OFFICE of PRIVATE SECTOR
LIAISON INFORMATION REPORT (LIR)

GOVERNMENT FACILITIES SECTOR

24 July 2020 **LIR 200724004**

Criminals are Posing as Chinese Law Enforcement in Phone Scams to Target Chinese Citizens on Student Visas at U.S.-Based Colleges and Universities for Financial Gain

References in this LIR to any specific commercial product, process or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service or corporation on behalf of the FBI.

The FBI Albany Field Office, in coordination with the Office of Private Sector (OPS), prepared this LIR to inform academia financial offices and other financial institutions regarding telephone-based scams targeting Chinese citizens on student and/or work visas. Recent reporting from several sources and multiple states indicates scammers may be employing a variety of tactics to defraud Chinese students of money, resulting in large dollar losses often in excess of $100,000 per victim. In most of these schemes, criminals impersonated Chinese law enforcement agencies, consulates, embassies, banks, or government officials, and typically advised the victim they were under investigation in China for varying criminal activities.[a] Examples of these schemes included, but were not limited to, the following:

- The student received a call from a Chinese consulate or embassy and was told that someone was using the student's passport and opening bank accounts in their name for criminal activity, or their passport was used in a criminal case. The student was then telephonically transferred to a police department or law enforcement official, who confirmed the student's name and/or accounts were being used in a fraud case or a criminal investigation. Sometimes the student was also telephonically transferred to a criminal prosecutor, who then informed the student that money must be paid to avoid a consequence (such as arrest, revocation of their visa, extradition, imprisonment, or having their financial accounts frozen), to pay bail or bond, or to prove their innocence. In some cases, the student received the initial call directly from someone impersonating a Chinese law enforcement official or police department instead of a Chinese consulate or embassy.

- The student received a call from a shipping company, such as DHL or UPS, saying a package was undeliverable or was intercepted at Chinese customs and contained some kind of illegal item, such as drugs or fraudulent credit cards, and the package had the student's name and residential address on it. The student was then telephonically transferred to a Chinese customs agent, law enforcement official, or police department, and told they were suspected of being involved of criminal activity. The student was ultimately told money must be paid to avoid a consequence (such as arrest, revocation of their visa, extradition, imprisonment, or having their financial accounts frozen), to pay bail or bond, or to prove their innocence.

- The student received a call from a Chinese bank or financial institution and was told an account in their name was used in money laundering and fraud activities, or bills from an account in their name hadn't been paid. Typically, the call was from a bank from which the student had never had

[a] For more details on a similar Chinese Consulate extortion scheme see LIR titled, "Robocall Scammers Impersonate the Chinese Consulate to Extort Money" dated 12 September 2019.

accounts. The student was then advised they may be a victim of identity theft and the call was transferred to a Chinese police department. The police department then informed the student they had reason to believe the student was involved in a large-scale fraud investigation or other criminal activity. Extradition and jail time were usually threatened, and the student was convinced to send money in order to prove their innocence.

In nearly all of the referenced schemes, the student was asked to provide personal and sensitive information, to include, but not limited to: name, date of birth, Chinese ID number, passport number, email address, phone number, work experience, family situation or information, financial account information, and photo. Oftentimes, the student was told that because it was a sensitive criminal investigation, they were not permitted to discuss the matter with anyone and were asked to sign a non-disclosure agreement.

The following are some best practices to identify related suspicious activities and similar scams. These suspicious activities include but are not limited to any individual, group, or activity and should be observed in context and not individually.

- Students should be aware of unsolicited calls by people claiming to work for a Chinese police department or other law enforcement agency, a Chinese consulate or embassy, a shipping company (when not expecting packages), and a China-based bank with whom they do not have accounts. Students should also be cautious of any documents or identification provided to them by these individuals.

- Students should be cautious of any unsolicited phone calls, emails, and text messages requesting personally identifiable information, bank account information, or money.

- Verify the authenticity of the communication through known means (i.e., official website, phone number, physical office location, retail facilities, etc.). Criminals use official-sounding names to make you trust them by impersonating and using the name of a legitimate law enforcement, consulate and/or embassy official. To make their call seem legitimate, scammers may also use internet technology to disguise their area code. Scammers will also routinely transfer your call to people claiming to be authorities. Instead of accepting these call transfers, independently contact the respective 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.

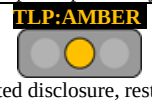
If you or someone you know believes you were the victim of the scam, contact your local FBI Field Office, report details regarding the incident to your academic institutions' security office, the U.S. Federal Trade Commission (FTC) at www.ftc.gov, and the FBI's Internet Crimes Complaint Center (IC3) at www.ic3.gov.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. Direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.