



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



COMMERCIAL FACILITIES SECTOR

5 June 2020

LIR 200605-007

Uptick in Invoice Schemes Increases Losses from Business Email Compromises (BEC)

The FBI Atlanta Field Office, in coordination with the FBI's Office of Private Sector (OPS), prepared this LIR to alert private sector partners regarding the use of fraudulent invoices to advance BEC schemes. Cyber-criminal actors are using fraudulent invoices to redirect payments and steal money from **companies in various sectors**. The criminal actors exploit publicly available tools and the trust inherent in business relationships.

The FBI is issuing this report due to recent complaints from several companies targeted by BEC actors using fake invoices. The invoices looked legitimate and were likely created with an online PDF editor, targeting different industries, including companies involved in transportation, manufacturing, and online marketplace solutions.

- In April 2020, the FBI was contacted by a transportation company reporting fraud by cyber-criminal actors who intercepted communications between them and one of their third-party vendors. The scammers used the trusted third-party vendor relationship and a fraudulent invoice to target the transportation company in order to steal approximately \$1,500,000.
- In May 2020, several customers of an Atlanta-based company reported receiving fraudulent invoices appearing to come from the company. There were approximately seven customers contacted, all having some form of online payment set up with the company.
- In May 2020, a company received an email with a fraudulent invoice. The email appeared to come from an employee of one of the company's vendors. The victim company received regular invoices from the vendor and compared a legitimate service invoice from April with the fraudulent invoice. The fraudulent invoice appeared nearly identical except there were changes to an email address and phone numbers.
- In April 2020, BEC cyber actors sent six fraudulent invoices to a victim company totaling approximately \$336,000. The BEC cyber actors impersonated a third-party company recently purchased by a manufacturing company.

Online PDF editors can be used to alter a legitimate PDF invoice with realistic results. In some cases, the only altered information may be a spoofed email or phone number with one letter or number change. In two of the instances mentioned above, the BEC cyber actors exploited a smaller, third-party relationship to advance a scheme. The corporate telework environment also creates vulnerabilities for cyber threat activity, including the use of personal devices and networks, communication security challenges, and



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)







difficulty adhering to network security policies and procedures designed to prevent fraud and cyber-criminal activity. These combined vulnerabilities could increase the success rate of cyber-criminal scams.

Company Mitigation Efforts for BEC Schemes

- Immediately report any online fraud or BEC activity to the Internet Crime Complaint Center (IC3) <https://www.ic3.gov/>,
- Frequently monitor your Email Exchange server for changes in configuration and custom rules for specific accounts,
- Consider adding an email banner on emails coming from outside your organization, so they are easily noticed,
- Conduct End User education and training on the BEC threat and how to identify a spear phishing email,
- Ensure company policies provide for verification of any changes to existing invoices, bank deposit information, and contact information,
- Contact requestors by phone before complying with e-mail requests for payments or personnel records,
- Consider requiring two parties sign off on payment transfers,
- Be aware of vulnerabilities related to third-party business partners.

This LIR was disseminated from OPS’s Information Sharing and Analysis Unit. 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): <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>	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.
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</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.	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>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</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.	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>TLP:WHITE</p>  <p>Disclosure is not limited.</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.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.