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

FOREWARNING REPORT: INVOICE FRAUD

ISSUED: OCTOBER 2019

1. Introduction

In an effort 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.

'Invoice Fraud' occurs when someone purposely invoices for more than the correct amount, causing individuals or entities to overpay or even pay a person that has never offered them goods or services. In some instances, invoice fraud occurs when a perpetrator poses as a vendor who then deceives a company or person to send funds to a specific account that can be accessed by the fraudster[1]. Mostly, the company would be directed to send such funds to an account which has a similar name or service as a legitimate vendor. This means, fraudsters may submit an invoice, or other requests for payment that is not genuine in the hope that the prospective victims pay without detecting the irregularity. Invoice fraud is a growing trend, alarmingly affecting entities and individuals. This may occur in three forms, such as:

- **Inflated invoices:** a fraudulent invoice which typically means the prices or amounts are higher than the agreed upon sums/amount;
- **Duplicate invoices:** this is when an entity/individual is requested to pay for an invoice which they have already paid for (more than one invoice), even when they only received a product or service once; and
- **False invoices:** A false invoice (non-existent invoice) may attempt to solicit payment for goods and services that were never rendered.

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 from such scams.

[1] https://www.trustedsec.com/2019/04/invoice-fraud-is-soaring-what-you-need-to-know/

2. How do these schemes operate?

Criminals usually commit invoice fraud in various ways, below are some methods employed in such scams:

Step 1 – Taking a phishing trip

A fraudster may find a way to access the email account you have used to send or receive invoices. They may do that by getting you to click on a link in a phishing email, or by intercepting your connection from a non-secure public wifi. The prospective victim may login and passwords are transmitted unencrypted, hence, it is easier for the fraudsters to read your details. They could also manage to install software or malware on your device to monitor everything you do.

Step 2 – Invoice hack

Now that the fraudster can see or have access to your emails, they may look out for any types of invoice you regularly send/receive, or a big one which may be forthcoming. At the same time, they may also research what your invoices look like, how you normally write your emails, and any other information which would help them to impersonate you, in order to deceive your clients/suppliers or others.

Step 3 – The payment

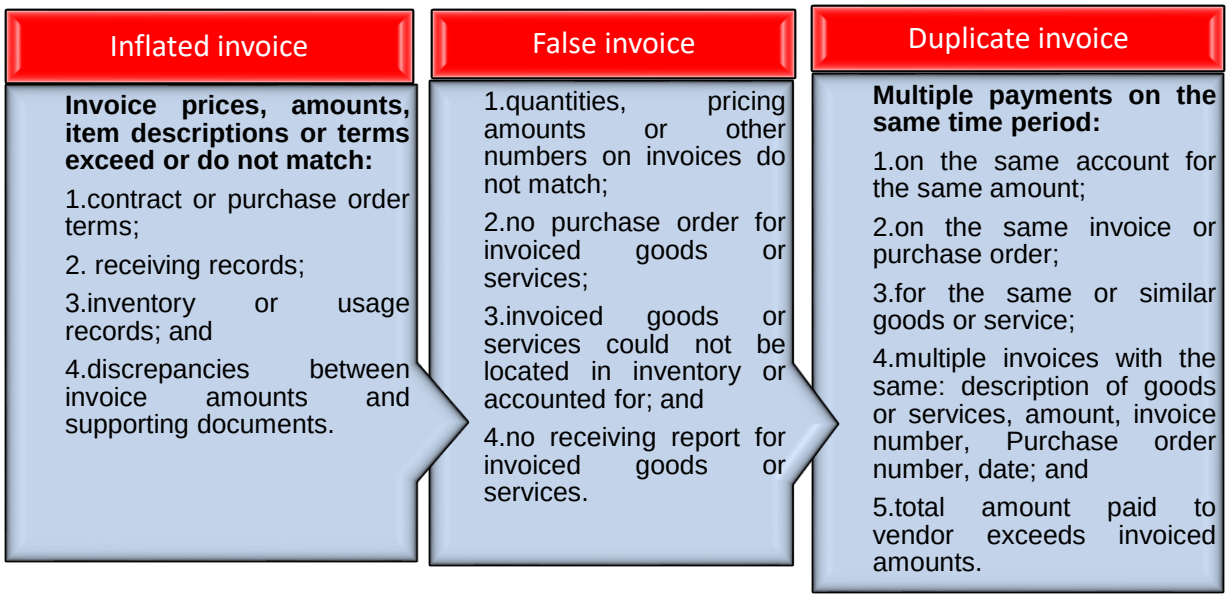
Once the fraudster sees an invoice coming in or out, they may delete that email and re-send either from the original hacked account, or from an account which looks just like the original one. For example: "ebid.jonas@tovessolicitor.com" rather than "ebid.jonas@tovessolicitor**s**.com".

