Financial
Intelligence Centre

SCAMS AND TYPOLOGIES

DECEMBER 2018

CONTENTS

INTRODUCTION

The Financial Intelligence Centre (FIC) is committed to ensuring the safety and integrity of South Africa's financial system. This document is geared to assist the reader against becoming a victim of cybercrime. As much as people use cyber technology for honest work and play, there are cyber criminals doing the opposite. The evolution of cyber technology has also increased the risk of business and ordinary citizens alike being exploited by those involved in cybercrime. This document also contains typologies which illustrate how the FIC, as part of the value chain in combating crime, assists the authorities in their investigation and prosecution of criminals.

POPULARITY OF SCAMS

Why are scams via cyber networks increasingly such a popular modus operandi for criminals? There are manifold reasons including but not limited to:

ANONYMITY – Criminals can operate virtually anonymously accessing their victim's business and/or private information. From the victim's perspective it may be difficult to tell whether an e-mail pleading for funds to aid families dying of starvation in an earthquake struck region is genuine or not.

DATA IMPROVEMENT – Continuous improvement in data and information analysis is a boost for criminals. Gathering information and drawing analysis helps criminals build profiles on the movements, worth, value and status of their target.

TACTICAL ADAPTABILITY – Using cybercrime, criminals are able to adapt and plug into their target's desires such as instant wealth, helping those in need, economic and social freedom and so on. Typical examples will be during the holiday season where criminals will run holiday scams. During floods and other national disasters, they will use these ordeals to skim off monies. Legitimate charities to end child labour; curb animal mistreatment; support victims of war and others are easily misused.

EASE OF ACCESS – As technology evolves and improves the lives of users, it also paves the way for criminals. Transnational financial transactions, for example, have made international banking commonplace and increased trade across continents. It has eased the possibility of illicit money moving more easily between jurisdictions.

GEOGRAPHICAL ADVANTAGE – Technology allows criminals to create domains in one country, operate in another and target victims in a third. This while law enforcement agencies and/or courts of law often have limited jurisdiction over cross-border cybercrimes.

FIC AND ITS PARTNERS

Businesses, including financial and non-financial institutions, are obliged to submit certain reports to the FIC. Using these reports, the FIC conducts its analysis and develops financial intelligence reports. In turn, these reports provide valuable financial detail and information for the investigative, police, tax and other competent authorities with which the FIC works. Where necessary, the FIC is called upon to assist or request information from financial intelligence units in foreign jurisdictions.

The typologies in this document illustrate the value of the co-operative relationships the FIC has with its partners in law enforcement and in foreign jurisdictions in helping to identify, disrupt and prosecute crime.

WHAT YOU CAN DO

PRACTICAL STEPS

- **PERSONAL DETAILS** – Do not provide your personal details unless you are absolutely sure that the person/organisation/business/retailer/bank/website etc. asking for it is genuine and that they have a legitimate reason for asking the information requested. If you have any doubts, do not answer any questions and shut off contact.
- **DO NOT BE SWAYED** – Cyber criminals can be charming, persuasive, convincing, and making you believe that if you do not take action immediately you will lose a fortune. Remember, if what anyone is saying sounds too good to be true it is most likely not true. This includes that a donation to a person or a cause will secure a special reward from a long lost love, an ancestor, a religious leader or a spiritual healer.
- **SHORTCUT TO WEALTH?** – It is unlikely that a stranger whom you have never heard of, never contacted or never come across before in your life would consider giving or offering you considerable wealth. Should they make direct or indirect contact with you, and if you choose to listen to them, listen with a great deal of scepticism. You are unlikely to become wealthy from the contact; more likely they will be benefiting from your intentions.
- **EVERYONE IS FAIR GAME** – When they seek out their victims, criminals do not distinguish between educated/uneducated, employed/unemployed, poor/rich, old/young, healthy/sick. Do not believe they will never target you. Remain cautious, alert and wary – it is your best protection.

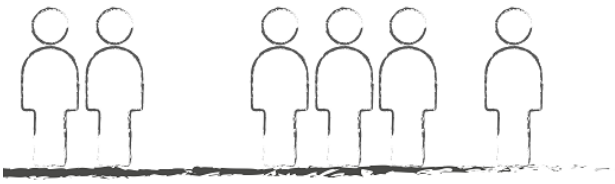
.

