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

FRAUDULENT JOB SCHEMES

ISSUED: MARCH 2019

1. Background

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.

Lately, the FIC has observed a worrying increase in fraudulent employment schemes. Such schemes are usually premised on false employment promises. The job seeking public or the unemployed are promised or enticed into believing that a third party or agent can place them into a desired employment. However, before such placement, they are expected to pay some form of deposit or advance payment, which usually is said to be used to enable the employment arrangements.

Generally, scammers are on the increase, with more complex techniques of illegitimate job listings appearing on different employment platforms and innocent job seekers being conned into parting with their hard earned money, or becoming victims of identity theft. It is worth noting that whatever the scammer's techniques and how they go about their *modus operandi*, their goal is to illicitly obtain/steal funds or personal individual identification from the public. Illicitly obtained identification information can be used to advance other crimes. Proceeds from fraudulent job schemes and from identity theft are often laundered or layered[1] through the financial system.

It is against this background that the FIC presents this communication to:

a. enhance awareness of such scams;
b. help protect members of the public and the integrity of the financial system; and
c. minimize the occurrence of these scams, which in turn reduces the chances of laundering proceeds from such activities through the financial system.

[1] Refers to moving funds through the financial system

2. How do Job Schemes operate?

Perpetrators across the globe are conscious that finding suitable employment may be a challenge. They thus advertise non-existent vacancies or employment opportunities with the hope that the public would be interested in such. Perpetrators often advertise on platforms where legitimate employment are advertised. It has been observed that platforms such as Facebook, Twitter, Instagram, Newspapers, Radio, WhatsApp and other online networks are used to attract members of the public or potential job seekers.

When job seekers engage the fraudsters with regards to employment, as per the said adverts, there is often a catch or requirement that advance or upfront payments be made. Equally, they require that personal information be availed as well. Their objective is to trick or deceive the public into believing that if they avail the said advance payments or personal information, such persons can be presented with such employment opportunities. Below are some of the red flags that prospective job seekers or members of the public should keep an eye on:

a. **Too good to be true –**You may not have contacted them in the first place but they already have your details and have made contact with you offering employment. This always seem too good to be true. They may justify that they obtained your details elsewhere. They would normally contact members of the public through some of the platforms mentioned above; In some circumstances, they would either offer you a job right away or say they want to interview you for a certain position. They often do not focus on educational qualifications or previous work experience which legitimate employers focus on;

b. **Requesting of new graduate's details -** Fraudsters may contact institutions such as colleges/universities and request details of graduate's in a specific program, for example in Commerce. In this case, they may call directly the head of department for such program and introduce themselves as prospective employers who would want to assist the new graduates by providing them with suitable employment opportunities. Believing that it is acting in the graduate's interest, the institution will most likely

provide such details (including full names, date of birth or identification and contact numbers etc.);

c. **Advance fee requirements** – When fraudsters have personal information of their potential targets, they would often contact such individuals to offer employment opportunities. Such offers often require that the unemployed or job seekers first make an up-front payment for services such as administration charges, travel expenses, background security checks, amongst others, before employment placement cane be finalized. Members of public are cautioned that legitimate employment agencies or employers do not request for upfront or advance payments. If you are told to purchase or pay for services, be cautious.[2]

d. **Money laundering job schemes** - This is another type of job opportunity scam through which scammers may request your banking details to facilitate receipt of funds into your account. If such funds are received into your account, you are then expected to get a commission from such funds and pass-on the rest to the fraudsters. The funds paid into your account could emanate from fraudulent activities. This is a form of money laundering and is a criminal offence;[3]

e. **Vague job requirements and job description** – Scammers generally would make sure their communications sound authentic by listing job requirements. Often, these requirements are crafted in such a manner that most people would meet them. For instance, the applicant must be 18 years old and above, must be a citizen, must have access to the internet and so on. The job requirements may not mention the level of qualification or years of experience. On the other hand, the requirements of legitimate job opportunity are usually specific. Scammers usually do not provide such information, and if requested, often ignore or promise that it would be available later. Many a times, they even provide responses such as “Don’t worry, we will train you”;

[2] https://www.thebalancecareers.com/top-job-scam-warning-signs-2062181;and
[3]https://www.scamwatch.gov.au/types-of-scams/jobs-employment/jobs-employment-scams.

f. **Unprofessional emails** - If the email message does not include the company's physical address and contact numbers, in most cases, this is an indication of a potential scam. In addition, using email address such as (yahoo.com, gmail.com, hotmail.com) is more obvious to believe that is a scam. Scammers may provide excuses for using personal email addresses by saying the company's server is down, or the company is experiencing too many problems with spam, or the company has not yet set up its email system etc. Also, the public needs to be suspicious of poor spelling, incorrect grammar, incorrect usage of capital letters and generally unprofessional writing or communication; and

g. **Schemes asking to provide confidential information** – In other circumstances, fraudsters may request members of the public to access specific websites and provide personal information including credit card information or completing credit report forms in order to ensure registration on the company insurance or employee's lists. If unsuspecting members of the public avail such information, they could become victims of identity theft. Before availing any personal information, especially online, verify the legitimacy of such website or third party requesting such information. With the website address bars, the bar should for example reflect as: "https://" and NOT "http://".[4]

3. How do I protect myself from these Schemes?

❖ Members of the public are urged not to deal with potential employers or companies that does not have relevant information such as physical address or contact number. Be very suspicious when dealing with job offers or employers who do not have a direct telephone line and/or never answer when you call their numbers but return your call later with a different number. This is often a sign of fraudulent activities;

❖ Background and history of employer – As part of the due diligence process to be conducted, potential job seekers are urged to gain some understanding of a company's performance history from reliable sources. For example, the company's management information, past and present operations, products/services offered,

[4] https://www.thebalancecareers.com/how-to-avoid-identity-theft-when-you-are-job-searching-2062151.

published financial performance records (financial statements) and other relevant information that could verify the authenticity and legitimacy of its existence;

- Unsolicited job offers – Members of the public are cautioned to be careful when entertaining unsolicited telephone calls, emails, social media adverts and other means of communications, offering any form of job opportunity. Scammers are skilled at convincing unsuspecting persons that the employment offered is legitimate;

- Avoid any arrangement with a stranger or supposed employer that requests for up-front payments: Whether it is a direct deposit, wire transfer, international funds transfer, pre-loaded card or any other form of payments. Legitimate employers do not request or demand such payments;

- Never agree to receive funds on your account from doubtful employer and/or transfer money for someone else, unless you know them or can verify the legitimacy of such related transaction;

- Fraudsters are targeting social media sites such as LinkedIn, Facebook etc., to clone themselves as headhunters or recruitment agencies. They may access your personal profiles, career histories, CVs etc and modify such documents. Potential job seekers should be vigilant of unexpected job offers through these routes and be sure not to indicate or provide personal and sensitive information on their social media profiles;

- Avoid sharing your personal details including copies of identification documentation (ID), passport, driver's licence, or bank account details if you are not familiar with the person or employer requesting same. Scammers may use this information to steal from you or other members of the public (identity theft);[5] and

- File a report with the FIC - Be aware that scammers often share details about people they have successfully targeted or approached, using different identities to commit further frauds. If you become a victim of a job scam, immediately file a report with the

[5]https://www.ucas.com/article/job-scams-and-internet-fraud

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.

REMEMBER

Scammers generate funds by applying pressure tactics that forces unsuspecting persons into making hasty decisions influenced by great promises. Minimizing the occurrence of these schemes reduces the chances of laundering proceeds from such activities in the financial system. Therefore, exercise extreme caution and verify the legitimacy and status of the involved prospective employer before engaging them.