OFFICE of PRIVATE SECTOR
Liaison Information Report (LIR)

HEALTHCARE & PUBLIC HEALTH SECTOR

25 SEPTEMBER 2025 LIR 250925014

Fraudsters Impersonating Federal Law Enforcement Are Targeting Medical Practitioners in Gold Courier Schemes

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 St. Louis Field Office, in coordination with the Criminal Investigative Division, and the Office of Private Sector, prepared this Liaison Information Report (LIR) to alert private sector companies within the healthcare and public health sector about criminal actors ("fraudsters") targeting the assets of medical practitioners[a], ("complainants"), particularly physicians, using a gold courier fraud scheme.[b] The FBI is reporting a rise in schemes involving fraudsters impersonating federal law enforcement agents[c] who contact physicians at their practices, falsely claiming the physician is under investigation for drug trafficking and money laundering. The fraudsters claim the physician's information has been compromised and was used for criminal activity resulting in a federal investigation of their medical license for health care fraud. In some cases, the fraudsters escalate the scam by threatening physicians that refusal to cooperate will result in suspension of their National Provider Identifier (NPI) number.

On 25 July 2025, the DEA issued a public scam alert warning the medical community about fraudsters posing as DEA agents to obtain medical records, personal information, and payments. To supplement the DEA warning, FBI St. Louis is warning that fraudsters may target medical practices by claiming a physician's personal financial accounts are at risk. To secure their assets, the fraudsters instruct physicians to convert their savings into cryptocurrency, cash, or precious metals, such as gold, and provide the assets to a courier purporting to work for the federal government.

- In August 2025, a fraudster impersonating a DEA agent called a St. Louis, Missouri-based physician. The fraudster alleged the DEA was investigating the physician due to their personal information being stolen and exploited for drug trafficking and money laundering by transnational criminal enterprises in Texas. The fraudster provided the physician's

[a] Medical practitioner: A licensed professional qualified to diagnose and treat medical conditions. This term typically includes physicians, surgeons, and other healthcare professionals qualified to provide medical care.
[b] A gold courier scheme is a fraud scheme in which criminals impersonate law enforcement and deceive their targets into believing they are connected to criminal activity and, until their name is cleared, they must provide their assets to the government to protect them. Targets are instructed to convert their assets into gold bars or other precious metals, then arrange for an in-person handoff to a courier pretending to work for the government, resulting in the theft of the assets.
[c] *Analyst Note:* Fraudsters have impersonated officials from the following agencies: the Drug Enforcement Administration (DEA), the Department of Homeland Security (DHS), and the FBI.

actual medical license number and NPI, then requested a copy of the physician's driver's license, claiming it was needed to "secure their information."

- In July 2025, the FBI's Internet Crime Complaint Center (IC3) received nearly 40 complaints from physicians' offices across the US after they were contacted by fraudsters impersonating federal law enforcement agents. The techniques used in successful attempts suggest these calls were crafted to initiate gold courier schemes

  Regardless of outcome, IC3 complaints consistently revealed five recurring elements:

  - Complainant is a physician or other medical practitioner, age 50 years or older;
  - Complainant was contacted by phone at their place of employment;
  - Fraudsters provided the complainant's medical license number and NPI;[d]
  - Fraudsters impersonated federal law enforcement officials, claiming the physician's medical license, NPI, or DEA number was under investigation; and
  - Fraudsters linked the physician to alleged criminal activity occurring near the US-Mexico border in Texas.

- In April 2025, another St. Louis, Missouri physician was contacted via phone by a fraudster claiming to be a DEA agent. The fraudster told the physician they were under DEA investigation after their identity was reportedly exploited by transnational criminal networks for drug trafficking and money laundering operations in Texas. The physician was instructed to liquidate over $500,000 in personal funds, purchase gold with the funds, and hand it over to another fraudster posing as a government courier.

- In March 2025, a physician in California was contacted by a fraudster using the same impersonation and criminal tactics observed in the St. Louis, Missouri incidents reported in April and August 2025. As a result of the scam, the complainant was coerced into converting millions of their funds into gold, which was picked up by couriers involved in the scam.