CRYPTO ASSETS SCHEMES

Crypto assets such as Bitcoin, Ethereum and others are digital representations of value that can digitally be exchanged, transferred, or used for payment or investment purposes. Crypto assets are decentralised and do not include any digital representations of normal tangible money (or FIAT currency), securities or any other financial assets. Crypto assets are the latest and modern investment opportunities currently available. However it is imperative to note that along with the opportunity, comes risk. Risks lie in the complex and technical nature of crypto assets as well as the limited regulatory oversight to the digital currency.

MODUS OPERANDI

The technicalities of crypto assets are complex and can be confusing to new users, making it an ideal means for criminals to target their victims. Users are targeted through a scheme, known as “phishing”. It is very similar to the scheme where one receives a fraudulent e-mail that appears to originate from a bank. There is a request to click on a link and the user is redirected to malicious websites where security credentials such as the username and passwords of the client are harvested. In the case of crypto assets schemes, these fraudulent e-mail messages appear to originate from local crypto asset providers or wallet providers. The e-mails usually contain a link which will take the user to a website that looks identical to that of the crypto asset provider they usually use, but it would actually be a fraudulent website.



THREATS TO THE PUBLIC

Once the user enters their account details on this pseudo web page, anonymous criminals digitally collect all the information needed to log into the victim’s account and they are able to steal all the victim’s crypto assets.

WHAT YOU NEED TO DO

- ☑ Check if the website connects securely over https (not http). If the web address starts with “http” instead of “https”, the data or information one sends to the website is not secure.
- ☑ Make sure that you see the word “Secure” or an image of a locked padlock in the web browser address bar.

- ☑ Check if the company offers abnormally high returns on their website. This should raise red flags and is a common indicator of fraudulent activities.
- ☑ Look for the “About us” and “Contact” web pages. It should clearly indicate the company details and the people associated with the business. Look for the company registration details and the company registration number. If there is little or no information available, you could possibly be involved with a fraudulent scheme.
- ☑ Conduct internet searches to see if there are negative reviews of the website and the brand name of the company. Searches will indicate if the site is trustworthy and respected. Check if there are legitimate and reputable links on the crypto asset website.
- ☑ Conduct your own due diligence before providing any personal or financial information to any website or mobile application.

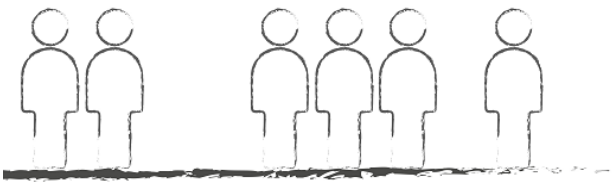
FRAUDULENT INITIAL COIN OFFERINGS

Several internet users in South Africa have received unsolicited e-mail messages and advertisements from an internet entity, offering the purchase and investment in crypto asset tokens. Internet users are attracted to these schemes, believing that as early adopters they stand to earn a fortune. Pensioners and persons going on early retirement are the new target to buy initial coin offerings (ICO) tokens from fraudulent internet entities. With many new buyers having limited knowledge of how the crypto asset industry works, this is the perfect operating environment for these scamsters.

MODUS OPERANDI

The fraudulent entity indicates it has only 500 000 ICO tokens available for purchase. They then pressurise interested parties to purchase ICO tokens as soon as possible and to invest before the tokens are listed on “African global markets”.

Their goal is to develop the virtual asset token into a widely accepted form of payment that will promote trading between African countries. South African internet users are then promised the possibility of earning commission for referral sales of these non-existing tokens. Organisers of this scheme claim to offer “huge” benefits with small risks.
These organisers use cunning marketing methods and hype to convince people to buy a non-existent crypto asset.



WHAT YOU NEED TO DO

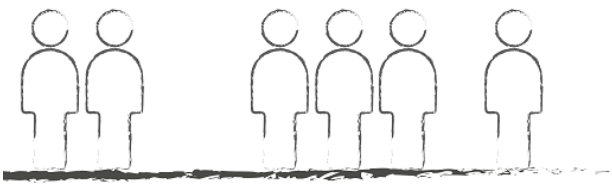
- ☑ If you envisage getting rich quick from an ICO, be aware that for every ICO success story there are many, many more failures, even if the project is not a scam.
- ☑ Thoroughly research any ICO before considering buying in. Review the team behind the project, search for their white paper (a detailed report on their product) which should contain details such as: the purpose of the crypto asset currency, the technology behind it and the specifics of the token sale.

