Republic of Namibia

Financial Intelligence Centre

FINANCIAL INTELLIGENCE CENTRE (FIC)

REPUBLIC OF NAMIBIA

P.O.BOX 2882, Windhoek

Tel: + 264 61 2835100, Fax +264 61 2835259

Web address: www.fic.na

E-mail address: helpdesk@fic.na

ADVANCE FEE FRAUD SCHEMES

ISSUED: SEPTEMBER 2019

1. Introduction

In its efforts to enhance the ability of various stakeholders to mitigate Money Laundering (ML), Terrorism and Proliferation Financing (TF/PF) risks, the Financial Intelligence Centre (FIC) has a duty to enhance public awareness with regards to known fraudulent schemes that the public could be exposed to. The increased ability of criminals to operate globally is a potential danger for social and economic order in every country. The massive potential profits to be gained from such organised crime encourage criminals, who usually are already involved in other serious crimes, to extend their activities to organised crimes such as Money Laundering, Terrorism and Proliferation Financing on a national and international scale.

Generally, and within this report, the term 'Advance Fee Fraud' is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit, in return for providing some modest payment in advance[1]. This fraud is also known as the '419 scam'. In other words, an 'Advance Fee Fraud' is a confidence false pretense in which victims are persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. The fraud has been around for decades and usually targets entities and individuals.

This document aims to forewarn the public by sharing information about the *modus operandi* used by perpetrators in such practices. Equally, the forewarning report avails guidance on how members of the public can protect themselves. It is hoped that can, inter alia, minimize the occurrence of these scams, which in turn reduces the chances of laundering proceeds from such activities through the financial system.

As mentioned above, modern scams are on the increase across the globe. Lately, the FIC has worryingly noted increasing incidents of members of the public becoming targets of advance fee fraudulent scams. Fraudsters are using advanced and new techniques with intent to defraud or obtain money from innocent members of the public by false pretense.

[1] Smith, Holmes & Kaufmann 1999:1

2. How do these schemes operate?

The perpetrators use various platforms with the most significant platform emails, direct telephone calls and other online networks to engage their targets. Such fraud typically involves fraudsters promising the prospective victims wealth, gifts, prizes or employment in exchange for a small advance payment. When a victim goes along with the story (persuaded) and pays the fee, fraudsters may either completely disappear (become unreachable) or invent a series of difficulties which require further payment from the victim until the victim is out of money or stops such payments completely. Below are sampled case studies shared to highlight certain common features of advance fee fraud schemes:

Case study 1: Deceased estate

Dear Ms. Luu,

I am Mrs. Vilo Bali, the wife of late Mr. Nilo Bali, both Namibian citizens. My husband worked with the Texa Company in South Africa (SA) for twenty years before he died in the year 2018. When my late husband was alive he deposited the sum of NAD 6.5 Million in a Financial House in SA. The management informed me a sole beneficiary that my account is DORMANT and if I do not re-activate the account, the funds will be CONFISCATED, or I rather issue a letter of authorization to somebody to receive it on my behalf, since I cannot come over. I have decided to select you, so that the money can be transferred to your account electronically once you activate the DORMANT ACCOUNT and I need the following details below to send the LETTER OF AUTHORIZATION to the financial house in SA that you are now the sole beneficiary. See below:

NAME IN FULL:
CONTACT ADDRESS:
DATE OF BIRTH
COUNTRY:
OCCUPATION:

I want the project to be kept very secret and details of my contact with you should not be disclosed to anybody and this is because my husband's family might want to do everything to gain possession of this money for their own selfish interest.

Case study 2: Lottery Winnings

Dear Mr. Xuli,

Congratulation!!

I would like to inform you that your cellphone number was selected from our database and you have won a large cash prize of NAD 1 000 000.00. This is from a total cash prize of USD 5 000 000, shared among the (25) twenty-five international winners in this category. However, I would like to inform you that in order to claim your prize, we would like you to confirm your personal details and contact number. You are further required to pay a small payment as a release fee for your prize. Kindly reply to this email so we can arrange your prize as soon as possible.

