FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC ADVISORY

No. 4 of 2025 23 September 2025

HEIGHTENED ALERT REGARDING SOCIAL MEDIA COMPROMISE AND IMPERSONATION SCAMS

The Financial Intelligence Unit (FIU) of The Bahamas is issuing this advisory to raise awareness about the increasing prevalence and sophistication of social media compromise and impersonation scams. These illicit activities pose a significant threat not only to individual users but also to the integrity of the financial system. We urge all individuals and financial institutions to exercise extreme caution.

Elevated Threat Landscape:

The FIU has observed a concerning trend in the exploitation of social media platforms for fraudulent purposes. Scammers are employing increasingly deceptive tactics to compromise user accounts and impersonate individuals, often with the ultimate goal of financial gain. These scams can manifest in various forms, including:

- **Creation of Fake Profiles:** Impersonators are creating convincing fake profiles that mimic individuals known to the target, including friends, family members, business associates, and even representatives of financial institutions or government agencies. These fake profiles are used to request funds, gather sensitive information, or facilitate other illicit activities.

- **Investment and Romance Scams:** Scammers often use compromised or fake profiles to lure victims into fraudulent investment schemes or develop fictitious online relationships to manipulate them into sending money. These schemes can result in substantial financial losses for individuals.

- **Unauthorized Account Access:** Malicious actors are gaining control of legitimate social media accounts through methods such as phishing, malware distribution, and the exploitation of weak passwords. Compromised accounts are then used to disseminate fraudulent solicitations to the victim's network.

Recommended Actions for Individuals:

1. **Adopt Robust Password Practices:** Utilize strong, unique passwords for all social media accounts. Passwords should include a combination of uppercase and lowercase letters, numbers, and symbols. Regularly update your passwords and avoid reusing them across different platforms. Consider using a reputable password manager.

2. **Exercise Caution with Online Interactions:** Be highly suspicious of unsolicited messages, friend requests from known and unknown individuals, and links shared on social media, even if they appear to come from trusted contacts. Verify the authenticity of any requests for personal or financial information through alternative communication channels.

3. **Protect Personal Information:** Limit the amount of personal information you share publicly on social media platforms. Scammers can use this information to craft more convincing impersonation attempts. Be particularly cautious about sharing details related to your finances or travel plans.

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