The following suspicious activities are potential indicators of activity related to a gold courier scam. A single indicator does not accurately identify whether an organization is a target or complainant of fraudulent activity. Healthcare and public health organizations should consider the totality of facts and circumstances when reporting to security or law enforcement personnel.

- Cold call from an individual claiming to be with a federal law enforcement agency such as DEA, FBI, DHS, often with a foreign accent;

[d] *Analyst Note:* Providing LE or complainant-specific information is an alleged attempt to bolster their impersonation of federal law enforcement.

- Caller provides their name and title as "Officer"[e];
- Caller uses urgent, aggressive language to pressure the recipient, often discouraging contact with law enforcement or others;
- Caller alleges the physician is under investigation by a federal law enforcement agency or state medical board;
- Caller alleges the physician has an active arrest warrant due to health care fraud, drug trafficking, money laundering, or physician-prescribed narcotics found in cars at the US-Mexico border in Texas[f];
- Caller attempts to validate the scam by providing the physician with their medical license number or NPI[g];
- Caller requests bank account information, online login and password information, social security numbers, or other personally identifiable information; and
- Caller places a financial demand on the physician to resolve the investigation, secure the physician's medical license, NPI or personal funds. Financial demands of the physician may include converting personal funds into cryptocurrency, cash, gold, or other precious metals, that will be picked up by a government courier.[h]

Medical professionals within the healthcare and public health sector are encouraged to take the following actions to mitigate potential gold courier scams by law enforcement impersonators:

- Train front desk staff to recognize signs of scam exposure, such as unsolicited calls from individuals claiming to be federal law enforcement agents, and requests involving financial transactions, asset liquidation, or courier pickups;
- Conduct regular staff training on scam tactics targeting healthcare and public health professionals; share examples of recent fraud attempts and how they were identified or avoided;
- Spread education and awareness regarding the scam to clinic and administrative staff;
- Include scam awareness in patient and staff newsletters or email updates;
- Establish internal communication protocols to handle suspicious calls or requests, including designating a point person, creating a reporting chain for staff to escalate concerns quickly and discretely;
- Establish a log of unusual or suspicious communications for reference and investigation, documenting any identifying information for callers or alleged couriers including names, phone numbers, email addresses, appearance, license plates, and vehicle make/model;

[e] *Analyst Note:* A DEA, FBI, or DHS agent is *not* called "Officer," they are exclusively referred to as "Special Agent" or "Agent".
[f] *Analyst Note:* In general, federal law enforcement agents will not provide specifics of open investigations to members of the public. In the extremely rare event they do share information, it will not be provided over the phone.
[g] A physician's medical license number or NPI is public record and easily obtainable through open-source resources.
[h] *Analyst Note:* Federal law enforcement agents will never request money from members of the public.

- If a caller claims to be from a government agency, hang up and call the agency directly using a publicly listed number; and
- If you believe you are being targeted through a law enforcement impersonation scam, consider challenging the caller with the following requests:
    - Insist on meeting at an official office of the law enforcement agency;
    - Insist on talking to the law enforcement official in person; and
    - Request to involve an attorney on your behalf for representation. [i]

If you have been targeted for a gold (or similar asset) courier scheme and provided a courier with personal savings in the form of cryptocurrency, or are awaiting the courier's pickup of gold or cash, immediately contact local law enforcement, then report it to IC3 at https://www.ic3.gov.

The FBI's Office of Private Sector 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.

[i] *Analyst Note:* Legitimate federal law enforcement officers will accommodate these requests, while a fraudster will not.

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP: RED For the eyes and ears of individual recipients only, no further disclosure.	Sources may use TLP: RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.	Recipients may therefore not share TLP: RED information with anyone else. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.
TLP: AMBER Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP: AMBER+STRICT restricts sharing to the organization only.	Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP: AMBER+STRICT.
TLP: GREEN Limited disclosure, recipients can spread this within their community.	Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.
TLP: CLEAR Recipients can spread this to the world, there is no limit on disclosure.	Sources may use TLP: CLEAR 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: CLEAR information may be shared without restriction.