



# OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



## CROSS-SECTOR

13 October 2020

LIR 201013-007

### **Criminals Posing as Law Enforcement and Medical Boards as Part of Mass Marketing Fraud Schemes to Target Medical Providers for Financial Gain**

*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 Detroit Field Office, in coordination with the Office of Private Sector (OPS), prepared this LIR to inform members of the health care industry and the financial sector on mass marketing fraud schemes targeting medical providers for financial gain. Recent reporting from multiple sources indicates criminals impersonated law enforcement agencies and medical boards and advised the victims they were under investigation, often for illegal drug activities. Examples of these schemes included, but were not limited to, the following:

- A Michigan medical provider was contacted via a virtual phone number by an unknown individual who stated the medical provider's medical license was suspended. The medical provider also received documents claiming to be from the state's Board of Medicine and the US Department of Justice instructing the medical provider to wire USD 13,000 to avoid legal action.
- A Michigan medical professional returned a fraudulent phone call that claimed to be from the state's Board of Medicine to her place of employment. The caller then claimed to be with the state's Licensing and Regulatory Affairs investigative unit and had the medical professional's state professional license number and National Provider Identifier (NPI) number. The caller further claimed the Federal Bureau of Investigation (FBI) wanted to suspend her professional license immediately based on illegal drug trafficking and money laundering. The caller contacted the medical professional multiple times and asked for the medical professional's bank account balances. Additionally, the caller discouraged the medical professional from disclosing information about the calls to a third party and from using the internet for further research.
- A Michigan medical provider received fraudulent documents claiming to be from the state's Board of Medicine and the FBI. The documents contained the medical provider's medical license number and NPI number and claimed both had been suspended by the state's Board of Medicine because of the medical provider's alleged involvement in an illegal drug trafficking investigation. The documents required a refundable bond approximately USD 50,000 to ensure cooperation with the authorities and the medical provider would not leave the area. Additionally, the documents threatened the medical provider with suspending their medical practice and prohibited the provider from disclosing the investigation to a third party.
- A Michigan pharmacist received a fraudulent phone call that claimed to be from the state's Board of Pharmacy. The callers had the pharmacist's pharmacy license number and claimed the pharmacist was under investigation for illegally distributing opioids.



# OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



- The Drug Enforcement Administration (DEA) released a national press release on scammers spoofing DEA telephone numbers and posing as DEA employees to threaten DEA-registered practitioners for alleged violations of federal drug laws or involvement in drug-trafficking unless victims pay the scammers. Scammers may reference NPI numbers or state license numbers.

In the referenced schemes, the criminals knew the medical providers' information such as name, phone number, medical license number, pharmacy license number, state license number, or NPI number. The criminals used multiple methods to contact victims, including via mail, telephone, and virtual telephone number. Additionally, the criminals used false identities with the victims during the scams and for re-contact purposes.

The FBI has identified the following best practices for health care professionals to identify related suspicious activities and similar scams. These suspicious activities include, but are not limited to any individual, group, or activity and should be observed in context and not individually.





- Be wary of requests from alleged law enforcement agencies or regulatory entities requesting money or other forms of payment regarding criminal investigations.
- Verify the authenticity of communication from alleged medical board officials or alleged law enforcement through known means such as official websites for phone numbers or physical office locations. In addition, independently contact the respective entity/agency to confirm the identity of those contacting you.
- Do not provide personal identifying information, such as social security number or date of birth, financial information, or professional information, such as medical license numbers, NPI number, or DEA license numbers in response to suspicious emails, letters or phone calls.

If you believe your organization was the victim of a similar mass marketing fraud or scam, contact your local FBI Field Office and report details regarding this incident to the Internet Crimes Complaints Center at 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?
<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>