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

SPECIAL FRAUD ADVISORY

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

FROM: Jeffrey E. Schanz
Inspector General

DATE: December 14, 2020

SUBJECT: LSC Business Email Compromise Fraud Scheme

The Office of Inspector General (OIG) for the Legal Services Corporation (LSC) is informing you of an FBI warning related to a significant increase in Business Email Compromise (BEC) schemes due to the COVID-19 pandemic. Since the pandemic, there have been a number of cyber-threats reported to the OIG Hotline by LSC grantees, including potential threats of BEC schemes.

The OIG believes that the LSC community is at risk of being targeted by BEC schemes. We ask grantees to make their employees aware of the known threat and provide them with the resources included in this advisory.

A BEC scheme is a fraud scheme that aims to trick employees into revealing sensitive information or into making payments based on fraudulent instructions. BEC schemes typically target companies that have the ability to send wire transfers, checks, and automated clearing house (ACH) transfers.

Perpetrators can initiate a BEC scheme by compromising a company's email account (network breach) or by spoofing a company's email account (impersonating a company's legitimate email domain). Due to known spoofing attempts against the LSC community, this advisory will focus on BEC schemes perpetrated through spoofing legitimate email domains.

A company's email account can be spoofed by registering an email domain that looks similar to the actual email domain. For instance, any communications from LSC will always end in .gov and will never end in .com or .org. In addition, an LSC grantee reported a more subtle change to their spoofed email domain, e.g., changing "legalaid" in part of the domain, to "legal-aid."

Once a company's email domain is spoofed, the perpetrators will use social engineering to trick an employee(s) into providing sensitive business information, such as bank

account information and/or making a payment or money transfer to a fraudulent account. Typically, employees that perform legitimate fund transfers as part of their work duties are most often targeted by the spoofed emails. Based on reports to the OIG Hotline, all types of payments and money transfers are being targeted by cyber-threats including payroll, vendor payments, and grant remittances.

Report Cyber-Threat Incidents

The OIG requests that any grantees that believe they may have been targeted by a BEC scheme or other cyber-threat to contact the **OIG Hotline**.

BEC Scheme Online Resources

Listed below are online BEC scheme prevention resources, including from the Federal Bureau of Investigation (FBI). Please provide these resources to your staff, especially LSC grantee fiscal and information technology (IT) staff. Please take the appropriate suggested steps to avoid becoming a victim of a BEC scheme or other types of cyber-crimes.

- **FBI: Business Email Compromise** – Tips for identifying, preventing, and reporting BEC schemes

- **National Law Review** – BEC Scams: What You Should Know and What You Can Do To Be Prepared

- **JP Morgan Chase** – Protecting Against Business Email Compromise (includes a quiz for how to spot BEC tactics)

Additional Items to Prevent BEC Schemes

- Be alert to emails with hyperlinks that may contain misspellings or changes of the actual domain name.
- Beware of URL spoofing, when a fraudulent link including links to email addresses is masked to look like a legitimate and/or familiar source.
- When a payment or money transfer change (including wire, ACH, direct deposit, check, etc.) is requested, ensure that multiple steps are taken to verify the identity of the person/company requesting the change. Please note: LSC will never ask a grantee to update their banking information
- A two-part or multiple part identity verification could be as simple as an email and a phone call (to a previously confirmed email address and phone number) to verify the legitimacy of the requested bank account change. These requests include banking changes, address change related to payments, email changes for payment notifications, changes to person of contact, etc.
- Require at least a two-part authorization (review and approval by more than one employee) for any requests related to changes in payments or money transfers.

- Conduct an online search of bank routing numbers to ensure they match the other identifying information of the bank, including bank location and bank name.
- If a form is submitted as part of a payment change request, review the form for red flags such as smears, misspelled words, uneven spacing, etc.
- Verify payment change requests from one bank to another that appear unusual (for instance, a change to an out-of-state bank or online bank or a change from a national bank to a small community bank).
- Do not assume payroll is the only target; BEC schemes can also target vendor payments and grant remittances. Ensure all payments sent and received by the grantee follow proper prevention protocols.
- Ensure that staff, especially fiscal staff, is aware of the various types of social engineering techniques (the use of deception to manipulate individuals to provide confidential information for fraudulent purposes). Instruct staff to be wary of requests for information for items that should be common knowledge to the person requesting the information.
- **Talk to your insurance provider(s) about cyber-fraud insurance and consider purchasing coverage if you are not already covered. In addition, ensure the amount of coverage would be adequate for any potential losses.**

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

For additional cyber-threat resources issued by the OIG, please visit the OIG website for the following resources Fraud Corners, Fraud Alerts, and COVID-19 Fraud Scams.