Office of Inspector General
Legal Services Corporation
3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

# HOTLINE ADVISORY

TO: LSC Grantee Executive Directors, Chief Fiscal Officers, and Board Chairs

THROUGH: Thomas Yatsco
Inspector Gene

FROM: Daniel O'Rourke DOR
Assistant Inspector General for Investigations

DATE: June 13, 2023

SUBJECT: Protecting Your Organization Against Business Email Compromise and Payroll Fraud Schemes

---

In a continuing effort to assist Legal Services Corporation (LSC) grantees and subgrantees in detecting and preventing cyberattacks, the Office of Inspector General (OIG) for LSC is issuing this Hotline Advisory to notify grantees of two recent Business Email Compromise (BEC) frauds perpetrated against LSC grantees. In this advisory, the OIG provides updates on BEC schemes and emerging BEC threats as well as details on how the two recent direct deposit BEC schemes were perpetrated on LSC grantees. We also offer best practices for detecting and preventing BEC schemes, such as the recent BEC payroll schemes and others, and provide grantees with the Federal Bureau of Investigation's (FBI) guidance on reporting BEC schemes. Taking action to protect yourself against these threats will help you mitigate financial, cybersecurity, and reputational risks.

## Statistics Show Rising Threat of BEC Schemes

The FBI's Internet Crime Complaint Center (IC3) reported that losses from BEC scheme complaints increased from $360 million in 2016 to more than $2.7 billion in 2022. According to the FBI, the reason for the large increase in BEC scheme losses was likely due to "ever-evolving tactics" of cybercriminals. Evolving BEC scheme tactics include more sophisticated impersonation using AI such as ChatGPT in an effort to deceive employees.

Since 2018, LSC and its grantees reported 22 BEC schemes to the OIG hotline, with 18 occurring since the start of the COVID-19 pandemic in March 2020. Direct deposit payroll scams (described in detail below) are the most common type of BEC scheme perpetrated against grantees. BEC schemes have also targeted grant remittances, vendor payments, grantee

financial institutions, and gift card requests. The loss amounts resulting from BEC schemes to the LSC community have ranged from $800 to $1.1 million.

**Types of BEC Schemes and Emerging Threats**

BEC schemes aim to exploit vulnerable business processes that involve a financial transaction by compromising email accounts to deceive employees. Most BEC schemes include multiple email communications between the cybercriminal and a business' targeted employee(s). Initial communications aim to trick the employee into disclosing sensitive information. Typically, the ultimate goal of a BEC scheme is to divert funds to a cybercriminal through a financial transaction such as a wire transfer or a gift card purchase.

Common targets of BEC schemes at LSC grantees have been executive directors, fiscal employees, human resources (HR) employees, new employees, and entry level employees. BEC attacks against grantees have targeted payroll direct deposits, grant payments from a funder to the grantee, vendor payments through a false invoice scheme, communications with grantee financial institutions, and gift card requests by cybercriminals impersonating the executive director. In addition, an emerging BEC threat that grantees should be aware of targets clients of law firms. In this scheme, the cybercriminal sends an email to a client, impersonating their attorney, and requests payment.

Based on information from the FBI, the following tactics are used by cybercriminals to deceive employees and compromise email accounts in furtherance of BEC schemes. Each of the strategies detailed below has been used in BEC schemes reported to the OIG and many times the scams reported to the OIG have included multiple elements to deceive employees:

1. **Spoofing a Grantee Email Account:** Cybercriminals have created slight variations to a legitimate business email domain in order to deceive employees or third parties into believing that they are communicating with a legitimate employee. For example, a grantee's legitimate email domain of "legalaid.com" was spoofed by a cybercriminal with a subtle change such as "legal-aid.com." The cybercriminal then used the spoofed email domain to impersonate a grantee employee. (For example, John Smith's spoofed email would appear as jsmith@legal-aid.com instead of jsmith@legalaid.com.) Cybercriminals have used similar tactics to communicate with a grantee's funder, such as LSC, a grantee financial institution, another grantee employee, or with a grantee vendor.

