Warning: Beware of Bank Impersonation Scam Calls

The banking industry, including Bank of China USA, has recently observed a significant increase in Bank Impersonation Scam Calls. Scammers may attempt to impersonate Bank of China USA employees, by spoofing our official phone number, (212) 935-3101, or other numbers affiliated with the Bank, to gain your trust and/or reduce your vigilance. Do not rely on Caller ID—scammers can make any number or name appear on your caller ID. Do not provide private, sensitive information (like account details or passwords) to a caller, even if they claim to be from Bank Of China USA. Watch out for a false sense of urgency on the calls, and hang up if the call seems suspicious—it's safer to hang up and contact us directly to verify the situation.

We may need to verify personal information if you call us, but we will never ask for your login credentials, PIN, or one-time security codes over the phone. If you receive a suspicious call, hang up immediately and contact us at contactus@bocusa.com or call BOCNY Corporate and Personal Banking Services at 1 (212) 935-3101 (9 a.m. – 4 p.m. Mon – Fri) for the New York City Branch and 1 (212) 925-2355 ext. 8800 (9 a.m. – 4 p.m. Mon – Fri, 10a.m – 3p.m. Saturday) for the Queens Branch. Please stay vigilant to protect your information.

Please also always be vigilant when you receive any contact or materials not sent by bank personnel that you are familiar with or the entity you have a formal relationship with. Always check the domain address that it is in fact coming from @bocusa.com. If you receive any materials claiming to be from the Bank of China USA, please feel free to reach out to us to verify the authenticity.

When you receive any contact or communication about your banking relationships or information, please kindly consider the following:

- **Verify Communications**: Always ensure that any communication to you is legitimate. If you receive unexpected requests for personal or financial information via phone, email, or text message, please verify it by contacting the Bank directly through our official channels.
- **Secure Your Information**: Never share your personal information, account details, or passwords with anyone. We may contact you about your information primarily for verification and service processing purposes and we will never ask for sensitive information such as passwords over the phone.
- **Monitor Your Accounts**: Regularly review your account statements and activity to spot any unauthorized transactions. If you notice anything unusual, please report it to the Bank immediately. You may also need to follow up with law enforcement if you ultimately become a victim of financial fraud.
- **Beware of Scams**: Be cautious of unsolicited offers, promises of high returns, or any communication that seems suspicious. Fraudsters may try to impersonate our company or claim to offer services on our behalf.

You can report impersonation scams to the U.S. Federal Trade Commission @ https://reportfraud.ftc.gov/