Republic of Namibia

Financial Intelligence Centre

P.O.BOX 2882, Windhoek

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

Web address: www.fic.na

E-mail address: helpdesk@fic.na

COURIER SERVICE-RELATED SCAMS

ISSUED: NOVEMBER 2022

1. Background

Over the years, people have lost substantial funds owing to courier-related scams. The COVID-19 pandemic has changed the way various businesses are conducted, with online purchasing expanding steadily worldwide. The general increase in online purchases has resulted in increased package deliveries for consumers.

Fraudsters abuse online business activities and related courier deliveries as a way of illicitly soliciting funds from members of the public through deceptive, dishonest, and fraudulent means. These scams often result in huge financial losses for victims. Other than the obvious financial loses, the proceeds from such activities are often laundered. Money Laundering (ML) activities undermine the integrity of our financial system. The FIC is sharing this publication to help contribute to efforts geared towards combatting such activities.

2. How do these fraudulent scams operate?

Scammers are increasingly enhancing the sophistication and complexity of their methods. There are constantly new innovative ways employed to advance courier-related scams and associated fraud. Most people are familiar with typical courier-related scams wherein an unsolicited email, call or text message requests them to provide sensitive information, usually to those involved in identity theft. Below are some common techniques of courier-related scams1:

[1] https://www.worldwidecouriers.co.za/website/how-to-guides/courier-scams/

Additional charges scam: With the increase in deliveries of packages through courier services, members of the public may/are receiving illegitimate and unsolicited delivery notification scams such as calls, text messages, and emails, purporting to be from a courier service or delivery company. Fraudsters may further claim that additional charges such as customs duty or tax fees are payable on the items before release of such deliveries;

Delivery notification scam: This type of scam occurs when scammers send a text message or email to the victim about the package/parcel to be delivered to their address. The message may often include a "tracking link" that you are urged to click to update your delivery or payment preferences. In some cases, the scammers may send a voicemail message with a call-back number, or a "missed delivery" tag on your door with a number to call;

Re-arrange scam delivery: The victim may simply receive a text message or email alleging to be from a local delivery company, asserting that they have missed your delivery address and you are urgently required to "re-arrange". When you follow/click the link to "re-arrange" the correct delivery address, you may be requested to provide your personal information along with a fee for re-delivery; and

Mix-up delivery scam: This scam is less common, but it does happen. It also affects both buyers and courier services. When scammers have access to information that let them know when and where goods will be delivered, they can wait for a package to be delivered and wait for the delivery service to leave. Then, dressed in courier clothes, they can simply ring the doorbell of the delivery address and explain there has been a mix-up, and take the goods.

3. How do you protect yourself from these Scams?

If you receive a suspicious email, text message or call, go to the courier services' known/verified website directly to verify the sender's identity and avoid dealing with third parties;

Should you be dealing with a company, take time to do the research to ensure that the company is in existence and active prior to any funds transfer;

Safeguard your personal information. Never share personal or financial information with anyone who sends you emails (or calls) requesting this information;

Stay abreast of the latest security measures/threats and if possible, use the latest security controls which can effectively prevent/block unwanted access to malicious sites and spam mails as well as detect malware;

Ensure that your computer and other devices are secure. When a software update is available, consider installing such. Software updates often eliminate any potential or new security threats; and

Verify the sender's contact details to ensure it matches that of the institution it purports to belong to.

REMEMBER

If you become a victim of a courier-related scam, or any other fraudulent activity, immediately file a Suspicious Transaction or Activity Report with the FIC at the Bank of Namibia. Alternatively, you may contact the nearest police station to initiate a criminal investigation.