TECHNICAL SUPPORT FRAUD

Anonymous criminals contact unsuspecting victims by telephone or mobile phone. These criminals claim that a fictitious “central system” has triggered a virus infection from the victim’s computer system, which needs immediate attention. They then attempt to offer legitimate technical support services to the victim.

MODUS OPERANDI

These criminals will convince the targeted user to allow them remote access to their computer. They then download and install software from a remote website. After installing the remote administrative tools, these criminals obtain access to their target computer systems. Once they gain access, the scamsters rely on confidence tricks, typically involving utilities built into the operating system and other software to install malicious backdoors to steal security credentials and internet banking credentials from their victim.



WHAT YOU NEED TO DO

- ☑ Do not entertain these fraudulent callers at all. Never provide any remote access to any of your cell phone, tablet or computer devices to anyone you do not know.
- ☑ If your devices are in genuine need of repair, submit your system physically to a reputable technician.

“eHomeAffairs”
STEALING PERSONAL DETAILS

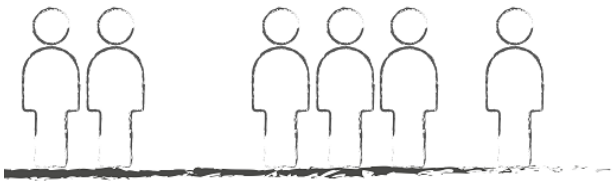
The Department of Home Affairs offers on-line “eHomeAffairs” to enable South African citizens to apply for their Smart ID Card or passport online. This enables applicants to capture and verify their biometric details at authorised banks. Applicants complete their personal information on a prescribed form (DHA-73) before submitting their details and to confirm an appointment at an authorised bank.

MODUS OPERANDI

Criminals create Department of Home Affairs documentation online on authentic looking websites. These documents are electronic copies of the real official application documents for ID or passports. Unfortunately, users cannot download these documents to their local computer. Applicants are therefore forced to complete the document online, by typing their full details, ID number and all relevant application information on the form. Once the form is completed online, the user cannot print the document or save it to their computer system.

The user is prompted to register an account on a “cloud” service, where the document is then stored. The user has to subscribe to these services and provide their credit card and three-digit security code (CVV number) to allow the user to print or view their own personal information.

Information gathered by this method allows criminals to abuse the personal and the credit card information provided by victims.



WHAT YOU NEED TO DO

- ☑ Avoid completing and submitting official Department of Home Affairs documentation online at all times. Rather download the required documentation from the official home page of Department of Home Affairs.
- ☑ Save the document on your local computer and print the document.
- ☑ Complete the document with your own handwriting. After signing and dating the document, scan the completed document. Upload the document via the secure portal to the Department of Home Affairs.

PROMINENT INFLUENTIAL PERSON

A prominent influential person (PIP) is a term used to describe someone who has been entrusted with a prominent public function. A PIP presents a higher risk for money laundering and financing of terrorism due to their functions in public office and influence. Thus they are more susceptible to be involved in bribery and corruption. In the context of the case below, the FIC was called upon to assist in a matter involving a PIP who was a foreign national.

CASE STUDY

The FIC was requested by one of South Africa's law enforcement agencies (LEAs) to assist in locating bank accounts, properties and associated companies linked to a high profile PIP from an African country. The LEA's case related to investigation of money laundering by a former high ranking PIP who had embezzled large sums of money from state coffers of his jurisdiction, which he had spent in foreign jurisdictions.

Three countries were involved in the case: South Africa, the home country of the PIP, and a third country where the money laundering crimes had initially been detected and investigated. It should be noted that the PIP had been detained and was on bail in the third country when he absconded by dressing as a woman and fleeing that country.

The FIC requested financial information linked to the PIP from accountable institutions in the South Africa. It also accessed state and public databases with the aim of locating the assets of the PIP under investigations.

Analysis of the information received revealed that the PIP owned a high value property, worth approximately R2 million, in a prime residential area in the country. Also, whilst in the third country, the PIP had liaised with his local lawyers to assist in procuring real estate for him.

To transfer funds, the PIP utilised a shell company registered in another country (under a different name) as a conduit to ensure that his identity remained unknown. Analysis revealed the attorney's trust account had been used to receive the funds, to purchase and to register the property under the shell company's name. The FIC was also able to determine that the shell company was indeed controlled by the PIP.

