Bank Scam Notice

Text scams, email scams, and telephone scams are increasing of late against banking consumers. This notice provides basic information about how such scams are being perpetrated so that you can stay alert.

Bank text scams and email scams often share common characteristics. For example:

A bank text scam or email scam often appears to be a legitimate message from a financial institution. Such scams may request that you click on a link in an SMS or email message concerning a transaction, or ask you to change your login password. The scam tries to create a sense of urgency so that you will act immediately and without caution.

Telephone scams can take many forms and share some common characteristics. For example:

1) **Impersonation of Government Authorities**: Fraudsters often pose as government officials, including embassy or consulate representatives, customs personnel, public security bureau officers, prosecutors, or even bank employees. They employ tactics to mask their true identities and have the ability to manipulate caller IDs.
2) **Fabrication of Criminal Charges:** Fraudsters may fabricate false allegations against you or your family members, claiming your or your family's involvement in identity theft or other criminal activities. They may present seemingly authentic law enforcement documents such as "Arrest Warrants" or "Police Reports." To further isolate you, they may request that you sign a "Confidentiality Agreement" preventing you from discussing the matter with anyone, including your parents, friends, or Bank of China New York Branch ("BOCNY"). In some instances, they may create a false environment of video surveillance to induce panic and prevent you from seeking outside help. **Remember, feeling pressured is a warning sign that something may be amiss**.
3) **Coercion and Money Transfers:** Fraudsters employ coercive tactics, pressuring you to "cooperate with the investigation." They use various excuses, such as "paying guarantees," "checking funds," or "transferring funds to secure accounts," to convince you to wire money to them.

Should you receive suspicious text messages, email messages, or phone calls, please consider taking the following steps:

- **Stay Alert:** Be cautious of unsolicited phone calls and terminate them immediately if they raise suspicion.

- **Safeguard Your Personal Information:** Any call requesting personal or financial details should raise a red flag. Hang up immediately. Refrain from clicking on links in text or email messages from unknown sources, and exercise caution with regard to advertising or investment opportunities. Pay close attention to the email addresses soliciting your information, and do not click on any links in an email sent from an email address that you do not recognize (including spoof email accounts and websites with slight variations on legitimate email addresses or URLs). Before a request is authenticated, do not provide any personal information, including account logins and passwords, PIN numbers, validation codes, bank account numbers, debit card numbers, and/or your Social Security Number.

- **Avoid Wire Transfers to Unverified Recipients:** Never wire money to individuals who claim to be government agents, such as those requesting that wires be sent to accounts located in Hong Kong. Scammers target wire transfers because they are difficult to recover.

- **Courier Notifications:** Be wary of any notifications claiming to be from a courier service regarding a package. These are typically fraudulent.

- **Carefully Verify Payment Information:** If you are making payments through a not-over-the-counter channel (e.g., by phone or computer), please carefully verify the payment information.

- **Review Bank Statements Regularly:** Review account statements regularly to ensure all charges are accurate.

Please note that the above are only illustrative examples, and not the only ways a fraud can be perpetrated. Stay alert and vigilant!

In case you encounter any suspected fraudulent activity, please consider taking the following steps:

Report to Bank of China New York Branch: If you suspect that your BOCNY 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 (9 a.m. – 5 p.m. Mon – Fri).

Contact Local Law Enforcement: To help stop fraud, you may report the incident to the police or your local FBI office. BOCNY also may report customer incidents to law enforcement and/or appropriate regulatory authorities as required.

Important: BOCNY 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 appropriate authorities if you have incurred financial loss or unintended disclosure of Personally Identifiable Information (PII) or other confidential information.