GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT

MINISTRY OF FINANCE

FIU REFERENCE: ADV/001/2019

FIUTT ALERT AND ADVISORY NOTICE TO FINANCIAL INSTITUTIONS, LISTED BUSINESSES AND MEMBERS OF THE PUBLIC:

RISE IN EMAIL COMPROMISE

The Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") is publishing this Advisory in accordance with Section 17(1) (b) of the Financial Intelligence Unit of Trinidad and Tobago Act.

PURPOSE OF THIS ADVISORY

This *Advisory* is intended to provide financial institutions (in particular commercial banks), listed businesses and members of the public to exercise caution when handling email payment instructions for business transactions and large value personal foreign currency transactions, in order to reduce monetary loss and emotional harm.

GENERAL INFORMATION

The FIUTT has noticed an increase in cases of individuals and businesses falling victim to social engineering tactics such as email phishing[1].

For the period December 2017 to December 2018, several businesses and individuals lost funds in excess of TT$2.5 Million in foreign currency transactions to cybercriminals through social engineering tactics.

SOCIAL ENGINEERING TACTICS

- **E-mail Phishing**
- **Email Spoofing and Contact Spamming**
- **SMiShing**

[1] Phishing remains one of the main social engineering techniques used on the Internet to steal ID-related information for fraudulent use. Variations include "SMiShing" (mobile phone text messages to seek the disclosure of information) and "spoofing" (a person or programme is masquerading as somebody or something else to gain trust and make them enter their details into a counterfeit website). http://www.coe.int/moneyval

HOW THE FRAUD WORKS

Social Engineering techniques are used to manipulate financial institutions and members of the general public to unknowingly install malware onto their computers, workstations or wireless devices. This is an effort to compromise and steal personal sensitive information such as emails and other online account login credentials.

Once social engineering attackers get access to the account, they can then monitor emails, intercepting those that contain an invoice or a payment instruction to a Financial Institution **(FI)** or Money or Value Transfer Services **(MVTS)** provider. Social engineering attackers can now change the payment instructions on a specific invoice or planned transaction. This allows the transaction to be processed with the funds going to a bank account of a cybercriminal group instead of the intended and rightful beneficiary.

CAUTION AND RED FLAG INDICATORS TO FINANCIAL INSTITUTIONS AND THE GENERAL PUBLIC

- **Scrutinise documents** thoroughly for any errors, missing information and alterations. Read emails carefully as fraudulent email messages often contain misspellings or poor grammar.

- Any new email instructions to transfer funds to a different beneficiary with a different address and banking account information from what was previously known, requires FIs and MVTS providers to **conduct enhanced due diligence for suspicious payment instructions**.

- Conduct **Customer Due Diligence or if in doubt**, **Enhanced Due Diligence,** contact the sender of the email by telephone to verify the information before sending any money to the *'named'* beneficiary.

- **Financial Institutions and Listed Businesses:** Any suspicious email payment instructions for business transactions and personal foreign currency transactions that can be linked to email compromise, should be immediately reported as a Suspicious Transaction/Activity Report to the FIUTT.

- Any transaction/activity involving the use of compromised email should be reported to **Fraud Squad of the Trinidad and Tobago Police Service (TTPS)** at Telephone numbers: 1(868) 625-2310 or 1(868) 623-2644 or; Fraud Squad South office at 1(868) 652-8594; or by Email: fraud@ttps.gov.tt.

Dated: March 1st, 2019

Nigel Stoddard
Director (Ag.)
Financial Intelligence Unit

---END OF DOCUMENT---