NAMFISA
NAMIBIA FINANCIAL INSTITUTIONS SUPERVISORY AUTHORITY

SCAM ALERT

SUBJECT: MICROLOAN SCAM

ISSUED: OCTOBER 2021

Lower Ground Floor, 51-55 Werner List Street, Gutenberg Plaza | P.O. Box 21250, Windhoek, Namibia
Tel: +264 (61) 290 5000 | Toll: 0800 290 500 | Fax: +264 (61) 290 5194 | www.namfisa.com.na

1. INTRODUCTION

The Namibia Financial Institutions Supervisory Authority (hereinafter referred to as NAMFISA) is a Supervisory Body in terms of Schedule 2 of the Financial Intelligence Act, 2012 (Act No. 13 of 2012) ("FIA").

In terms of the FIA, NAMFISA is responsible for supervising, monitoring and enforcing compliance with the provisions of the FIA or any regulation, order, circular, notice, determination or directive issued in terms of the FIA, in respect of all accountable and reporting institutions supervised by it.

In the course of executing its mandate, NAMFISA took note of the significant role the microlending sector ("the sector") plays in the economy, through disbursement of unsecured short-term loans to the public.

However, NAMFISA noted that the speed and ease of access to microloans present a window of opportunity for fraud in the sector. Criminals disguise their identity as impostors to defraud microlenders. This is done through theft of privileged information, a conduct widely known as "identity theft".

The Financial Action Task Force (FATF) identified fraud and all other crimes of benefit, as predicate offences (underlying offenses) of Money Laundering (ML). Therefore, in terms of schedule 1 of FIA read with section 39 of FIA, microlenders are obliged to adopt prescribed measures to mitigate the risks of ML, Terrorist Financing (TF) and Proliferation Financing (PF).

Therefore, NAMFISA issues this scam alert to the sector, to enable the sector to apply AML/CFT/CPF measures to effectively mitigate the risks of ML/TF/PF.

2. BACKGROUND

The outbreak of the unprecedented COVID-19 pandemic and the subsequent introduction of public health regulations saw various players in the financial sector

turn to online platforms as new delivery channels of offering financial products and services.

While some microlenders deemed such delivery channels as optimal, in doing so, some of them fell prey to fraudsters/scammers. The fraudsters/scammers identified a window of opportunity to perpetrate fraud against microlenders who use online platforms to disburse loans.

The fraudsters/scammers steal privileged information of unsuspecting members of the public ("the victims") through hacking or unauthorized access, and defraud microlenders by impersonating the victims.

3. MODUS OPERANDI

- ✓ Fraudsters/scammers may hack into the victims' computers and steal privileged information or gain physical access to properties and steal confidential information, which they use to apply for microloans. The aforementioned confidential information may include but is not limited to:

    i) Full names of the victim;
    ii) National identity number of the victim (a copy of identity card);
    iii) Residential address of the victim (a copy of the utility bill);
    iv) Proof of employment (a copy of pay slip);
    v) Address of the victim's employer;
    vi) Bank account number of the victim (bank statement drawn from the bank account of the victim); and
    vii) Email address of the victim.

- ✓ Fraudsters/scammers request the microlender to email the loan application form to them. The email address used is usually that of the victim or may closely resemble that of the victim;

- ✓ Fraudsters/scammers complete the loan application form using the stolen privileged information and return the completed application form with

supporting documents to the microlender via the victim's email address or an email that closely resembles that of the victim;

- ✓ Fraudsters/scammers often make it appear as if they have a dire need for funding and need the funds urgently;

- ✓ Fraudsters/scammers often demand that the funds be paid via an electronic wallet (e-wallet, blue wallet or easy wallet, pay to cell etc.), instead of a bank account;

- ✓ Fraudsters/scammers will redeem the funds at the Automatic Teller Machines (ATMs); and

- ✓ After the funds are successfully redeemed, they destroy the sim card used to contact the microlender.

4. CONSEQUENCES

- ✓ At the stage of repayment of the microloan advanced in this manner, the microlender would then debit the bank account of the victim whose details were used by the fraudsters/scammers.

