# A D V I S O R Y

## PROLIFERATION OF FRAUDSTERS POSING AS "GOVERNMENT EMPLOYEES" AND/OR "BANK REPRESENTATIVES"

The Securities and Exchange Commission (SEC) warns the public against the continued proliferation of fraudulent schemes involving individuals who falsely represent themselves as government employees and/or bank representatives.

The Commission has received reports that these individuals contact unsuspecting victims through social media platforms, including Telegram and Viber, as well as through phone calls, text messages, emails, and other electronic communication channels, claiming to be affiliated with legitimate government agencies or banking institutions. These fraudsters employ deceptive tactics to induce victims to disclose sensitive personal and financial information or to authorize fraudulent transactions.

This scheme constitutes an impersonation scam, commonly referred to as bank phishing or "vishing," where perpetrators exploit trust and urgency to gain unauthorized access to confidential information, resulting in financial loss and/or compromise of personal data.

The modus operandi observed is consistent with previously reported incidents of phishing and vishing targeting banking clients and the general public.

**PUBLIC ADVISORY**

In light of the foregoing, the SEC strongly advises the public to exercise utmost caution and vigilance and to observe the following precautions:

- **Do not disclose** personal, banking, or financial information (e.g., OTPs, passwords, account numbers) to any individual making unsolicited calls or messages.
- **Verify directly** with your bank or relevant government agency through official and publicly listed contact details before taking any action.
- **Be wary of urgent or threatening messages** that pressure immediate compliance or transaction approval.
- **Do not click** suspicious links or attachments sent via SMS, email, or messaging applications.
- **Report immediately** any suspicious activity to your bank, the concerned government agency, or appropriate law enforcement agencies.

The public is further reminded that legitimate government agencies and financial institutions do not request sensitive information such as passwords, one-time PINs (OTPs), or account credentials through phone calls, text messages, or informal online channels.

The SEC urges everyone to remain vigilant and report any similar fraudulent activities to the Commission or appropriate authorities for proper investigation and action.

Should you have your inquiries and official assistance, you may send it to the Enforcement and Investor Protection Department at imessage@sec.gov.ph .

**For the information and guidance of the public.**

Issued on 14 May 2026 in Makati City, Philippines.