

**COMMERCIAL FACILITIES SECTOR**

23 MAY 2023

LIR 230523008

**Financial Fraud Scheme Targeting Authors by Impersonating Film  
Production Studios**

*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 Los Angeles Field Office, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform private sector partners in the Commercial Facilities Sector, specifically Production Studios and Publishers, about recent financial fraud schemes targeting authors by impersonating film production studios. These schemes involve authors receiving an email from someone claiming to represent a production studio and suggesting they can help the author attain a movie deal. The scammer then requests funds to move the process along and convert the literary work into a screenplay. In some instances, the scammers have impersonated executives with the production companies; in others, the name the scammer uses is not that of an actual studio employee.

An indicator alone does not accurately determine impersonation; organizations should evaluate the totality of apparent fraud or theft-related behavior, including message delivery and other relevant circumstances before notifying security/law enforcement personnel.

The following indicators may point to financial fraud schemes targeting authors by impersonating film production studios. These indicators should be observed in context and not individually.

If an individual contacts your organization or arrives at your facility claiming to have been working with someone within your organization, determining who they believe they have been communicating with and through what email address and phone numbers can help identify if they have been targeted by these scammers. Some possible indicators include:

- The name of the individual they have been communicating with does not correspond to an actual employee or executive within your organization
- The email domain does not correspond with your organization's legitimate domain
- The name of the individual they have been communicating with *does* correspond with an employee or executive, but the phone or email does not match with the employee's contact information
- The author indicates the individual they have been communicating with requested funds
  - Note: The author may or may not have actually provided the funds







**OFFICE of PRIVATE SECTOR**

**Liaison Information Report (LIR)**

If you believe your organization’s name or personnel information has been used to conduct such a scheme, please contact your local FBI Field Office and report details regarding the incident to the Internet Crime Complaint Center (IC<sup>3</sup>) at <https://www.ic3.gov/default.aspx>. If an author contacts your organization and you suspect they have been the target of this scheme, please advise them to also contact their local FBI Field Office and report the details to IC<sup>3</sup>.

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?
<p><b>TLP: RED</b></p>  <p>For the eyes and ears of individual recipients only, no further disclosure.</p>	<p>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.</p>	<p>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.</p>
<p><b>TLP: AMBER</b></p>  <p>Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that <b>TLP: AMBER+STRICT</b> restricts sharing to the organization only.</p>	<p>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.</p>	<p>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 <b>only</b>, they must specify TLP: AMBER+STRICT.</p>
<p><b>TLP: GREEN</b></p>  <p>Limited disclosure, recipients can spread this within their community.</p>	<p>Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.</p>	<p>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.</p>
<p><b>TLP: CLEAR</b></p>  <p>Recipients can spread this to the world, there is no limit on disclosure.</p>	<p>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.</p>	<p>Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.</p>