Source: <https://www.fbi.gov/contact-us/field-offices/washingtondc/news/fbi-washington-field-office-warns-of-scam-targeting-chinese-communities-in-the-us>

**Image 1**

Embed image:



**Image 2**

The FBI Washington Field Office is warning the public about a scam targeting Chinese communities in the U.S. and students attending U.S. universities. In this scheme, criminals pose as law enforcement officials from China to defraud victims, threatening the victims to build plausibility. They tell victims that they are the subjects of criminal investigations in China and convince them to pay to avoid arrest or deportation.

**Image 3**

"These fraudsters pose as Chinese investigators to intimidate their victims and then prey on their victims' fear to steal their money," said Assistant Director in Charge David Sundberg of the FBI Washington Field Office. "The scam is so convincing because it consists of multiple layers and perpetrators. We hope to educate Chinese communities about this threat to empower victims to file reports."

The scheme consists of four phases

**Image 4**

Phase 1: Initial Contact — U.S. Business or Chinese Embassy or Consulate Impostor

Criminals call their victims to discuss a minor problem such as an outstanding credit card balance, undeliverable package, or unpaid bill. They use technology to disguise or "spoof" their true telephone numbers, calling victims from phone numbers that appear to belong to U.S. businesses or Chinese Embassies or Consulates.

**Image 5**

Phase 2: Scare Tactics — Chinese Police Impostor

The caller transfers the victim to another fraudster who poses as a law enforcement official from China. This impostor tells the victim the details of the alleged crime and provides fraudulent documentation, such as an arrest warrant. At this point, criminals may pressure victims to return to China to face trial or threaten to arrest them.

**Image 6**

Phase 3: Surveillance of Victims

Criminals force victims to consent to 24/7 audio and video monitoring. They tell victims not to discuss the case or conduct Internet searches. Scammers may also try to recruit victims to participate in investigations of other subjects. They may ask victims to take photos or videos of other victims or to receive cryptocurrency or wire transfers.

**Image 7**

Phase 4: Final Act — Extortion of Victims

In the last phase, criminals direct victims to wire money to a Chinese bank account to prove their innocence or to post bail to avoid having to return to China. They may provide scripts for victims to follow when they go to the bank. In some cases, the scammers order victims to lie to friends and family to secure more money. They may also force victims to serve as money mules or facilitate similar criminal schemes against others.

**Image 8**

Protecting Yourself

* If an unknown person contacts you to accuse you of a crime, **do not** share personal or financial information, and **do not** send money. Cease contact with the person.
* Contact from a seemingly official phone number is not proof of official action. Criminals can use technology to mask or "spoof" telephone numbers.
* If a U.S. government agency contacts you, **you can verify** whether the contact is official. Use public sources (phone book, internet, etc.) to identify the government agency’s contact information. Contact the agency to confirm the legitimacy of the interaction.
* **Do not** consent to 24/7 audio or video monitoring.
* If someone claiming to be a Chinese authority contacts you, contact your local FBI office. Foreign government officials conducting legitimate law enforcement activity in the U.S. must act in coordination with U.S. federal authorities.
* Victims should report fraudulent or suspicious activities