2. **Spear Phishing Emails:** Spear phishing is a type of phishing attack that targets specific people with emails that appear to be from a trusted sender. Spear phishing can trick grantee employees into disclosing sensitive information, such as providing the cybercriminal with the name of the employee in charge of payroll, or with internal processes related to financial transactions such as how to change a bank account number for direct deposit payroll. Several BEC attacks on grantees have been initiated by an email account that appeared to be the personal email account of a grantee employee or the executive director but, in fact, was a cybercriminal.

3. **Social Engineering:** Cybercriminals use deception to manipulate employees into providing sensitive data such as login credentials, internal forms, and bank account information. Many times, cybercriminals will use publicly available information about an organization or its employees to assist in social engineering efforts. Many not-for-profit organizations aim to be transparent to the public and often disclose business data and information. Cybercriminals that have targeted LSC grantees have often known the names and positions of fiscal employees and in some instances the names of a grantee's financial institutions. The FBI has warned that intended targets of BEC schemes are monitored and studied by cybercriminals prior to initiating the scam. Through these social engineering efforts, the cybercriminals "are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment."

4. **Network or Computer Intrusion:** Intrusions occur when cybercriminals gain unauthorized access to a grantee network or an employee computer. Intrusions allow cybercriminals to access grantee data and legitimate accounts such as an employee's email or payroll account. Intrusions can occur through malware links (malicious software) embedded in emails. For example, through a computer intrusion, a cybercriminal was able to gain access to a grantee chief financial officer's (CFO) email. Once inside the CFO's email account, the cyber-criminal enabled the auto-forwarding function so that all emails from LSC's email domain (@lsc.gov) would be automatically forwarded to the CFO's junk folder, where the cybercriminal could view and respond to LSC's emails undetected. The cybercriminal was attempting to divert the grantee's monthly LSC grant payment to the cyber-criminal's account.

**Recent BEC Scheme Incidents Against LSC Grantees**

Incident 1: Diversion of Payroll Direct Deposit through Spear Phishing

A cybercriminal impersonating a grantee employee emailed a grantee HR employee from what appeared to be the employee's personal email (a spear phishing email) requesting a change to their direct deposit bank account for payroll. The HR employee forwarded the cybercriminal's email to a grantee payroll employee. The payroll employee instructed the cybercriminal to independently change the direct deposit information in their online payroll account. The cybercriminal created a sense of urgency stating they had been unable to change the direct deposit information after several attempts and that it was urgent that the account be changed by the next payroll which was occurring in two days.

The payroll employee agreed to change the direct deposit information for the cybercriminal in the grantee online payroll system and requested a voided check from the purported employee (cybercriminal) to confirm the account information. The voided check provided by the cybercriminal appeared to be from the grantee employee. The autogenerated email notification of the direct deposit change was sent to the employee's email account when they were on leave. The employee's payroll was deposited into the cybercriminal's bank account and the incident was not detected until after the employee noticed they had not received a payroll deposit.

Incident 2: Diversion of Payroll Direct Deposit through Computer Intrusion

A cybercriminal was able to access a new employee's online payroll account and change their direct deposit information. It appears the new employee clicked on a malware link embedded in an email sent by the cybercriminal. Through the link, the cybercriminal was able to gain access to the employee's payroll account (computer intrusion) and change the employee's direct deposit bank account to their own.

Most payroll vendors will notify employees when their payroll settings are changed. In this instance, the direct deposit change was not detected because the new employee's payroll account was linked to a non-grantee email account. The employee's payroll was deposited into the cybercriminal's bank account and the incident was not detected until after the employee noticed they had not received a payroll deposit.

