OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)

FINANCIAL SERVICES SECTOR

18 APRIL 2024 **LIR 240418008**

Criminal Actors Impersonate Heavy Equipment Vendors on Websites and Social Media Marketplaces

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 Mobile Field Office, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform private sector partners in the financial services sector about criminal actors posing as heavy equipment vendors on websites and social media marketplaces. Criminal actors leverage the inherent anonymity of the internet to create fictitious profile accounts or fictitious websites to post advertisements for heavy equipment such as utility tractors, construction vehicles, and shipping containers. Unsuspecting customers who attempt to purchase these items are instructed to either wire money or pay using online payment applications. Once the money is received, customers never receive the purchased goods and are defrauded of their money. Repeated incidents are occurring primarily on fraudulent websites and online marketplaces.

- Beginning in November 2023, a criminal actor created multiple fictitious personas and posted multiple advertisements for utility tractors via a social media marketplace in major cities across the United States. Customers interested in purchasing the equipment were instructed to wire money to a specific account. Once payment was received, communication ended and the customers never received their equipment. The criminal actor also attempted to falsely list wheel loaders and excavators.

- As of January 2024, the same criminal actor traveled throughout the United States to find established and verifiable used equipment and vehicle dealers without websites. The criminal actor then created fictitious websites using those company names without the companies' permission or knowledge to advertise vehicle sales. When customer orders were received, the criminal actor collected the proceeds and then moved to a new geographic location to repeat the process.

- Beginning in April 2023, an identified US business owner reported a criminal actor was using their company name to advertise and sell shipping containers via social media and online marketplaces. The criminal actor sold the containers for approximately $4,000 each. Unsuspecting customers interested in purchasing containers were sent links to online payment applications. Once payment was received, communication ended and the customers never received their containers.

Indicators

While an indicator alone does not accurately determine if online vendor impersonation is actively occurring, financial services sector partners should evaluate the totality of suspicious behavior including message delivery and other relevant circumstances before notifying security/law enforcement personnel. The following suspicious activities/indicators include, but are not limited to, any individual, group, or business (observe these indicators in context).

- Lack of clear instruction on equipment transportation;
- Significantly lower prices for equipment than competitor pricing;
- Online marketplace listings created by accounts with little to no identifiable information;
- Sellers who aggressively respond to questions about their equipment or vehicles or are evasive regarding methods of payment;
- Poor grammar and sentence structure or spelling errors in common words; and
- Improper use of a right holder's company name or trademark.

Mitigation

The following strategies may assist private sector partners in mitigating the online vendor impersonation threat:

- When possible, physically inspect the equipment before the sale or request a virtual walkthrough.
- Ensure the vehicle identification number (VIN) and serial number of equipment matches any documentation.
- Inquire about the history and use of the equipment and/or request a vehicle inspection report.
- Determine if the equipment you are purchasing is considered non-titled equipment.[a] If so, request Proof of Original Purchase or Affidavit Attesting Ownership documents for all equipment purchases.
- Research the seller through reputable sources such as the Better Business Bureau or other professional organizations that post alerts of potential fraud activity.
- Educate yourself on existing fraudulent equipment, intellectual property infringement or payment scams and activity.

[a] Heavy equipment such as excavators, bulldozers, skid steer loaders, and tractors are considered non-titled equipment in most states.

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

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.