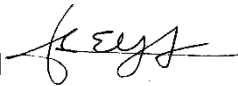




## **FRAUD ADVISORY 25-0192-A-FA**

**TO:** Executive Directors and Board Chairs

**FROM:** Thomas E. Yatsco  
Inspector General 

**DATE:** December 16, 2025

**SUBJECT:** Cyber Threat Notice: Avoiding Donation and Accidental Payment Scams

---

### **Donation and Accidental Payment Scams**

- Our legal assistance community benefits from donations and receipt of other funds to serve clients. However, scams have surfaced that rely on donation reversals or refunds that could result in financial losses to Legal Services Corporation (LSC) grantees.
  - By understanding the ways fraudsters use donation scams or other accidental payment schemes, LSC grantees can help mitigate risks associated with these deceptive practices designed to steal funds from your program.
  - The LSC Office of Inspector General (OIG) urges you and your staff to become familiar with these schemes and to review the suggestions within this advisory.
- 

### **What is a Donation or Accidental Payment Scam?**

It is a common occurrence for nonprofits, including legal assistance programs, to receive donations from various sources in order to support their mission. Donation or accidental payment scams

---

involve illegitimate donors sending fraudulent or counterfeit checks to nonprofits that will never be cleared by their bank.

Through this scheme, the scammer sends a check, which the nonprofit deposits into its bank account. After the check is deposited, the scammer contacts the nonprofit claiming they accidentally overpaid the nonprofit and need a portion of the funds back. The scammer requests the nonprofit to wire the amount of overpaid funds or to send a separate check back to the scammer. After the nonprofit sends the requested refund amount, the original check bounces, since it was fraudulent.

The same scheme can be carried out through credit cards or bank account information. In these accidental payment scams, fraudsters use stolen credit cards or bank account information to send money to users on apps like Zelle, Apple Cash, Venmo or PayPal. Soon after payment is received, the bad actor contacts the recipient of the funds claiming it was a mistake and pressures the recipient to return the funds.

### **Scam Attempted Against an LSC Grantee**

The OIG recently received a hotline complaint from a grantee involving a donation made in the name of a grantee client for \$75,000 via an e-check.<sup>1</sup> The grantee's bank initially showed that the donation check cleared the grantee's bank account and that the funds were available. However, five days after the donation was deposited, the transaction was reversed due to the bank's inability to identify the origin of the alleged donor's bank account. The OIG believes the scammer intended to request a refund from the grantee prior to their bank recognizing the e-check was a bogus payment. If this scam had been successful, it could have resulted in a \$75,000 loss to the grantee.

The above e-check scam is becoming more common. When nonprofits are targeted, a scammer donates using the online e-check and before the check clears, the alleged donor purports to change their mind about the transaction and asks for either a full or a partial refund.

Since e-checks are not refunded in the same way as credit or debit card donations, the legal aid organization might cut a check to the alleged donor and soon after, the alleged donor's e-check

---

<sup>1</sup> An electronic check, or e-check, is a form of payment made via the Internet, or another data network, designed to perform the same function as a conventional paper check and is processed in fewer steps.

bounces. As a result, the nonprofit is left without the donation or the money they sent as a refund to the scammer.

Scammers may also make a bogus donation or payment in the name of a person or business known to the grantee in an attempt to make the grantee believe that a request for reversal or refund of the payment is legitimate.

## **Other Accidental Payment Scams Explained**

Accidental payment scams are a way fraudsters trick people into sending them money. This is how the scheme typically unfolds:

1. **Unexpected Payment:** You receive money from a person through check, credit card, or a digital payment service such as Venmo, Zelle, or PayPal.
2. **Urgent Request:** The sender quickly messages you, claiming they sent the money either by mistake or sent more than they intended, and requests you return all or some of it. If the payment is made by credit card, the fraudulent donor may file a chargeback with the credit card company and a refund request from the organization.
3. **Wired Refund:** The organization sends the requested refund. Since the original check was fraudulent, the original check bounces. The organization is then left with a loss, not only of the funds they returned, but also of any bank fees incurred.
4. **Stolen Funds:** The money sometimes comes from a hacked credit card or bank account. If you send it back, you're actually sending your own money to the scammer.
5. **Reversal:** If the original payment was from a stolen or fraudulent account, once the fraud is detected, the bank reverses the stolen funds. Any money you sent as a refund will become a loss to the program, while the scammer walks away with your refund payment.

## **How to Protect Your Program**

- **Verify the donors are legitimate** before accepting donations, especially from new or unknown donors, verify their identity and the legitimacy of the donation. Contact the donor directly using official channels, not through the contact information provided in suspicious emails or letters.

- **Wait** until any e-checks or payments have completely cleared the bank. It can take several days for the check to be processed by the bank. Your service provider may be able to work directly with the companies who process e-checks to get the money returned to the donor, which may take a few days.
- **Call** your online donation service provider instead of writing the refund requester a check yourself.
- **Report** suspicious transactions to your bank or payment application.
- **Be cautious with payment applications**, as they often do not offer fraud protection the way credit cards do.
- **Educate** your team to ensure they are aware of these scams and the importance of verifying checks and other payment methods for donations.

We also encourage you to report incidents to the OIG hotline ([OIG Hotline | Legal Services Corporation OIG](#)), even if they are thwarted. Doing so will enable us to track trends and understand how these scams might be evolving.

## Questions and Contacts

If you have any questions or would like additional information about this or any other issue, please contact Daniel O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at (202) 441-9948 or by email at [dorourke@oig.lsc.gov](mailto:dorourke@oig.lsc.gov).

## Sign Up for LSC OIG Alerts & Advisories

If you would like to stay current with our most recent OIG fraud alerts and advisories, please follow the directions on our homepage at <https://oig.lsc.gov/>, see "Sign Up for Email Updates" to subscribe to new LSC OIG website postings.