The hacked invoice sent may look almost identical, except for the different email address, telephone and bank account number.

Step 4 – The loss

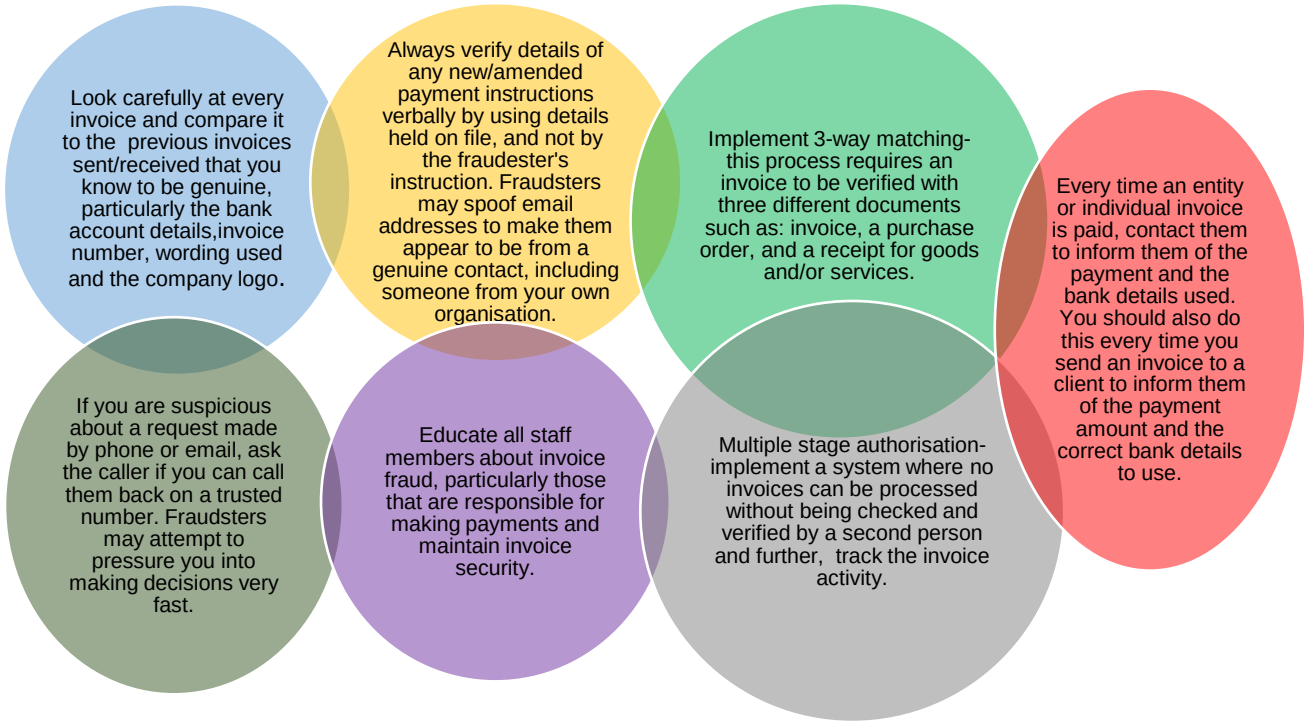
When a payment is made into a fraudster's account, it is usually immediately withdrawn and practically impossible to recover. Because the payment was approved with all security passcodes, it is difficult for the bank's fraud prevention system to pick it up as unusual. As a result, investigations tend to be lengthy and losses are hard to recover.

Red flags for invoice fraud



2

3. How do I protect myself from these Schemes?



[2] https://guide.iacrc.org/potential-scheme-false-inflated-and-duplicate-invoices/

REMEMBER

If you become a victim of invoice fraud scheme, immediately file a report with the FIC at the 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.