

## *10 Ways to Catch Fraud (and Mistakes) from Outside the Nonprofit*

---

Fraud and error can occur both within and without an organization. Your employees and board may be completely trustworthy, but fall prey to a number of scams that are now more frequently targeting nonprofit because of the general trusting nature that is part of nonprofit culture. Here are some tips to help you catch outside fraud (or mistakes) before it affects your bottom line:

1. **Verify all packing slips and receipts.** When orders are delivered, (or at the check-out counter, if purchases are made in-store) double-check packing lists and receipts against orders to be sure that you have received all you were billed for, and haven't been double-billed for an order.
  
2. **Verify all invoices**
  - a. **(part 1 - error)**. Before writing the check, be sure that you haven't already paid a bill. Because of the economy and increased need for immediate cash flow, many vendors are accelerating their payment cycle, and you might get a "reminder invoice" close in time to receipt of the original invoice.
  
  - b. **(part 2 - fraud)**. Make sure you have actually received the product for which you have an invoice. There have been recurrences of an old fraud scheme to bill a customer for a product that was never ordered and never received, on the theory that the accounting department will routinely pay any bill that looks "legitimate."
  
3. **Never place orders with cold-callers.** No matter how great of a "deal" a cold-call sales person might have, NEVER place an order with an unfamiliar vendor that calls you. This, too, is an older scam that has been resurrected as a result of the poor economy.
  
4. **Use Bids for Larger Purchases and Service Contracts.** Get a second (or third) quote or bid for larger purchases, such as HVAC improvements and repairs, computer and network purchases and installation work, and office improvements. Check references for new contractors, such as outsourced payroll and benefits services, building repair and services, HVAC contractors and custodial services.
  
5. **Watch Outsourced Services.** Monitor third-party payroll and accounting services to be sure that the work is accurate and timely, including required government reports. If you use a third-party fund-raising service, be especially vigilant of over-reporting and hidden fees.

6. **Use Conservative and Rated Investment Services.** For nonprofits lucky enough to have endowment funds, investments, and reserves, place these funds with reputable and rated investment firms. Ask a board member familiar with banking and investment practices to review the investment statements to be sure that the investments are appropriate for a nonprofit (nonprofits are held to a “prudent investor” standard of care, and prohibited from making risky or speculative investments).
  
7. **Closely monitor cash events.** Have at least two vetted volunteers monitor cash receipts at events where cash plays a large part of the revenue (gate receipts, cash sales or products at an event, silent auction payments). Insist on taking your time to calculate amounts due and in counting money. It is very easy to scam cash when there is a crowd of people competing for the person “running the till” at a cash-intensive event.
  
8. **Pursue bad checks.** It is tempting to “let go” bad checks because of the hassle involved - especially when a small amount is involved. Knowingly writing bad checks is a criminal offense, and can be costly to the nonprofit in bank fees. Have a system and policy to pursue repayment of bad checks, and (if necessary) keep a list of and enforce “cash only” customers.
  
9. **Verify Credentials.** Verify credentials of any professional services you partner with or hire. Many times, a quick “Google” search will confirm (or not) credentials claimed by a new acquaintance/potential project partner. Watch for suspicious “blanks” in someone’s history or credentials, or credentials that seem “too good to be true.” Ask for and check references.
  
10. **Secure the Premises.** Have a practice of locking all doors when the nonprofit business is closed and organize your office space for secure and monitored access during the day. Is the door visible from the office so someone can monitor public traffic? Are valuables (cash, computers, supplies) secured from public access during business hours? Is someone ALWAYS in the office during business hours or when the office is accessible to the public?
  - a. Apply a philosophy of security to any public event sponsored by the Nonprofit to extend physical security practices to event sites.
  - b. Don’t forget to secure computers from outside invasion. Be sure the software monitoring, virus and spyware is up-to-date and activated. Safeguard and use passwords for computer access, and backup regularly.