BOC 中國銀行

Notice: Protect Yourself Against Money Mule Scams and Criminal Networks

As technology continues to advance rapidly, financial crimes are becoming increasingly sophisticated and complex. Criminal networks are exploiting these technological developments to orchestrate scams and recruit money mules, who may unknowingly facilitate the movement of illicit funds. This notice aims to inform you about these emerging threats as vulnerable people, often international students and non-permanent residents, are targeted to act as money mules.

What Are "Money Mules"?

The term "money mule" refers to an individual who moves illegally obtained money for others. Criminal networks will use a money mule, their identification, and/or their account details to distance themselves from these illicit funds. Money mules may move money using methods including but not limited to cash transfers, bank accounts, checks, digital currencies, or remittance services. They may use personal or third-party accounts, sometimes even opening business accounts.

Some money mules sell their personal bank accounts to criminals, often responding to ads seeking such accounts. Many money mules are unaware that their actions are illegal, believing that they are engaged in legitimate employment. It is crucial for you to stay alert and report any suspicious activity/inquiry to local authorities to avoid becoming a money mule.

Potential Targets and Recruitment Channels

Students and non-permanent residents from East Asia are at higher risk of recruitment by criminal networks. Characteristics of potential targets include but are not limited to:

- Individuals with international passports and/or proof-of-age cards who identify as students;
- Targeted by online games and advertisements;
- Approached by migration agents and/or international student support organizations who are in frequent contact with students and trusted with personal details;
- Targeted when they first arrive in a country other than their home country or at the time of departure.

Criminal networks use a variety of means to recruit foreign students as money mules through face-to-face contact or online platforms.

- International students may be recruited as money mules to earn money while studying, partly due to their familiarity with *daigou* (i.e., individuals or companies who purchase goods abroad for clients in China, often for a profit), and needs for USD while residing in the U.S.;
- Individuals may be offered payment in exchange for opening accounts or registering companies in their names, or for using existing accounts, which are then used by criminal networks to launder funds.

Important Steps to Take

If you encounter possible money mule requests or activity, including outreach from a potential criminal network, please consider taking the following important steps:

- **Do Not Engage**: Avoid interacting or cooperating with the individuals or groups involved to protect yourself from becoming implicated.
- **Contact Local Law Enforcement:** Immediately report the incident to local law enforcement or relevant agencies such as financial crime units, anti-money laundering bodies, and/or cybercrime divisions.
- **Protect Your Personal Information**: Secure your personal and financial information. If you suspect that your Bank of China US Branches (BOCUSA) banking information has been compromised, please report the incident immediately to BOCNY at contactus@bocusa.com or call BOCNY Corporate and Personal Banking Services at 1 (212) 935-3101 (Mon–Fri, 9:00 a.m. – 3:30 p.m. (EST)) or Queens Branch at 1 (212) 925-2355 (Mon–Fri, 9:00 a.m. – 4:00 p.m. (EST), Sat 10 a.m. – 3p.m.(EST)). Please note that BOCUSA may be required to report the incident to law enforcement and/or appropriate regulatory authorities.

Important: BOCUSA will never ask for your card PIN number, temporary PIN number, or online banking password.

This Notice is provided for informational purposes only, and is not intended nor should it be construed as legal advice. Please contact a legal advisor and/or law enforcement, as appropriate, if you have incurred financial loss or unintended disclosure of Personal Identifiable Information (PII) or other confidential information.