Scammers Impersonating People’s Republic of China (PRC) Law Enforcement Targeting PRC Citizens in the United States

(U) This document is: [Unclassified].
(U) Please direct comments and queries regarding this product to the FBI Office of Partner Engagement’s Enhanced Engagement Unit at OPE-EEU@fbi.gov.

AWARENESS REPORT

The FBI has received various reports regarding telephone scammers targeting citizens from the People’s Republic of China (PRC) who are in the United States on nonimmigrant student visas\(^1\) to fraudulently obtain money. Scammers typically claim to be a PRC law enforcement or government official, representative from a financial institution, or a shipping company and use fear, intimidation, and threats to target PRC students at US colleges and universities. This Public Safety Awareness Report is for situational awareness and to facilitate law enforcement efforts to connect victims to federal resources, identify potential telephone-related extortion schemes, promote awareness to educational institutions with international or exchange student programs, and warn the public to report any individuals instructing, demanding, or threatening to send money to avoid fictitious law enforcement penalties.

BACKGROUND OF INCIDENTS

Following are examples drawn from incidents of fraudulent telephone calls resulting in significant monetary losses to Chinese students in the United States:

1. A call from an individual impersonating a PRC consulate or embassy official who informed the Chinese student that his/her passport was used to illegally open bank accounts to commit crimes. The student was transferred to a second individual claiming to be a law enforcement official or criminal prosecutor who confirmed the student’s personally identifiable information (PII). The scammers demanded the victim pay a fee to

\(^1\) According to U.S. Citizenship and Immigration Services (USCIS), there are two nonimmigrant visa categories for persons wishing to study in the United States, which are commonly referred to as F and M visas. (www.uscis.gov).
prove his/her innocence and avoid consequences such as arrest, visa revocation, extradition, imprisonment, or suspension of bank accounts.

2. A call from an individual impersonating a representative from a shipping company stated that a package addressed to the student was undeliverable because it was intercepted by the PRC customs for containing illegal drugs and fraudulent credit cards. The student was transferred to another scammer impersonating a PRC customs agent or law enforcement official who accused the student of involvement in criminal activity. A monetary fee was demanded from the victim to avoid legal penalties.

3. A call from an individual impersonating a representative from a PRC-based financial institution informed the student that his/her name was used in money laundering and fraudulent activities resulting in identity theft. The scammer transferred the call to another impersonator claiming to be from a PRC police department, who accused the student of fraud and other criminal activity. The scammers threatened the victim with extradition and jail time, and demanded money be sent as proof his/her innocence.

Complaints received by the FBI indicated that the victims were asked to provide sensitive information such as name, date of birth, PRC ID number, passport number, email address, phone number, financial account information, other personal information (work, family, etc.), and a photograph. Victims were also told that, due to the sensitive nature of the ongoing “criminal investigation,” he/she was not permitted to discuss the matter with anyone, and was asked to sign a non-disclosure agreement.

**GUIDE FOR PUBLIC AWARENESS**

There are many ways scammers can obtain PII. As a best practice, the public should limit the amount of personal information shared online, including social media sites. Phone scammers typically convey a sense of urgency by using fear, intimidation, and threats to get a victim to send money right away.

**Be Aware** of unsolicited calls by people claiming to work for the PRC government, law enforcement agencies, shipping companies (especially when not expecting a package), or financial institutions. Scammers often disguise their phone numbers (called “spoofing” 

**Be Cautious** of any unexpected communications—whether in-person, by phone, or online—requesting PII, financial information, family details, or money.

**Verify** the authenticity of the communication through known means such as official website, phone number, physical office location, and retail facilities. Scammers may impersonate legitimate law enforcement or government officials by using publically

---

2 According to the Federal Trade Commission, the term “spoofing” is “the practice of abusing the Caller ID system (Caller ID spoofing) so that a false number appears on a consumer’s Caller ID screen.” (www.ftc.gov).
available names from agency websites. Scammers may also spoof the caller ID information or transfer calls to people claiming to be PRC law enforcement authorities. Instead of accepting these call transfers, recipients are encouraged to independently contact the respective law enforcement agency/entity through official channels, such as an email address or phone number, on the official agency website to confirm the identity of those contacting you.

INFORMATION HELPFUL TO LAW ENFORCEMENT

Reporting this type of criminal activity not only helps direct victims to federal resources, but also increases the likelihood of successful law enforcement investigations. The following information can help identify leads or patterns of criminal activity:

- Identifiers of the perpetrator(s) (e.g., name, telephone number, bank account details)
- Details on how, why, and when you believe you were defrauded
- Actual and attempted loss amounts
- Details about the impersonation
- Other relevant information that can support your complaint

TIPS TO PROTECT AGAINST FRAUD

- Always be suspicious of unsolicited phone calls.
- When targeting international students, scammers may build their credibility by revealing information about the student’s immigration status or details about the school program.
- Never give money or personal information to unknown individuals who initiate contact for the purpose of requesting money via wire transfers, money orders, Bitcoin, cryptocurrency, or third-party prepaid debit or gift cards.
- Scammers count on a victim’s lack of knowledge and fear of implications regarding blackmail and fraud schemes and often change their tactics to remain successful.
- Trust your instincts. If an unknown caller makes you uncomfortable or says things that sound suspicious, just hang up.

ONLINE RESOURCES

- If you or others have been victimized by scammers, or if you are unsure, contact your local FBI field office (https://www.fbi.gov/contact-us/field-offices), and report details of the incident to appropriate personnel (e.g., campus police) at your college or university.
- All types of fraud schemes and scams can be reported to the FBI’s Internet Crime Complaint Center (IC3) at www.ic3.gov. For more information about scams and to

- To file a complaint with the Federal Trade Commission (FTC), visit: https://www.ftccomplaintassistant.gov/?utm_source=takeaction#crnt&panel1-1.
- FBI Victim Services Division resources: https://www.fbi.gov/resources/victim-services.

(U) THE INFORMATION IN THIS PUBLIC SAFETY AWARENESS REPORT (PSAR) PREPARED BY THE FBI OFFICE OF PARTNER ENGAGEMENT AND IS PROVIDED TO ENHANCE PUBLIC SAFETY AND FOR SITUATIONAL AWARENESS PURPOSES ONLY. NO INFORMATION CONTAINED IN THIS PSAR, NOR ANY INFORMATION DERIVED THEREFROM, MAY BE USED IN ANY PROCEEDING (WHETHER CRIMINAL OR CIVIL), TO INCLUDE ANY TRIAL, HEARING, OR OTHER PROCEEDING BEFORE ANY COURT, DEPARTMENT, AGENCY, REGULATORY BODY, OR OTHER AUTHORITY OF THE UNITED STATES WITHOUT PRIOR APPROVAL FROM THE FBI. THESE RESTRICTIONS APPLY TO ANY INFORMATION EXTRACTED FROM THIS DOCUMENT AND USED IN DERIVATIVE PUBLICATIONS OR BRIEFINGS.

(U) To report any leads, threats, and suspected criminal activity, please visit, https://www.fbi.gov/tips or contact your local FBI Office: https://www.fbi.gov/contact-us.