Fraud Prevention
Nonprofit Organizations

How to Prevent Fraud at Nonprofit Organizations

Fraud is devastating to organizations of all sizes, but nonprofits are particularly vulnerable. With fewer resources to prevent and recover from those losses, the results can be catastrophic. As financial transactions and fraud schemes become more complex and sophisticated, recognizing the wide variety of internal and external fraud threats is essential to detecting and deterring fraud at your organization.

Business Email Compromise

Also known as BEC, this scheme typically starts with an email that appears to be from either a known vendor, someone with whom the nonprofit has been corresponding, or the recipient of nonprofit funds. A compromised email will provide details for how to send a payment OR will request that prior remittance details be changed due to some "problem" with the prior account.

There are two types of BEC to watch for: "spoofed" emails that look like a legitimate email with just minor changes and "hacked" emails that utilize the actual email address because the fraudster has taken control of an email account.

Some Ways to Prevent Business Email Compromise:

- Verify, verify, verify
  - Does the email appear to be written appropriately, without typos or slang?
  - Is the number in the email one you have called in the past? Call sender at a known phone number to verify instructions.
  - Does the person you're speaking to know details of your last discussion and understand your current conversation?
  - Do the instructions in the email align with your needs? Does the beneficiary's bank information make sense?
- Establish and follow the following procedures:
  - Dual Control - Only send out wires or create ACH transactions under the authority of two people – one to create and one to verify. Both parties should independently review the details of the transaction and have the authority/ expectation to question anything that seems out of place.
  - Written Authorization for Disbursement - Include supporting documentation with instructions for remittance and how those were received, as well as the details of any callbacks or verifications that were performed.

Don't feel bad about performing these verifications! Fraud is a very real threat, and once an ACH or a wire is sent, recovery is NOT guaranteed. You want your funds to be used to help your target beneficiaries, NOT fraudsters.

HERITAGE
BANK OF COMMERCE
www.HeritageBankofCommerce.bank

Check/ACH Fraud

Although old school, this type of fraud continues to increase. Fraudsters steal mail, either at delivery or at the sending point, because stolen checks can be altered by adding a new payee. This is easy to miss because the check still posts for the correct amount and check number. Stolen checks can be used as a template to create counterfeit checks, and accounts can be "slammed" with a large number of counterfeit checks. These are often for smaller dollar amounts, with fraudsters hoping to fly below dollar thresholds. Bank information and account numbers can be used to create fraudulent ACH (electronic) debits, often through payments to credit cards.

Your best ally in preventing check and ACH fraud is Positive Pay. Issued checks and authorized ACH originators/transactions are input through the online banking system. If a transaction is presented that does not match your "authorized transactions", it is flagged for review. Using online banking, you decide manually whether each item is to be paid or returned, or you can establish a default decision to "Return" or "Pay" rejected items. The default goes into effect if you do not make manual decisions on the items.

Embezzlement

This internal fraud occurs when someone in the organization has too much autonomy, is believed to be "above reproach", and/or has an excessive amount of authority to independently conduct transactions. Newer staff or rotating staff, a common situation for nonprofits, may be less likely to know the standard procedures and, therefore, less likely to recognize when something is unusual or suspicious.

There are two important ways for nonprofits to avoid internal fraud:

1. Establish dual control and separation of duties so transactions are always completed by at least two individuals. For checks, one person issues the checks and a different person signs them. For online transactions, including wires, ACH, and transfers, one person creates the transaction and a second verifies it, with both carefully reviewing the authorizing documentation.

   Someone other than the person involved in issuing checks or creating and approving transactions should be reviewing and balancing the statement. This should be a documented procedure, including explanations for any transactions that might appear unusual. The balanced statement as well as supporting documentation should be presented to the Board or another person in authority who was not involved in executing the transactions. This reporting should be done in a timely fashion, on a regular basis.

2. Create a culture of transparency where no one is considered above verification. From the top down, all staff should encourage oversight and validation. More than one individual should be involved in all decision-making and transaction processing. While this might not be as efficient, it is more effective and well worth the extra time and effort in preventing embezzlement.

For more tips, tools and resources to help protect your nonprofit organization from fraud attacks, please visit **heritagebankofcommerce.bank/fraud-awareness**.

www.HeritageBankofCommerce.bank