OFFICE of PRIVATE SECTOR
LIAISON INFORMATION REPORT (LIR)

HEALTHCARE & PUBLIC HEALTH SECTOR

21 January 2021 LIR 210121002

Scammers Posing as Medical Board Members and Law Enforcement Agents to Target Medical Providers for Wire Fraud Scheme

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's Boston Division, in coordination with the FBI's Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform the private sector of a financial fraud scheme targeting medical professionals for financial gain. Scammers are contacting medical professionals and claiming to be agents of the professional's medical board, agents of the DEA, and agents of the FBI. These scammers claim that the professionals' medical and drug licenses have been compromised and are being used by other entities in a scheme to traffic drugs.

As a result of these allegations, the scammers direct the medical professionals to wire money to foreign bank accounts, in some cases informing them the money will be returned within three days. The scammers then claim other entities are linking fictitious accounts to the medical professionals' personal, business, and investment accounts, and instruct the professionals to wire funds to additional foreign bank accounts to prevent their money from being stolen. The scammers make excuses for why funds are not being returned. In one case, a nurse practitioner was instructed to comply and pay a fee of over $5,000. In another case, dental professionals were instructed to wire a large sum of money to a foreign bank account as a refundable federal bond to "move the investigation forward."

The scammers primarily communicate via text message and phone calls, including a spoofed contact number for the Massachusetts Board of Registration in Dentistry (BORID), (617) 973-0971. They claim to be agents of medical boards, the DEA, and the FBI, and provide victims with fictitious names and badge numbers. Initially, the scammers often contact the medical professionals at their place of business. The victims receive faxed documents containing information allegedly detailing aspects of the investigation, including FBI and DEA case updates, evidence of the fictitious bank accounts, notice of license suspension, and receipts for the wire transfers. These documents include official-looking letterhead, seals, stamps, and water marks from the FBI, DEA, DOJ, and BORID. The documents include publicly available information such as the victims' National Provider Identifier numbers, license numbers, and business addresses. In some cases, victims were also contacted through email.

The following mitigation steps are considered best practices; if you believe one of these scammers has contacted you or if you believe you are the victim of a similar fraud scheme.

- Determine the accuracy of phone numbers given and contacted with by checking them against phone numbers identified on FBI, DOJ, DEA, and medical board websites. Be aware that scammers have the ability to spoof phone numbers to appear as though they legitimately belong to the entity they are claiming to be.

Limited Disclosure, Restricted to the Community
TLP:GREEN

- Confirm the identities of the individuals who contacted you by calling into your local FBI field office or medical board.
- Do not share any personally identifiable information, such as date of birth, social security number, financial information, or professional/licensing information until you confirm the identities of the individuals who contacted you.

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

- Receiving similar texts, or faxed documents(particularly those including spelling and grammar mistakes) claiming involvement in drug trafficking schemes, especially if they come from a foreign telephone or facsimile numbers.
- Requests from medical board representatives or a law enforcement agency asking for money transfers, especially to foreign bank accounts
- Telephone solicitations requesting money are likely fraudulent schemes. The FBI, DEA, and DOJ will never call and solicit money to resolve allegations of drug trafficking.

If you believe you have been contacted by one of these scammers, or believe you have been the victim of this fraud scheme, please inform your security office, contact your appropriate medical board, and report details to the Internet Crimes Complaints Center (IC3) at IC3.gov or your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices. Additionally, contact your bank, report the fraud, and request payments be halted.

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.

OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

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.