



TRANSPORTATION SYSTEMS SECTOR POSTAL AND SHIPPING

09 June 2021

LIR 210609006

Mailed Extortion Threats Targeting Technology and Pharmaceutical Companies

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 Washington Field Office, in coordination with the FBI Office of Private Sector (OPS) and the United States Postal Inspection Service, developed this LIR to inform private sector partners about recent mailed extortion threats targeting companies in emerging technology and the pharmaceutical industry. In April 2021, the FBI became aware of a number of extortion threat letters, which were sent primarily to senior-level executives of publicly traded technology and pharmaceutical companies. The letters provide the recipient with the options to (1) purchase their freedom at the cost of one million dollars in stablecoin,^a (2) earn their freedom by providing company stock information, or (3) death.

All identified letters share the same language. The letters were addressed to the executives by name with their business address. The instructions provided in the letters demand that action be taken by a certain date within a specific timeframe. Common characteristics of these letters include:

- Threatening death if communication or payment is not received by a specific date
- Demanding payment via the USDC stablecoin
- Reference to and a request for information on stock movement related to company news
- Instructions for the recipient to communicate on media websites with encrypted posts only decipherable by the sender of the extortion letter

The FBI requests that private sector partners follow the below Handling Instructions, should they receive a similar extortion attempt or threatening letter:





1. Notify local and federal law enforcement
2. Be sure to use gloves when handling
3. Minimize the number of individuals handling the letter and envelope
4. Store the letter and envelope in separate **paper** bags or **paper** envelopes
5. Keep a record of who has touched the letter within the office

^a In the October 2020 [Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework](#), stablecoins are described as a type of cryptocurrency designed to have a stable value as compared with other types of cryptocurrency, which frequently experience significant volatility. To maintain a stable market value, stablecoins may be pegged to fiat money (like the U.S. dollar), an exchange-traded commodity, or other cryptocurrencies.



The OPS Information Sharing and Analysis Unit disseminated this LIR. Direct any requests and questions to the 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>TLP:RED</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>TLP:AMBER</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. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</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>TLP:WHITE</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>