STANFORD DEPARTMENT OF PUBLIC SAFETY

COMMUNITY ADVISORY

LAURA L. WILSON, DIRECTOR

THREAT-BASED TELEPHONE SCAMS

HERE ARE SOME COMMON TACTICS SCAMMERS USE:

- Impersonate law enforcement or other government officials over the phone.
- Spoof a law enforcement phone number, creating false information that is displayed on the victim's caller ID.
- Threaten their victims with arrest for outstanding warrants or other legal issues.
- Instruct the victims to "resolve" the matter by paying a fee or "bail."
- Ask for payment in the form of gift cards, pre-paid cards, or wire transfers, often demanding payment while on the phone.

TO AVOID FINANCIAL LOSSES AND IDENTITY THEFT, CONSIDER THESE PREVENTION TIPS:

- If you feel certain about the origin of the call, text, or email, verify the identity of the sender through an independent source, such as an official agency website. DO NOT use the contact details provided by the caller.
- NEVER send money or give your bank account details, credit card, or other personal information to anyone you don't know or can't verify.
- The Stanford Department of Public Safety, or any other law enforcement agency, will never ask for any type of payment over the phone.
- Financial transactions with DPS or other law enforcement agencies are handled in person at the Public Safety Building (233 Bonair Siding) or law enforcement agency.
- A government agency will never ask you to pay by unusual methods, such as with gift cards or wire transfer.
- Don't let the caller convince you to take immediate action; hang up and verify their story.

If you or someone you know has been targeted, please contact the Stanford University Department of Public Safety 650-329-2413
In addition, all types of fraud schemes and scams can always be reported to the FBI's Internet Crime Complaint Center (IC3) at https://www.ic3.gov.

FRAUD SCAM

Stanford University
Department of Public Safety
233 Bonair Siding
Stanford, CA 94305
(650)723-9633
police.stanford.edu

The Stanford University Department of Public Safety (SUDPS) has received reports of email, text, and phone call scams in which the perpetrators are scamming individuals by imitating various Chinese law enforcement agencies. Scammers are primarily targeting Chinese students.

In the most recent scam at Stanford, the student was told by scammers, via email and phone, that they were under investigation in China for money laundering or other crimes. The victim was then told they were required to send money to the law enforcement agency supposedly conducting the investigation. As a result, the student suffered a significant financial loss. To help others in the community, the victim offered these words to describe the financial and emotional impact on her:

"These perpetrators claimed that I was a financial crime suspect and interrogated me with harsh words. They used facetime to monitor me 24/7, threatened to deport me, put me into jail, and defame my family unless I sign the confidentiality contract and pay bail. It was a targeted attack, as they had all my US and Chinese government ID copies and my family information. I fell into the trap, since family and my visa status here are my vulnerabilities. The mind control lasted for two months, as they continued to deliberately ask for more money, using law jargon, during which I lost all my ability to think critically under extreme fear, loneliness, and mental pain. I immediately contacted Stanford police the moment I realized it is a scam."

SUDPS wants the Stanford community to learn about this scam in order to avoid being victimized, if contacted by these scammers. Community members who have been defrauded are also encouraged to report their loss to SUDPS. Reporting this type of fraud as soon as it occurs increases the likelihood of a successful investigation by law enforcement.

If contacted by anyone representing themselves as Chinese law enforcement, you should strive to verify the authenticity of the communication. Contact the law enforcement agency through official channels such as an email address or phone number on the official agency website to confirm the identity of those contacting you. Finally, community members can reduce their chances of being victimized by protecting their personally identifiable information, such as date of birth or passport number.

It is important to be aware that e-mails, text, or phone calls may appear to be from a law enforcement agency, when they are actually from scammers. Email spoofing—the forgery

of an email header so that the message appears to have originated from someone or somewhere other than the actual source—is a common tactic in many scams.

If you or someone you know has been targeted by this Chinese law enforcement impersonation fraud, please report it to SUDPS by calling (650) 329-2413 (24/7).

In addition, all types of fraud schemes and scams can always be reported to the FBI's Internet Crime Complaint Center (IC3) at https://www.ic3.gov.

The following information is helpful to report:

- Identifiers for the perpetrator (name, website, bank account, email addresses);
- Details on how, why, and when you believe you were defrauded;
- Actual and attempted loss amounts;
- Heading information from email messages (from, to, and subject fields);
- Other relevant information you believe is necessary to support your complaint; and
- Reference to this specific Chinese law enforcement impersonation scam (if applicable).

Filing a complaint through the IC3 website allows FBI analysts to identify leads and patterns from the high volume of complaints received daily for referral to the appropriate law enforcement agency for response.