FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC ADVISORY

No. 1 of 2023 2 August 2023

NOTICE TO ALL FINANCIAL INSTITUTIONS

The Financial Intelligence Unit (FIU) of The Bahamas hereby advises financial institutions and the public at large of incidences of fraudulent activities that are adversely affecting account holders of varies commercial banks in the jurisdiction. Consequently, the public is being advised to be aware of, and take note of the following.

The FIU has noticed an increase in Suspicious Transaction Reports (STRs) where commercial banks have reported instances of account holders reporting unauthorized online transfers to persons unrelated or unknown to them.

The FIU has identified the following information relative to these unauthorized transfers. The fraudulent activity involves two separate circumstances involving the victim and, in some cases, complicit or non-complicit recipients of the funds transferred.

Based on information received, victims reported the unauthorized transfers but would also note being contacted previously by a purported representative from the bank. The victims would then admit providing their account information to the purported representative. These individuals are victims of telephone banking fraud. Telephone banking fraud occurs when an individual is contacted by someone who is claiming to be from an organization you trust, whether it be a bank or a governmental agency. The purported representative would then advise that there is an issue with your account information or requesting verification of a recent transfer. They induce the account holder to provide them with their personal banking information. The purported representative then uses this information to either use the client's online banking or block the account holder from their account to use their online banking.

In other cases, victims have been noted to provide information as a result of an email purporting to come from their banking institution requesting that the account holder confirm their banking information to avoid being blocked from their account. The email will contain a link the account holder would click on to provide the information. This type of fraud is known as a phishing scam where the victim is induced to reveal sensitive information.

On the other hand, the recipient can be either a complicit or a non-complicit participant in the fraudulent scam. Based on information received from the recipient, they would have been contacted by an unknown individual through a social media platform where they are recruited by the individual for a job which requires them to determine the product or service of a business. The recipient is then advised that their account would be credited, and they were to keep a portion of these funds as payment for the completed job and the remainder should be transferred to them. These recipients genuinely believe that they were hired, and the funds were legitimately transferred. In other cases, the recipients have some knowledge of the fraudulent activity and are aware that the transfers to their accounts are unauthorized and some attempt to defraud the fraudsters by collecting the funds but not wiring out the funds to the fraudsters as instructed. These people become complicit in the fraudulent scam.

The FIU is advising the public to be aware of the following trends that have been gleaned from these reported cases.

1. The victims appear to be elderly and generally people that appear to have minimal knowledge of technology.
2. The fraudster is utilizing both telephone banking fraud and phishing scams as the primary method of inducing the victims.
3. The fraudsters are using social media platforms such as Facebook to contact the persons that would be the recipients of the unauthorized transfers.
4. The recipients are generally young adults who are unemployed or making minimal wages or students that are currently enrolled in college and in some cases high school.
5. The monies received by the recipients are required to be transferred to the fraudster via Money Gram or Western Union.

The FIU therefore advises that the following precautionary measures should be taken to avoid becoming a victim of any fraudulent activity.

1. If you receive a call or email and cannot verify that the same is legitimate it is advised to never provide personal account information via telephone or email and to visit your bank branch in person to confirm the veracity of the call or email.
2. It is advisable in general to be weary of any email that provides a link that requires the production of any personal information.
3. There are occasions where establishments would legitimately use social media platforms for recruitment. However, it has been determined that the recruitment for employment as seen in these cases is generally a part of a larger fraud scam.
4. If you are the recipient of funds that you have not legitimately earned, you are unaware of the sender or it is a transfer that you have no prior knowledge of, it is advised that this should be reported to the bank or the Royal Bahamas Police Force. Under no circumstance should the monies be withdrawn for your personal use or to remit to the fraudster.
5. For financial institutions, where such fraudulent activities are evident, the financial institution must adhere to its obligation to report these matters to the FIU as soon as practicable.

The FIU appreciates your continued support and cooperation.