Yours Faithfully,

Mr. Yobu

Red flags of these schemes

- *Fraudsters may claim that political climate, taxes or other regulatory restrictions prevent them from accessing funds in a foreign bank account and request your help to gain such access;*
- *Fraudsters may claim that your last name is the same as that of the deceased person who owned an account and may suggest that you act as the next of kin of this person in order to gain access to the account's funds;*
- *The perpetrators may inform you that you have won some huge prize and may even produce or send you an illegitimate previous pay-out to other people globally to buy your confidence. In addition, they may use forged letterheads of known law firms to enhance your confidence in their scheme;*
- *They may claim that a wealthy individual, who has a terminal illness, needs your help to distribute his/her wealth to charity;*
- *The perpetrators may attempt to mitigate the risks involved for the email recipient. The messages may indicate that the transfer scheme is safe and will be legally binding, using language like "this transaction is totally free of risk and troubles," or "this will be a proper and legal money transfer and there is no risk. Some messages may begin with a greeting such as "greetings in the name of our Lord Jesus Christ";*
- *The victim is promised a dream job, but has to make payments for taxes, visas, "anti-terrorism certificates" or any other formalities; and*
- *The perpetrators may use critical and serious tone language in the subject line of the message that may tempt recipients to open the e-mail such as "Urgent Attention", "Read and Reply As Soon As Possible", "Attention Friend", "Payment Agent Needed." "Congratulations" and "Attention Winner" amongst others.*

3. How do I protect myself from these Schemes?

Be extremely cautious with offers via email, especially if they are unsolicited and are from unknown sources; and

Be vigilant of bogus sites. Cybercriminals can create websites that mimic popular sites to trick people into revealing their personal information.

Do not trust strangers- Fraudsters often pretend to be someone from a trustworthy profession, such as a policeman, a charity fundraiser or an employee at your banking institution. In the real world, such people will never request you for sensitive information such as passwords, credit card numbers and others, so if they do, be suspicious.

Do not be tempted to respond positively in the hope of getting more information. You may merely be confirming your email address and making it easier for the perpetrators to pursue you.

Obtaining personal information from the prospective victim appears to be the key purpose of fraudsters' e-mail contact, as they can then engage in identity theft or drain victim bank accounts.

Do not send money through wire transfers to someone you do not know; and Never believe the promise of large sums of money for your cooperation from someone you do not know.

Passwords and pin numbers-It is good practice to use different passwords each time you create an account online. Using a single password means that if a fraudster cracks one account, they can gain access to others. Commit pin numbers to memory and do not write them down.

Computers are a popular target for fraudsters. Scammers can create websites containing malicious code and emails with viruses attached in an attempt to steal important details. Downloading the latest anti-virus software and using an up-to-date operating system will prevent most of these attacks.

Remember that fraudsters may know basic details about you and may fake your details. If someone claiming to be from your banking institution contacts you out of nowhere, hang up the phone and get in touch with them directly using a known contact detail.

It is worth noting that several message categories were created on the basis of the stated credentials of the sender (scammer) and their reason for contacting the recipient (prospective victim). Regardless of the method used, victims may not report their experience to law enforcement agencies. Some victims may be reluctant to report the incident out of fear they will be prosecuted for their involvement in the illegal act. Victims may also feel too embarrassed to report that they have lost their money by simply responding to an e-mail message. As a result, it is unknown how many individuals actually receive, respond to, and defrauded through advance fee e-mail scams.[2]

REMEMBER

Scammers generate funds by applying pressure tactics that forces unsuspecting persons into making hasty decisions influenced by great promises. If you become a victim of an advance fee fraud scheme, immediately file a report with the FIC at Bank of Namibia or contact the nearest police station to initiate a criminal investigation. This can enable intervention that reduces risks of future illicit activities. Minimizing the occurrence of these schemes reduces the chances of laundering proceeds from such activities in the financial system.

[2] Buchanan and Grant, 2001