**Best Practices for BEC Detection and Prevention**

Implementing the following best practices can help protect your organization from becoming a victim of BEC schemes:

Require Employee Education and Awareness

- Require cyber-threat training and ensure staff, especially fiscal staff, are aware of various types of social engineering techniques. Cybercriminals actively target fiscal and administrative staff.
- Convey the importance of cybersecurity practices throughout the organization. Tone at the top matters.
- Train grantee staff to follow written policies without deviation when dealing with requests related to financial transactions.
- Prohibit the use of personal emails and computers by staff for grantee-related activities.
- Encourage the prompt reporting of suspicious emails and incidents by employees and establish a process for assessing and responding to cyber incidents.
- Routinely remind staff to report cyber incidents to the OIG Hotline.
- Instruct staff to be wary of requests for information for items that should be common knowledge to the person requesting the information.
- Periodically simulate BEC schemes for staff, especially fiscal staff, with follow-up on "lessons learned." Simulated BEC schemes can assist staff with spotting phishing links, spoofed email domains, and other red flags.

Implement Strong Financial Controls

- Enable automated notifications for changes to automatic or recurring payments. Some software, such as payroll, typically have settings that allow for automated notifications for changes such as bank account, contact name, email address, phone number, and physical address.
- When a payment or associated information is requested to be changed, ensure that multiple steps are taken to verify the identity of the person/company requesting the

change. Consider using video such as Microsoft Teams and Zoom to verify the identity of the requestor.
- Require at least two-part authorization (review and approval by more than one employee) for any requests related to changes in payments or money transfers.
- Consider using a system or software specifically designed to authenticate payments rather than sending invoices through email.
- Regularly review and update financial policies to ensure cybersecurity best practices and emerging threats are considered.

Strengthen Email Security

- Employ multi-factor authentication on grantee email accounts and other accounts such as payroll and billing software. A user would be required to present one or more verification factors in addition to their login credentials to gain access to the account or system. This additional measure helps prevent access when credentials are stolen.
- Consider blocking international IP addresses from accessing your systems, especially email systems.
- Implement email authentication protocols such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) to help identify and block spoofed emails.[1]

Implement Firewall Configuration and Software Patches and Updates

- Ensure your network includes a properly configured firewall that only allows traffic needed for grantee operations. A firewall is a network security device that monitors incoming and outgoing traffic and blocks certain traffic based on security rules.
- Ensure that the organization's software and systems are up to date with security patches and updates. Cybercriminals can exploit vulnerabilities in outdated or unpatched software and gain unauthorized access to the grantee's network.
- Regularly review and assess your organization's software inventory to ensure all applications are current and adequately protected.
- Review the devices on the organization's network against the devices inventory to ensure only registered devices are connected to the network.

**Reporting BEC Schemes**

The FBI recommends businesses report BEC schemes and losses to the following entities:

- OIG Hotline: LSC Grant Terms and Conditions require grantees to report cyber incidents to the OIG hotline. We are here to assist you.
- Financial Institution: For any fraudulent transfer of funds, contact your financial institution immediately and request that they contact the financial institution where the transfer was sent.

[1] For more information on SPF, DKIM, and DMARC visit: How DMARC Advances Email Security (cisecurity.org); What are DMARC, SPF and DKIM? How to master email security with these protocols | CSO Online.

- Local FBI Field Office: Report the crime to your local FBI field office.
- Internet Crime Complaint Center: File a complaint with the FBI's IC3.

**Prior OIG Warnings and Advisories Related BEC Schemes Against Grantees**

Financial Institutions

- BEC Schemes Targeting Grantee Financial Institutions (February 18, 2022)

Grant Remittances and Gift Cards

- Recent Ransomware and Phishing Attacks (July 13, 2021)
- Email Scams Targeting LSC and LSC Grantees (January 15, 2021)
- Business Email Compromise Schemes (December 14, 2020)

Payroll and Direct Deposit

- Payroll and Direct Deposit Phishing Schemes (October 18, 2018)

For additional cybersecurity resources, please refer to the OIG's cybersecurity site found here.

If you have any questions or would like additional information about this or any other Hotline Advisory article, please contact Daniel O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at (202) 295-1651, or by email at dorourke@oig.lsc.gov.

If you would like to stay current with our most recent alerts and advisories, please follow the directions on our website homepage (https://www.oig.lsc.gov/) and "Sign Up for Email Updates" to subscribe to the LSC-OIG website.