

**OFFICE of
PRIVATE SECTOR****Liaison Information Report (LIR)****CROSS-SECTOR****27 SEPTEMBER 2023****LIR 230927009****Criminal Actors Posing as People's Republic of China Law Enforcement Officers to Defraud Chinese Nationals Studying in the U.S.**

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 does not and will not target people based on their race or ethnicity.

The FBI Criminal Investigative Division, and the Boston, Buffalo, Philadelphia, and Springfield Field Offices, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform the U.S. academic community of an emerging trend in financial fraud schemes perpetrated against Chinese nationals enrolled at U.S. universities by criminal actors posing as People's Republic of China (PRC) police officers. The criminal actors posing as PRC police officers leveraged tactics such as monitoring victims via video calls and physically surveilling them to perpetrate the schemes. Monetary losses to the identified victims exceeded \$3 million dollars.

- In March 2023, a criminal actor posing as a PRC police officer named “Mr. Zhao,” contacted a Chinese university student in Pennsylvania. The criminal informed her she faced charges for broadcasting illegal fundraising messages and requested her to wire bail money to a bank in Hong Kong. After she wired \$193,000, the criminal requested more money and instructed the victim to tell her family in China she broke her leg and needed money for surgery. Zhao informed her she could pay off the remaining debt by assisting Zhao as a ‘specialist.’ Under Zhao’s instruction, she conducted a video call with a Chinese student attending a university in Massachusetts, pretended to have been hit by a car driven by the Boston student, and requested payment from the student.
- In March 2023, the same criminal actor posing as “Mr. Zhao” contacted a Chinese student attending a university in New Jersey. The criminal told the victim he faced extradition to China for transmitting illegal tax documents and instructed him to wire \$310,000 in bail money to a bank in Hong Kong. Zhao provided the victim with a document outlining criminal charges against him, which included the victim’s national identification photo. The criminal placed him on a 24/7 video call, and instructed him to travel to a Philadelphia hotel where the previous victim, who was continuing to act under Zhao’s instructions, took his electronics, provided a burner phone, and escorted him to a room. Zhao instructed the victim to cease contact with friends and family, and post a false story on social media about returning to China for a family emergency.
- In February 2023, a criminal actor who claimed affiliation with a U.S. retailer contacted a Chinese student attending a university in New Jersey. The criminal actor told the victim she was the victim of identity theft and offered to connect her to the Chinese police to report the incident. The victim was transferred to a criminal actor posing as a Chinese police officer who informed her there was a warrant for her arrest due to her connection to an international child kidnapping case. At the

**OFFICE of
PRIVATE SECTOR****Liaison Information Report (LIR)**

criminal actor's direction, the victim sent a selfie photograph and her location to the criminal actor every two hours. The criminal actor told her the Chinese police recovered \$1.6 million in connection to her case and to expect a deposit for that amount to appear in her bank account. After she received the \$1.6 million in her bank account, she converted the money to cryptocurrency and sent it to the criminal actor.

- In October 2022, a Chinese university student in Illinois received a text message indicating Chinese authorities had flagged a package sent by the victim to the PRC. The victim called the phone number provided in the text and spoke to a criminal actor posing as a PRC police official who stated a criminal enterprise used her personal information in furtherance of criminal activity. The criminal actor possessed the victim's personally identifiable information and photos. The criminal threatened the victim with legal penalties and deportation to China unless fees were paid. The criminal actor communicated via non-video conference calls, spoke Mandarin, and provided the victims with transfer instructions to 28 accounts, totaling approximately \$315,000.
- In June 2022, a criminal actor posing as a Chinese police officer called a Chinese student attending a university in New York and told the victim the PRC customs office was in possession of a package containing 17 credit cards in her name. The criminal actor stated the victim's personal information was used to commit fraud and she would need to pay bail money to avoid being arrested. The criminal actor led the victim to believe an individual associated with the case committed suicide and the family was seeking compensation. In total, the victim paid \$600,000.

An indicator alone does not accurately determine fraud activity; organizations should evaluate the totality of fraud behavior, including message delivery and other relevant circumstances before notifying security/law enforcement personnel. The following suspicious activities/indicators include, but are not limited to any individual, group, or business; observe these indicators in context and not individually:

- Students expressing fear or concern regarding international law enforcement
- Claiming to have received an arrest warrant from international law enforcement (all foreign government officials conducting legitimate law enforcement activity in the United States must act in coordination with U.S. federal authorities)
- Borrowing and wiring large sums of money in a short timeframe to unknown recipients
- Dropping off social media and telling friends verbally or electronically they are suddenly traveling somewhere unexpectedly
- Mentioning participation in calls with unknown individuals claiming to be affiliated with law enforcement







OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)

The FBI’s Office of Private Sector disseminated this LIR; please 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>For the eyes and ears of individual recipients only, no further disclosure.</p>	<p>Sources may use TLP: RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.</p>	<p>Recipients may therefore not share TLP: RED information with anyone else. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.</p>
<p>TLP: AMBER</p>  <p>Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP: AMBER+STRICT restricts sharing to the organization only.</p>	<p>Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP: AMBER+STRICT.</p>
<p>TLP: GREEN</p>  <p>Limited disclosure, recipients can spread this within their community.</p>	<p>Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.</p>
<p>TLP: CLEAR</p>  <p>Recipients can spread this to the world, there is no limit on disclosure.</p>	<p>Sources may use TLP: CLEAR 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: CLEAR information may be shared without restriction.</p>

ENDNOTES REMOVED BY ISAU PRIOR TO DISSEMINATION