud that lead to monetary losses for the entity involved. It allows for the redirection of a duplicate payment into the perpetrator's account.

HOW IT WORKS

An entity will make a payment to a service provider. A second duplicate payment would then be effected to the service provider with the exception that the funds are in actual fact being redirected to the account of the person at the entity affecting the payments.

Another permutation is for a duplicate payment to be made and the service provider is requested to refund one of these payments to an account belonging to the perpetrator.



POSSIBLE INDICATORS

- Duplication of payments from a single account
- Flow of funds that is inconsistent with the normal customer profile
- A possible purchasing of high value assets (i.e. property and vehicles) which might occur with the subsequent transferring of refunds into the account of the third party

CASE STUDY

DUPLICATE PAYMENTS |

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

It was alleged that the subject made duplicate payments to the municipality's service providers. The municipal manager discovered a discrepancy and reported the suspected unlawful activity.

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

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

FRAUDULENT COMPANY SCAMS

WHAT IS IT?

Entities are registered with the Companies and Intellectual Property Commission (CIPC) with names confusingly similar to already existing entities in South Africa with the aim to defraud them.

HOW IT WORKS

Entities are registered with the CIPC with names very similar to existing entities.

Accounts are then opened in the name of these duplicate companies. Banking details are then changed so that funds from the legitimate service provider are transferred to the duplicate accounts.

POSSIBLE INDICATORS

- Using fraudulent documentation to open bank accounts for companies with names confusingly similar to those of existing legal entities
- Change of banking details of established business
- Changing of banking details mid-contract, or when payments are expected, should be treated as suspicious
- Entities' business accounts used to receive money without having corresponding commercial activity
- New accounts receiving large credits followed by immediate withdrawal

CASE STUDY

DUPLICATE PAYMENTS |

The modus operandi of this syndicate involved them registering legal entities with the CIPC using names that were confusingly similar to those of legitimate, existing businesses in South Africa.

Using these details and employing false identity documents, the syndicate opened several bank accounts for the "duplicated" companies. The syndicate began making multiple changes to account information.

The syndicate then successfully changed the banking details of the aforementioned legitimate companies, and channelled the money of these firms into the accounts opened with false identity documents.

ILLEGAL GOLD SMUGGLING

WHAT IS IT?

Precious metal smuggling can take the form of either trading in illegally mined precious metals or obtaining the mined metals illegally and then selling it, with the proceeds of these illegal activities being laundered.

POSSIBLE INDICATORS

- Transfers of funds between business accounts and personal accounts that are not business related
- Suspicious withdrawals and deposits of large sums of money into accounts
- Attorneys' trust accounts that receives funds from clients and purchasing high value assets for clients
- Flow of funds from accounts to offshore destinations.

CASE STUDY

ILLEGAL GOLD SMUGGLING | The FIC assisted the South African Police Service with an investigation into illegal gold smuggling.

The suspected role players were linked to several multi-national legal entities. The FIC identified and traced the bank accounts of the subjects, their financial transactions, assets and foreign accounts.

The FIC uncovered suspicious deposits and withdrawals of large sums, and their transfers from business to personal accounts belonging to syndicate members. Analysis of financial statements identified funds being transferred to attorneys, who in turn purchased high-end properties and vehicles on behalf of syndicate members.

With the help of its international counterparts, the FIC determined that some of the syndicate members held offshore bank accounts and owned properties in other jurisdictions.

The FIC's report resulted in the local law enforcement agency arresting syndicate members and confiscating assets worth about R6.8 million. ■

ENVIRONMENTAL CRIMES

WHAT IS IT?

Environmental crimes involve the misuse of fauna and flora by criminal elements to enrich themselves, damaging nature in the process as well as the tourism industry. Examples include smuggling of ivory, abalone, endangered species and rhino horns.

HOW IT WORKS

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

POSSIBLE INDICATORS

- Unexplained large deposits into accounts
- High value property and vehicle purchases
- Financial activity inconsistent with the customer's profile
- Cash purchase of high denomination foreign currency

CASE STUDY

RHINO POACHER |

As part of a government task team, the FIC identified bank accounts and traced assets belonging to a rhino poaching syndicate.

After receiving suspicious transaction reports on accounts belonging to individuals linked to the rhino poaching syndicate, the FIC analysed transactional records that revealed large amounts of money being deposited into their accounts. This money had been used to purchase high value property and vehicles.

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

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

CORRUPTION

WHAT IS IT?

Corruption, as 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 at a price.

POSSIBLE INDICATORS

- Unexplained cash deposits into accounts of local prominent influential persons (PIPs)
- Sudden cash deposits into newly formed or dormant accounts followed by rapid withdrawals
- Utilisation of family members to launder funds

CASE STUDY

CORRUPTION |

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

Initial analysis revealed that funds were being diverted to projects benefitting former senior employees of the department who had been responsible for allocating grants for qualifying projects. Financial intelligence revealed front companies, through which these former employees' relatives set up projects or entities to receive grants from the fund. The proceeds of these illegal grants had been used to buy properties and vehicles. Some of the proceeds were laundered through an attorney's trust accounts.

