



## OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

### HEALTHCARE & PUBLIC HEALTH SECTOR

1 June 2022

LIR 220601003

## Criminal Actors Extorting Medical Professionals by Impersonating Drug Enforcement Administration (DEA) Agents

*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 Atlanta Field Office, in coordination with the Office of Private Sector, prepared this Liaison Information Report (LIR) to inform medical professionals and healthcare sector members in the Atlanta Area of Responsibility regarding a scheme where criminal actors called licensed medical professionals and suggests their professional licenses have been connected to ongoing criminal investigations. In the telephone calls, the fraudsters impersonate state licensing board representatives, FBI Special Agents, or DEA Special Agents. The criminal actors indicate the medical professional is a subject of a money laundering investigation and request the physician liquidate their accounts and pay thousands of dollars related to the investigations. The money is then disbursed to Coinbase or overseas accounts in Peru or Poland.

- In March 2022, a surgeon in Atlanta was contacted by criminal actors, who informed her that she would be arrested, her assets seized, and her medical license suspended as part of an ongoing criminal money laundering investigation. The fraudsters provided what appeared to be official looking Department of Justice, FBI, Department of Treasury, and medical licensing board letterhead documents to prove their claims. The fraudsters instructed the surgeon to wire funds to various secure international accounts controlled by the FBI while the investigation was ongoing. Over the course of one month, the surgeon wired approximately \$472,000 to accounts in Peru, Poland and Coinbase Inc. The surgeon received a receipt by fax or text after each transaction, appearing to be from the Drug Enforcement Administration. The impersonators informed the surgeon she may still be subject to asset forfeiture and that in order to prevent this from occurring she would need to increase her debt by taking out a \$30,000 bank loan. The surgeon took out a loan as instructed and provided the debit card and account information to the purported agents.
- In April 2022, fraudsters contacted an Atlanta-based physician purporting to be DEA Special Agents conducting a drug trafficking investigation. An individual identifying himself as a federal agent stated the DEA had intercepted a large quantity of illegally obtained prescription drugs with the physician's name on the packages. The callers also stated there was a warrant for the physician's arrest as she was associated with money laundering and drug trafficking. The callers informed the physician she would lose her medical license due to her involvement in the alleged criminal activity. The fraudsters instructed the physician to liquidate her bank account as her social security number was compromised, the agents provided an address to send the funds for safekeeping until she could obtain a new social security number. The victim mailed \$12,600 in cash via United States Postal Service (USPS) to a Costa Mesa, California address.



## OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

- In May 2022, an Atlanta-based physician purportedly received a call from the Georgia Composite Medical Board (GCMB) Special Agent. The fraudsters informed her an abandoned vehicle was located in Texas with cocaine and fentanyl prescribed by the physician. The fraudster stated the FBI and DEA contacted the GCMB requesting her medical license be suspended effective immediately as the physician was under investigation. The agents stated she would also be charged with money laundering as numerous accounts were opened with large sums of money totaling \$250,000. The fraudsters instructed the physician to travel to a local UPS store to receive a fax, where she received what appeared to be official documents. A purported FBI Special Agent contacted the physician stating her passport was flagged and she would be unable to leave the state or country until the matter was resolved. The fraudsters faxed additional documents on letterhead in reference to federal bond fees and instructed the victim to wire \$7,200 to a bank account in Peru. The agents indicated scammers compromised the physician's accounts and again instructed her to liquidate all her bank and 401K accounts to be transferred to the US government for safe custody until the funds could be returned.

Medical professionals should remain aware of this scam and conduct due diligence if contacted by purported federal agents. The following indicators and mitigation steps should be considered to avoid becoming victims:





- Be aware the DEA, FBI, or other federal law enforcement agencies will never solicit payment from a victim or alleged subject during an investigation.
- Use caution with any requests for payments related to an alleged criminal investigation from any law enforcement official, specifically law enforcement officers who indicate they are based in the United States and request money to be sent to overseas locations for safekeeping.
- Do not provide personal identifiable information (PII) such as date of birth, social security number, financial information, or professional certification/licensure numbers to suspicious calls, emails, text messages, or social media messages.
- Conduct verification of personnel claiming to be from state medical boards or law enforcement agencies.

Should you be contacted by a suspected scammer related to this scheme, please report it to your local FBI Field Office and the FBI Internet Crimes Complaint Center (IC3) at [www.ic3.gov](http://www.ic3.gov).

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. 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): <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><b>TLP:RED</b></p>  <p>Not for disclosure, restricted to participants only.</p>	<p>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.</p>	<p>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.</p>
<p><b>TLP:AMBER</b></p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>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.</p>	<p>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. <b>Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</b></p>
<p><b>TLP:GREEN</b></p>  <p>Limited disclosure, restricted to the community.</p>	<p>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.</p>	<p>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.</p>
<p><b>TLP:WHITE</b></p>  <p>Disclosure is not limited.</p>	<p>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.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>