PUBLIC ADVISORY
Beware of APK Files and Online Loan Scams

The Securities and Exchange Commission (SEC), through the Financing and Lending Companies Department (FinLenD), **warns the public** against installing unauthorized or suspicious application files (commonly known as **APK files**) received through links, messages, or online meetings.

Recent reports received by the Commission reveal a **growing modus operandi** involving the following scheme:

Unidentified individuals pose as representatives of legitimate institutions and invite victims to participate in online meetings or communications. During these interactions, victims are instructed to download files or applications outside of official app stores (e.g., Google Play or Apple App Store). These files, often in APK format, are used to gain unauthorized access to the victim's mobile device.

Once installed, such applications may:

- access personal and financial information stored in the device;
- intercept messages, including one-time passwords (OTPs);
- enable unauthorized transactions; and
- facilitate the availment of loans or other financial obligations **without the knowledge or consent of the account holder**.

In one reported case, the victim's mobile device was compromised after installing an APK file during an online meeting. Thereafter, the perpetrators were able to access multiple financial accounts and **successfully obtain a loan using the victim's account credentials**, resulting in financial liability on the part of the victim.

REMINDERS TO THE PUBLIC

The SEC strongly advises the public to observe the following:

1. **Do NOT install APK files or applications from unknown or unverified sources.** Only download applications from official platforms such as Google Play Store or Apple App Store.

2. **Be cautious of unsolicited messages or calls.** Government agencies and legitimate financial institutions **do not require the installation of external applications** through unofficial links.
3. **Never share sensitive information.** Do not disclose your passwords, PINs, OTPs, or biometric verification to any person or platform.
4. **Verify before you act.** Confirm the identity of any individual or entity requesting access to your personal or financial information.
5. **Immediately report suspicious activities.** If you suspect that your account has been compromised, promptly contact your financial service provider and report the incident to the appropriate authorities.

REPORTING AND ASSISTANCE

The public is encouraged to report incidents involving suspicious online lending activities or unauthorized loan transactions through:

📞 **14732 (1-4SEC)**
🌐 SEC iMessage Portal: https://imessage.sec.gov.ph/
🌐 SEC Official Website: https://www.sec.gov.ph

For incidents involving fraud, identity theft, or unauthorized access to accounts, the public may also coordinate with:

- Philippine National Police – Anti-Cybercrime Group (PNP-ACG)
- National Bureau of Investigation – Cybercrime Division (NBI-CCD)
- Cybercrime Investigation and Coordinating Center (CICC)