The FIC prepared a financial intelligence report for the requesting law enforcement authority and the jurisdictions in which money laundering crimes had been committed by the PIP. This led to a joint application by the three investigating agencies for the restraint and forfeiture of the real estate to the home country of the PIP, where funds had been misappropriated. The PIP was later convicted and jailed in his home country.

INDICATORS

- Abuse of attorney's trust accounts to hide true source of funds
- Usage of shell company registered in third party country as to act as a conduit for transferring proceeds of crime
- International wire transfers to countries considered to be tax havens
- Registration of property under company name to disguise true ownership
- Third parties used to open banking accounts.

DRUG TRAFFICKING

Local and global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws

CASE STUDY

The FIC received a request from a local LEA to conduct financial analysis on a suspected drug trafficking syndicate. The FIC requested financial information from accountable institutions. Official and open source databases were also accessed to source more information such as the movement of syndicate members in and out of the country, and assets registered in the name of individuals associated with the syndicate.

The information received and the analysis conducted by the FIC revealed that the syndicate had transferred large sums of funds into the country, which were suspected to be proceeds from international drug trafficking. The FIC was further able to identify assets such as real estate and a game farm that the syndicate had procured from these ill-gotten gains.

Outward funds transfers were also identified. These were multiple banking account transfers to the syndicate's home country. Some of the funds were transferred into their spouses' accounts. Through financial analysis, the FIC was also able to identify close associates of the drug trafficking king-pin.

This information was duly consolidated into a financial intelligence report and forwarded to the relevant authorities. The syndicate members pleaded guilty to racketeering, drug trafficking and money laundering. Ultimately properties and funds to the value of R3 million was forfeited to the state.

INDICATORS

- Purchasing of high value assets such as property to hide the proceeds of crime
- Frequent cross-border transfers of huge sums of funds
- Usage of spouse's banking account to hide the proceeds of crime (third party accounts)
- Transacting pattern inconsistent with client's profile
- Change of account behaviour without explanation.

RHINO HORN POACHING

The illegal hunting, poaching or capturing of rhino horns

CASE STUDY

The FIC received a financial intelligence request to assist in identifying bank accounts and related transactions of a syndicate involved in rhino horn poaching. The request included the tracing of assets.

Through analysis, the FIC identified reports filed by banks that showed large sums of money had been deposited into the accounts of one subject. The money was used to purchase property of high value. Further analysis revealed that one of the subjects, through his account, also purchased a high end motor vehicle for cash.

Analysis also identified two companies of which the first company's sole signatory was the main subject. During the analysis process, a suspicion was raised on a business cheque account of one of the companies. This was in relation to the account receiving large cash deposits followed by numerous withdrawals and debit card purchases. The second entity, which it was claimed to be in the import-export business, had three signatories, with the main subject included.

INDICATORS

- High value asset purchases (high-end house and vehicles)
- Transacting pattern inconsistent with client's profile
- Regular cash deposits and immediate transfers, usually round amounts
- Use of same branch or similar branches on multiple instances when a single transaction would be more efficient.

ARMED ROBBERIES

A form of robbery involving theft of property while carrying (or pretending to carry) a weapon

CASE STUDY

A LEA launched an investigation into a high flyer after he was arrested for a series of armed robberies. During this investigation, the agency sent a request to the FIC to assist in providing details of the subject's financial profile, bank accounts and associated assets.

At that stage of the investigation, the LEA had no financial intelligence view of the subject and whether he had any properties or accounts in foreign jurisdictions. The subject's associates were also of interest to LEA.

As a first step, the FIC requested financial information from relevant accountable institutions. Accessing both non-public and open source information, the FIC ascertained the ownership of real estate and directorship of companies. The FIC then made contact with its foreign counterparts to establish whether any funds were being concealed overseas.

Information received revealed that the subject owned an entertainment venue, an expensive mansion and a holiday home in a high end suburb, expensive motorbikes and motor vehicles.

An intelligence report was compiled and forwarded to the relevant authorities. With this financial intelligence from the FIC, the LEA was able to understand the subject's financial status and sources of income, and also to link the subject's transactions to the purchase of the above mentioned moveable and fixed property. From the analysis, it was clear that the subject had purchased all these assets from his armed robbery activities. The subject was convicted and handed a long prison sentence.

INDICATORS

- High value asset purchases (mansion and holiday homes)
- Opening of multiple accounts to spread the ill-gotten gains
- Usage of spouse's account to hide proceeds of crime (third party accounts)
- Multiple cash deposits.

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