



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

GOVERNMENT FACILITIES SECTOR

31 August 2022

LIR 220831003

Scammers Posing as US Law Enforcement are Targeting Chinese Citizens Attending US Academic Institutions 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 Seattle Field Office, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform US academic institutions of telephone-based scams targeting Chinese citizens attending U.S. universities and colleges through the student visa program.^a Reporting indicates that scammers target students using spoofed^b phone numbers showing the call is originating from government agencies, including immigration offices and the Consulate General of the People's Republic of China. The scammer claims there is evidence the student is involved with a crime, often involving drug trafficking, human trafficking, or smuggling, and the student must pay a fine or surrender their money for investigation.

- In July 2022, six Chinese students at a US university reported receiving calls appearing to be from the Consulate General of the People's Republic of China and China Customs. The callers spoke Mandarin and informed the students they had been tied to a smuggling ring in China. The calls were transferred to various alleged law enforcement agencies in China who told the students they must pay a fine to clear their names. The callers coerced students into asking friends and family for money. The students reported losses upwards of \$800,000 in total, paid through wire transfer from their foreign bank accounts.
- In July 2022, a Chinese student received a call appearing to be from the Consulate General of the People's Republic of China claiming the student was tied to a bank account which was under investigation. Under the guise of an investigation, the caller convinced the student to transfer all their money and passport information to the caller.
- In February 2022, an international student received a call appearing to be from Immigration and Customs Enforcement claiming the student had an arrest warrant for drug trafficking and operating as a money mule. The caller told the student they had to surrender themselves to law enforcement or pay a fine. The student paid over \$30,000 through Zelle and gift cards to satisfy the alleged fine.

^a For information on other telephone-based government impersonation scams targeting Chinese students involved in the student visa program, see LIR 200724004 titled, "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," dated 24 July 2020.

^b Spoofing occurs when a caller deliberately falsifies information transmitted to a caller ID display to disguise their identity, often making it appear that the call is coming from a trusted organization, such as a government agency. *Source:* Website | FCC | "Caller ID Spoofing" | fcc.gov/spoofing | accessed on 21 July 2022.



Academic institutions should alert their international students to this scam, provide indicators that they are being targeted, and suggest ways they can avoid becoming victims. Suspicious activities/indicators include but are not limited to any individual, group, or activity (these indicators should be observed in context and not individually).





- Students should be aware of unsolicited phone calls from individuals claiming to be from government agencies, and independently verify the authenticity of communications. Authenticity should be verified through a known and trusted avenue, such as independently calling the organization or visiting the organization's physical location. Since scammers spoof phone numbers to make it appear they are calling from legitimate organizations, searching the phone number online or relying on caller ID are not sufficient means for verifying authenticity.
- Students should be cautious of anyone requesting they provide personally identifiable information, financial information, or money. Scammers will use threats in an attempt to coerce students into quickly providing personal details. If a student suspects the call is legitimate, the best step is to ask for the caller's name, hang up, and call the agency using an authenticated phone number to verify the claims.
- Unlike a legitimate government agency, scammers often demand payment by wire transfer, gift card, or virtual currency. These forms of payment are difficult to track and almost impossible to recover. A legitimate government agency will never initiate contact with a student and demand immediate payment.

If you believe you or anyone you know was a victim of this scam, report the incident to your academic institution's security office, the FBI's Internet Crimes Complaint Center (IC3) at www.ic3.gov, and the U.S. Federal Trade Commission (FTC) at www.ftc.gov.

OPS's Information Sharing and Analysis Unit disseminated this LIR. 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>.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>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.</p>	<p>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.</p>
<p>TLP:WHITE</p>  <p>Disclosure is not limited.</p>	<p>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.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>