FINANCIAL INTELLIGENCE UNIT OF THE BAHAMAS

PUBLIC ADVISORY

No. 3 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.

Specific Risks to Institutions:

- **Business Email Compromise:** Employees of institutions are being scammed into making unauthorized transfers to email addresses that appear to be that of legitimate clients but are fraudulent.

- **Financial Losses:** Institutions may face liabilities if their security measures are deemed inadequate.

- **Reputational Damage:** Scams targeting clients of institutions can severely damage the institution's reputation and erode public trust.

- **Operational Disruptions:** Investigating and resolving these incidents can consume significant resources and disrupt normal operations for institutions.

Recommended Actions for Institutions:

1. **Monitor social media for Brand Impersonation:** Actively monitor social media platforms for brand impersonation and take swift action to report and remove fraudulent profiles or content.

2. **Implement Strong Authentication Measures:** Ensure that robust authentication mechanisms, including multi-factor authentication where feasible, are in place for all internal systems and client-facing platforms.

3. **Enhance Employee Awareness Training:** Conduct regular and comprehensive training programs for all employees on the risks associated with scams, particularly concerning Business Email Compromise and potential manipulation of client accounts.

4. **Review and Update Security Policies:** Regularly review and update cybersecurity policies and procedures to address the evolving threats posed by fraudsters.

5. **Promote Client Education:** Proactively educate clients about the risks of scams through various channels, including website notices, email communications, and social media posts. Provide clear guidance on how to identify and avoid these scams.

6. **Strengthen Client Communication Protocols:** Implement robust protocols for verifying client identities and the legitimacy of transaction requests received through all channels. Educate clients about the risks and encourage them to use secure communication methods.

7. **Establish Clear Reporting Channels:** Ensure that clients have clear and accessible channels for reporting suspected scams and fraudulent activity targeting their accounts.

The FIU remains committed to safeguarding the financial integrity of The Bahamas and protecting its citizens and institutions from financial crime. We urge all stakeholders to take these recommendations seriously and work collaboratively to combat the growing threat of the various types of fraudulent activities. Your vigilance and proactive measures are crucial in maintaining a secure digital environment.

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