OFFICE of PRIVATE SECTOR
LIAISON INFORMATION REPORT (LIR)

HEALTHCARE & PUBLIC HEALTH SECTOR

07/29/2022 **LIR 220729008**

Criminal Actors Impersonate Supply Chain Employees to Fraudulently Obtain Pharmacy Credentials and Medications to Commit Health Care Fraud

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 Criminal Investigative Division, FBI Little Rock, FBI Springfield, and FBI Dallas, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform private sector partners in the healthcare and public health sector about several reported incidents of criminal actors willfully impersonating government and pharmacy personnel to fraudulently obtain pharmacy licensing information and divert orders for medications and supplies. Criminal actors impersonated a "federal agent" from DEA's Controlled Substance Ordering System (CSOS) and representatives from pharmaceutical wholesalers and suppliers when communicating with pharmacies, and as pharmacy employees when communicating with the suppliers. Potential losses from the reported incidents exceed $21 million with actual losses of more than $10.3 million.

- Between December 2020 and May 2022, criminal actors impersonated employees of six pharmacies in Illinois, Arkansas and Colorado to order medications and supplies from three identified wholesale suppliers. Following the order, the criminal actors contacted the pharmacies posing as supplier employees and advised the orders had shipped in error and a courier would be sent to retrieve and return the medications and supplies. Potential losses exceeded $3.6 million with an actual loss to the pharmacies of over $2 million.

- In June 2021, a criminal actor impersonated a "federal agent" with CSOS during a contact with a Vermont pharmacy and requested proprietary customer and vendor information, including DEA licensing information. Believing the request to be legitimate, the pharmacy provided the requested information.
- Between October 2021 and December 2021, criminal actors impersonating pharmaceutical suppliers contacted pharmacies by fax seeking to "recall" medications. In one instance, couriers picked up medications produced by an identified pharmaceutical company from pharmacy warehouses in Wisconsin and Arizona, causing a loss of $2.5 million. In another instance, they claimed medications already on the shelf of a North Carolina pharmacy contained erroneous National Drug Code (NDC) information, but were unsuccessful in obtaining the medications.

- In April 2022, after obtaining access to the online ordering account for pharmacies in Louisiana and Texas, criminal actors fraudulently ordered more than $15.4 million in medications in a five day period. They then coordinated the theft of the medications using couriers for the "pickup and return" of the orders.

Pharmacies are encouraged to be aware of and document suspicious interactions with contacts exhibiting any of the following indicators (these indicators should be observed in context and not individually).

- Individuals contacting the pharmacy about erroneous shipments from suppliers/distributors.
- Individuals seeking information about supplier account information or proprietary vendor and customer information.
- Fax, email or other contact notifying the pharmacy of recalls to medication by the supplier/distributor.
- Individuals placing orders just under the pharmacy's allowable monetary cap with the supplier/ distributor.

Law enforcement and industry experts have identified the following strategies for businesses to consider in order to mitigate financial losses due to theft and diversion of medications and supplies:

- Do not provide supplier or vendor account information over the phone.
- Do not provide business or federal licensing information over the phone.
- Maintain a list of verified contacts at suppliers, distributors who can independently verify an erroneous shipment or request for recall.
- Maintain contact information for your local/regional DEA office to verify telephonic solicitations for licensing information purportedly from that agency.
- Pharmacies should contact their suppliers/distributors and find out what their processes are for recalls and erroneous shipments.
- Pharmacies should request courier's business credentials, as well as a state issued identification card, and maintain a copy in their files.
- Be aware of and scrutinize shipping or courier services that are unknown to your pharmacy.
- Install and maintain good quality security cameras for effective video surveillance to assist law enforcement in the event of criminal activity.

The OPS Information Sharing and Analysis Unit disseminated this LIR. 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.