The financial intelligence enabled the identification and subsequent subpoena of more than 100 bank accounts, which allowed forensic auditors to compile a detailed cash flow analysis of the scheme. ■

NARCOTICS

WHAT IS IT?

Narcotics refer to prohibited substances with addictive properties, which are manufactured distributed, and sold.

POSSIBLE INDICATORS

- Suspicious deposits of large amounts in small denomination notes
- Rapid cash in and out of funds
- Business accounts without business transactions
- Acquisition of high value assets (i.e. property, vehicles)

CASE STUDY

NARCOTICS |

The FIC supported the South African Police Service in an investigation into a drug manufacturing and trafficking syndicate. The FIC collected, analysed and provided financial intelligence relating to bank accounts and transactions linked to subjects of the investigation, including cross-border transactions.

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

Analysis of transactional records revealed regular cash deposits, soon followed by withdrawals. Another identified account reflected large cash deposits, and some funds were frequently transferred to a travel agency. One of the entities investigated had a business account that did not reflect any business transactions.

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

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 compromise entities or individuals allowing data or fund transfers to occur.

POSSIBLE INDICATORS

- Dormant accounts showing sudden high volume transactional activity
- Increased daily transactional limits followed by sudden large withdrawals/transfers
- Large volume of deposits followed by immediate withdrawals
- Use of duplicate cards to access accounts

CASE STUDY

CYBERCRIME |

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

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

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

The FIC created profiles on the beneficiaries of these transactions and identified various suspects and related bank accounts and investment portfolios. Cell phone data supplied by investigating authorities was analysed and links between suspects were identified. As a result of the joint operation, several suspects were arrested. Information supplied by the FIC was used to support preservation orders on high value properties and vehicles.■

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.

POSSIBLE INDICATORS

- Rapid cash deposits of a similar amount into a single account
- Shared geographic footprint of depositors
- Transactions inconsistent with customer 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

CASE STUDY

A SUSPECTED PONZI SCHEME | Alerted by 13 000 cash deposits into one account in one day, the FIC worked with the Asset Forfeiture Unit and the South African Police Service's Commercial Crimes Unit to identify a suspected Ponzi scheme.

The scheme promised unrealistically high, quick returns and a lavish lifestyle of international travel in return for an investment of just R295.

Prospective members were required to deposit money and attend a seminar on travel arrangements and investing. Little training was actually given at these seminars. Instead, participants were encouraged to recruit as many new members as possible into the scheme. Like all pyramid schemes, it was heavily dependent on continuous membership growth.

The investigating team froze five bank accounts containing R26 million and obtained preservation orders against the main accounts.■

STOLEN STUDENT LOANS

WHAT IS IT?

This is a form of fraud in which bank account details are amended with the intent of diverting funds from the intended recipients.

POSSIBLE INDICATORS

- Suspicious credits outside of normal salary credits
- High value vehicles and immovable property
- Use of third party accounts, often family members

CASE STUDY

STOLEN STUDENT LOANS | The FIC received a suspicious transaction report regarding an employee working in the finance department of a university.

The employee was diverting tuition payments from student loans into his personal bank account after advising the donor of a change in the university's banking details.

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

The FIC issued intervention directives on various bank accounts, securing more than R4.6 million, and the matter was referred to law enforcement agencies.

This financial intelligence assisted the Asset Forfeiture Unit to obtain a preservation order for funds in the subject's bank account and movable as well as immovable property. ■

TRUST ACCOUNT ABUSE

WHAT IS IT?

Attorneys using funds from their trust accounts for normal business expenses in contravention of the Attorneys Act.

POSSIBLE INDICATORS

- Transfers from attorneys' trust accounts into personal accounts
- Absence of a business account to service the practice
- Cross-border transfers involving an offshore tax haven
- Activities inconsistent with business profile

CASE STUDY

ABUSE OF ATTORNEY'S TRUST ACCOUNT

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

The suspicious transactions in the reports pointed out that multiple large sums of money were being deposited into the trust account by different people and companies over a period exceeding two years. These funds were used to make payments to other depositors in South Africa and abroad.

Funds from this account were being remitted to foreign jurisdictions deemed to be tax havens. Some monies were transferred to the attorney's personal credit card and his practice expenses were also paid directly from the trust account. No business account serviced the practice.■

ABOUT THE FIC

THE FINANCIAL INTELLIGENCE CENTRE (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.

THE FIC'S MANDATE IS THE IDENTIFICATION OF FUNDS GENERATED FROM CRIME AND COMBATING MONEY LAUNDERING AND TERROR FINANCING.

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