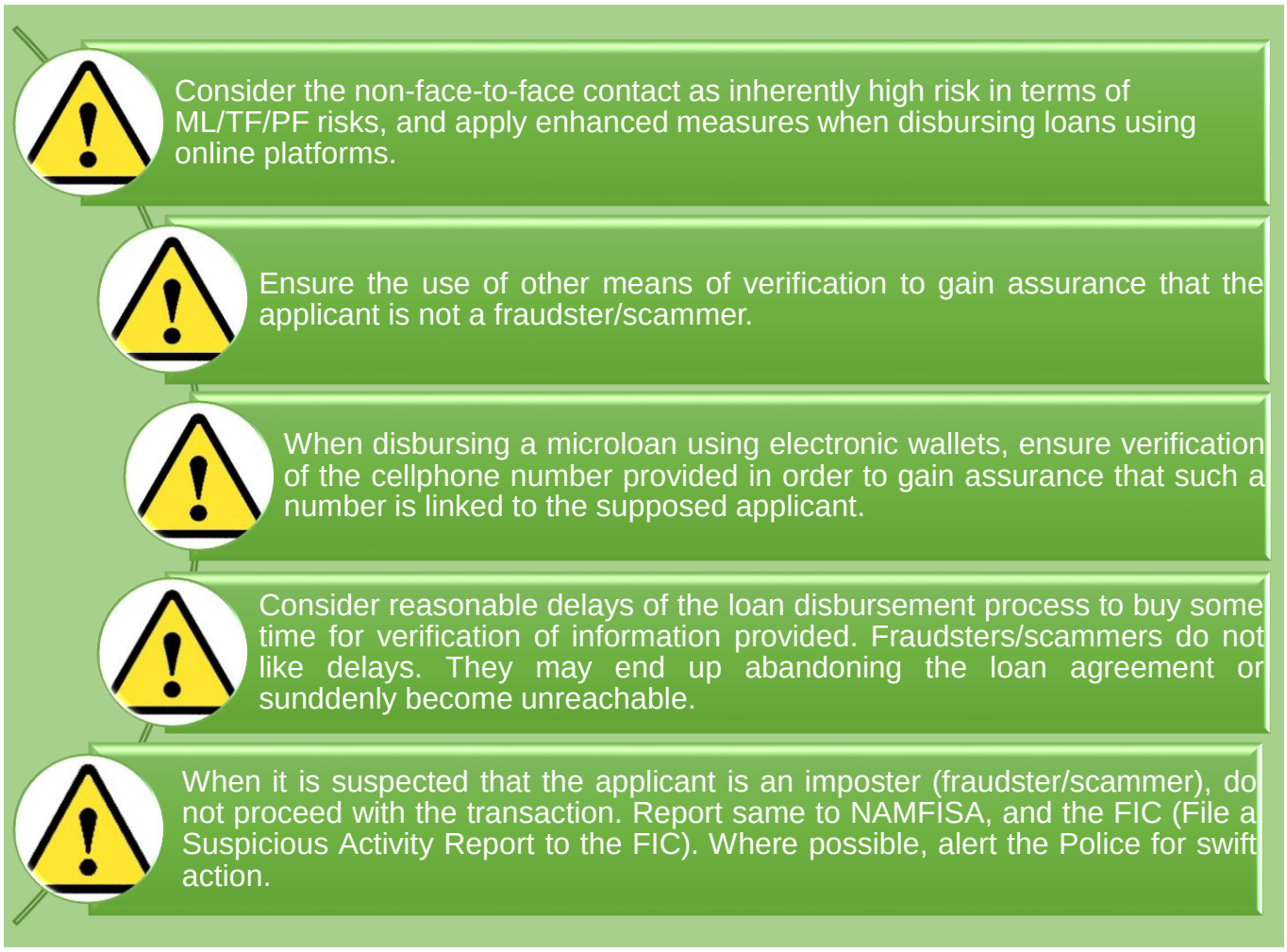
- ✓ When the victim detects a withdrawal from their bank account and confronts the microlender in question, the records at the disposal of the microlender often suggest that the victim applied for a loan on a specific date, on which ground the microlender debited the victim's bank account.

- ✓ In most cases the microlender refuses to refund the victim the funds it has withdrawn from the victim's bank account, which leads to a dispute and a subsequent complaint lodged with NAMFISA by the victim.

- ✓ Upon receipt of the compliant, NAMFISA institutes an enquiry and gathers information from both the microlender and the victim to determine the origin of the transaction that gave rise to the complaint.

- ✓ In most cases NAMFISA's findings suggest that the microlender(s) failed to conduct adequate customer due diligence as required in terms of sections 21(2), 23, 24 of the FIA read with FIA regulations 6, 12 and 13. Where non-compliance of this nature is detected, NAMFISA would impose appropriate administrative sanctions against the involved microlender(s), as well as direct the involved microlender(s) to refund the victim(s).

TIPS TO BE ON THE ALERT



KENNETH S. MATOMOLA
CHIEF EXECUTIVE OFFICER

HOW TO CONTACT NAMFISA:

All correspondence and enquiries must be directed to:

The CEO
NAMFISA
P.O. Box 21250
51-55 Werner List Street,
Gutenberg Plaza,
Windhoek
Republic of Namibia

Tel: +264 (61) 290 5000
Fax: +264 (61) 290 5194