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

TENDER CONTRACT SCHEMES

ISSUED: APRIL 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 evolution of public and private sector procurement (awarding of tenders) has escalated the risk of business as evidenced by the growth in exploitation of service providers (business contractors) by those criminals involved in tender contract schemes. This document aims to share information regarding such practices and help avail guidance on how members of the public can protect themselves. This 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 and lately, the FIC has noted with great concern increasing incidents of members of the public becoming targets of procurement schemes. Fraudsters are using advanced and new techniques to defraud unsuspecting businesses by providing illegitimate tender contracts.

2. Understanding the nature of legitimate procurement contracts/tenders

Generally, and within this report, the term 'tender' refers to an invitation to trade under the terms on offer. Further, a ‘contract' in this case would speak to the procuring agreement between a procuring entity and the service provider. Usually, the service provider is contracted to supply goods or services to the procuring entity for payment. Procuring entities include both private sector entities, state owned enterprises and government.

Before contracts are awarded to service providers or tenderers, the procuring entities or buyers would normally advertise the specifications for required products and services. In such advertisements or invitations, interested entities indicate their intention and ability to supply such products and services.

Over the past years a number of companies and individual members of the public have lost funds due to alleged fraudulent Requests for Quotations or Invitation to Bid, supposedly from government institutions or private companies. It is the FIC's view that many entities and persons involved in the procuring business may not be aware of the threat of these fraudulent tender invitations.

3. How do Procurement/Tender Contract Schemes operate?

The perpetrators use various advertisement platforms with the most significant platform being via emails or direct telephone calls to request or invite potential service providers to supply certain goods and services. When potential service providers engage the fraudsters as per the said adverts, there is often a catch or requirement that advance or upfront payments be made. In the same vein, they require that personal information be availed.

The fraudster's 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 proposed tendering or supply opportunities. Unsuspecting persons would make such advance or upfront payments and lose their funds. The FIC also cautions that availing personal information to fraudsters can enable fraudsters to fraudulently use such information, usually in crimes related to identity theft.

Similarly, the involved fraudsters may use illegitimate letterheads to send fictitious Request for Quotation (RFQ) tender to company A by requesting them to urgently supply goods. Usually, the tender specification is so unique that only company B (a fictitious company created by the fraudster) can supply the goods in question. Shortly after company A has submitted its quote it receives notification that it has won the tender contract. Company A may then continue to orders the goods and pays a deposit to the fictitious company B. Once company B receives the money, it disappears and as a result company A's money is stolen in the process. This entire process is a con, from the tender

invitation, the company that selling the products, and the information listed in the tender documents are all[1];

Furthermore, scheme appears as an email sent from government institution claiming that your company has been selected or awarded a tender by the institution to supply certain product or do construction project. The composed email or the letter attached to the email appears to be a legitimate tender contract with contact details provided. This would come as a surprise to you because in most cases you never anticipate such a tender from the such institution or did not either participate. Upon communicate back, fraudsters may then demand upfront payment for such favor or may claim payment stating that such amount would be for administration charges and so on.

4. Indicators of potential procurement fraud schemes

Below are some of the red flags that prospective service providers or members of the public should keep an eye on;

a. Fraudsters may use what appears to be official letter heads of government institutions or private companies often with fictitious logos and contact details;

b. Scammers may play pressure tactics to get unsuspecting person to pay funds in advance;

c. Unique tender specification that only one or few companies can supply such goods or service in question; and

d. Schemes asking for confidential information: In this case, scammers may instruct service provider to register in the tender portal before applying and submitting for tender. Such details are then harvested by the attackers for fraudulent use on other sites, and most probably to gain access to business owners' email accounts.

[1] https://mybroadband.co.za/news/security/215036-online-tender-scam-warning-in-south-africa.html

5. How do I protect myself from these Schemes?

a. With public sector or government tenders, an applicant must be in the database of the department or the ministry in order to be considered for such tender when advertised. No person or company can be awarded a tender without applying for it. Hence, individuals are advised to always engage the relevant procurement officials to verify validity before committing to tenders;

b. If you are registered on the institutions' supplier databases and you have received a request to supply products or services that seems to be from a government institution, contact the department or institution to confirm that the request is legitimate. Do not use the contact details on the tender document as these might be fraudulent. The contact details for all government institutions are available on the website and other open sources;

c. It would also be prudent for all the government institutions to ensure adequate communication is presented to make prospective bidders aware of the correct procedures to follow when applying for tenders or bids. Equally, it would help to provide relevant security warnings of such illegitimate phishing scam campaigns;

d. Unsolicited procurement/tender 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 procurement contract. Scammers are skilled at convincing members of the public that their operations are legitimate;

e. Always compare the name and contact number as shown on the tender invitation letter or email to that published on the relevant institute's website;

f. Small and medium types of businesses should always be cautious of suspicious emails and educate new staff members about normal ways of working when it comes to interacting with other organisations;

g. The banking details and email address provided with the tender document are most likely to belong to a private individual and are not in the company name. It thus helps to contact banking institutions to verify account holder information prior to making any payments;

h. Look for the purchase order and/or claim form number: Government institutions may not send an email requesting to supply equipment and goods without a purchase order and/or claim form number. The norm is that a valid Purchase order is presented to a service provider. Amongst other information, ensure the purchase order is approved and issued in your entity's name; and

i. Members of the public are encouraged to familiarize themselves with Public Procurement processes. Amongst others, the Public Procurement Act, Act No 15 of 2015 speaks to how the government regulate the procurement of goods, works and services in Namibia;[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 a tender 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. Members of the public are urged to exercise extreme caution and verify the legality and status of the involved institutions before engaging them.

[2] https://laws.parliament.na/annotated-laws-regulations/law-regulation.php?id=471