



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

CONNECT to PROTECT

HEALTHCARE & PUBLIC HEALTH SECTOR

18 February 2021

LIR 220218002

Criminals Extorting Medical Professionals by Impersonating Medical Licensing Boards and the FBI

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 New York Office, in coordination with the Office of Private Sector (OPS), prepared this LIR to inform the healthcare and public health sector about a scheme where criminal actors call licensed medical professionals and imply the professional's license has been connected to a criminal investigation. During the calls, the criminal actors impersonate members of the appropriate licensing board, and/or FBI Special Agents. The criminal actors then indicate the professional is a subject of a drug trafficking or money laundering investigation and request the professional pay a "bond" in the tens of thousands of dollars related to the investigation. The money is then remitted overseas to Thailand, Poland, or Singapore.

- In January 2021, fraudsters contacted a New York based dentist and intimated her dental license was going to be suspended, related to ongoing criminal investigations. The fraudsters provided official-looking licensing board, Department of Justice, and FBI documentation to validate their claims. The fraudsters instructed the dentist to send funds to an escrow account while the investigation was ongoing. Over the next few months, the dentist sent bank wires totaling approximately \$500,000 to Poland, Thailand, and Singapore.
- In August 2021, fraudsters contacted a Texas-based nurse from a phone number that appeared to be the Texas Board of Nursing (TXBON). An individual identifying himself as a special investigator for TXBON stated the FBI was investigating a case involving the nurse's license. The fraudster stated her license had been suspended because it was tied to a large drug interdiction as well as money laundering activity, and the FBI listed her as the primary suspect. The fraudsters provided the nurse extensive information related to the fabricated investigation and requested a "security bond" of \$18,600, and then \$23,000, both of which were sent to Thailand.
- In September 2021, a Texas-based doctor's office received a call from a number purported to be the Texas Medical Board out of Austin, Texas. The impersonator on the line identified himself as being from the Investigations Department and stated he needed to speak to a specific doctor. He told the doctor, due to findings in a DEA drug trafficking investigation and unless the doctor paid a "refundable government security bond," the doctor's license was going to be suspended. The impersonator faxed the doctor documents purporting to be evidence of the investigation and requested the doctor send \$22,400 to a bank account located in Thailand.



Licensed medical professionals should remain vigilant of this scam; the following indicators and mitigation steps should be considered to avoid becoming victims:





- Be aware the FBI will never solicit payment, a “refundable government security bond,” or any money from a victim or alleged subject during an investigation.
- Take caution with all requests for payments related to alleged criminal investigations from any purported law enforcement officers, especially law enforcement officers allegedly based in the United States who request money to be sent overseas.
- Do not provide personal identifying information, such as social security number, date of birth, financial information, or professional information (medical license numbers, NPI number, or DEA license numbers, etc.) in response to suspicious calls, emails, or text messages.
- Independently verify personnel purporting to be from medical boards or law enforcement agencies. Use official means like finding contact information on official websites or physical office locations and calling and/or visiting the locations in person to confirm the alleged personnel are employed there.
- Discuss this fraud scheme with colleagues to help prevent other healthcare practitioners from becoming victims.

If you believe your organization or members have been a victim similar schemes, report it to your local FBI Field Office and the FBI’s Internet Crimes Complaint Center (IC3) at www.ic3.gov.

OPS’s Information Sharing and Analysis Unit 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?
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.