FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC ADVISORY

No. 1 of 2025 17 February 2025

NOTICE TO ALL FINANCIAL INSTITUTIONS AND THE PUBLIC AT LARGE

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 being affected by various types of fraudulent activities.

The FIU has identified the unauthorized transfers, counterfeit cheques and unauthorized point of sales purchases as the most prevalent activities affecting account holders. As a result of the analysis conducted in these reports by the FIU, it is important to note that some of the identified fraudulent activity may have been directly linked to an initial phishing scam. This scam allowed the fraudster to gain access to the account holder's personal information, which in turn made the fraudulent activity possible.

UNAUTHORIZED TRANSFERS

Based on information received, account holders reported noticing unauthorized transfers upon checking their online banking profiles. The account holders provided details noting that they would have been contacted by a person purporting to be from their financial institution. The account holders were contacted via an SMS text advising that there was an issue with their account, and they should click the link to resolve the issue. Upon clicking the link, the account holders would be directed to log in to their online profile, hence providing their personal information.

These individuals are victims of SMS banking fraud. SMS banking fraud occurs when an individual is contacted via text and the fraudster uses the text message to trick account holders into providing personal or banking information. The fraudster 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.

The recipient of the unauthorized transfers can either be 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 provide a review on a product or service and thus the transfer would be compensation for their participation. Additionally, participants are contacted via social media to allow persons unknown to them to use their account for these unauthorized transfers and as such they are compensated for this service as well. 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 fraudulent activity and are aware that the transfers to their accounts are unauthorized and some complicit participants would themselves attempt to defraud the fraudsters by collecting the funds but not wiring out the funds to the fraudsters as instructed. Consequently, these participants can be charged and prosecuted for fraud.

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. Fraudsters are using social media platforms such as Facebook to contact people that would be the recipient 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 Remittance Service Provider.

COUNTERFEIT CHEQUES

The FIU is also advising the public and persons conducting business as a Law Firm to be advised of a scam involving counterfeit cheques.

This scam typically begins with an email or a phone call to a financial institution, where the fraudster requests assistance with a loan repayment dispute. A majority of the Suspicious Transaction Reports (STRs) received involved a law firm, with the fraudster seeking help related to a loan repayment issue. The fraudster informs the law firm of the dispute, and then the person allegedly accused of defaulting on the loan contacts the firm, claiming they were made aware that the lender had sought advice from the firm. The borrower expresses a desire to settle the loan by sending the defaulted amount to the law firm. The firm eventually receives a cheque from the supposed borrower. However, when the cheque is deposited at the bank and processed, it is discovered to be counterfeit. In the cases reported, the lender is using the alias "Mr. Chambers," while the borrower who settles the loan through the firm is using the alias "Andrew." The analysis of these STRs suggests that the fraudster is deliberately using names of individuals who are familiar within the community.

CRUNCHYROLL – UNAUTHORIZED POINT OF SALE PURCHASES

The FIU has dubbed the third most prevalent scam, the "Crunchyroll Scam." The Crunchyroll scam involves incidences of unauthorized point of sales purchases (POS). The commonality between all the STRs relative to this scam involves account holders reporting unauthorized POS purchases linked to Crunchyroll. Based on research conducted by the FIU Crunchyroll is a digital streaming platform that specializes in anime, manga and Asian dramas.

The account holders in this regard are mostly nationals having accounts at the same financial institution. The POS amounts range from $49.99 to $50.01. Although a determination was made that the commonality between the victims is that they are all account holders at the same financial institution, it is still unclear how the transactions occur. Therefore, persons are advised that if they become aware of transactions involving this online platform, to please report the matter to your financial institution as soon as possible.

Therefore, the FIU advises that considering the advancements in technology and the evolution of the digital age, it is crucial to remain vigilant and cautious when navigating any online platforms. Fraudsters are increasingly sophisticated, using tactics such as phishing emails, fraudulent websites, and SMS bank fraud to steal personal information and financial details. **NEVER** share sensitive data like passwords, PINs, or credit/debit card numbers in response to unsolicited messages, whether via email, text, or social media. Be cautious of unfamiliar links and attachments, especially if they appear to come from a trusted source, as these could be malicious attempts to access your personal information. Always verify the legitimacy of any communication with the official organization directly before acting. Protecting yourself from these fraudulent activities requires constant awareness and proactive measures. Stay informed, stay cautious, and never underestimate the potential risks of financial and online fraud.

The FIU appreciates your continued support and cooperation.

Mr. Emrick K. Seymour Sr., CM, KPM
Director
Financial Intelligence Unit
Poinciana House, 31B
Annex Building, 2nd Floor
East Bay Street
P.O. Box SB-50086
Nassau, Bahamas
Tele: (242) 397-6300/ (242) 326-3815
Fax: (242) 322-5551
Email: director.fiu@fiubahamas.bs