



# ***Fraud is a Crime of Opportunity: Is Your Not-for-Profit a Target?***



[www.kbgrp.com](http://www.kbgrp.com)

***Brought to you by:***  
***Robert J. Lane, CPA***  
***Patricia Entsminger, CPA***  
***(Shareholders)***

***Kerkering, Barberio & Co.***  
***Certified Public Accountants***  
***1990 Main Street, Suite 801***  
***Sarasota, FL 34236***  
***and***  
***6320 Venture Drive, Suite 203***  
***Lakewood Ranch, FL 34202***

***www.kbgrp.com***

***Phone:***  
***(941) 365-4617***

***Emails:***  
***rlane@kbgrp.com***  
***pentsminger@kbgrp.com***

***Dated:***  
***June 29, 2011***

Financial fraud has been on the rise, and it is no secret that not-for-profits have seen an increase in losses. The reporting of fraud and the bad publicity could reduce contributions and grants in the future and make it difficult to fulfill your organization's mission. As many organizations are struggling to keep their donors engaged, the risks to your reputation should be top of mind with you and your Board.

A recent study noted that on average it takes 18 months for an employer to catch an employee who is perpetrating fraud. The median length for fraud schemes at not-for-profits was 24 months. The median fraud loss for not-for-profits was \$109,000. The most common internal methods used were check fraud, embezzlement, skimming, payroll fraud, financial statement fraud, bribery and corruption. Compounding these concerns is the increase in external criminal fraud through computer network intrusions, online banking fraud and payment fraud.

Every one of the above has the opportunity to financially impact your organization. You cannot afford not to take action. Now is the time to take a closer look at your banking procedures and ensure that your policies, controls and systems are designed to protect you from fraud. Reduce the opportunity by implementing best practices.

Document and review the following banking controls:

- Limit authorization. Only give financial access to employees who need it.
- Review bank documents and contracts carefully to reflect authorization limits.
- Update signature cards at least annually and immediately when signers change.
- Require your bank to document individuals authorized to request and delete bank services.
- Segregate paper and electronic transactions into separate accounts to quickly identify fraudulent transactions.
- Review account activity daily. Report unauthorized activity to your bank immediately.
- Reconcile bank accounts daily and monthly.
- Review and research undeliverable and outstanding checks. Record as unclaimed property liability and destroy.
- Utilize dual controls for initiation of electronic transactions such as wire transfers and ACH (Automated Clearing House) transactions.

Address your organization's system controls:

- Install a firewall and all security patches and updates for your operating system. Frequently update virus and spyware protection on every computer you use to access the internet and online banking.
- Review employee access privileges regularly. If an employee transfers to a new department or position, review what systems the individual can access. If the employee leaves the organization, contact your bank immediately.
- Separate controls for your business online banking application. Use one computer to create online payments; have a second user approve from a different computer.
- Limit internet use on computers used for online banking. The American Bankers Association and the FBI are advising small and mid-size organizations that conduct financial transactions over the internet to dedicate a separate PC used exclusively for online banking. This reduces the risk of malicious programs being introduced to your systems.
- Use two-factor authentication, login ID and password, to strengthen transaction level security. Educate employees not to share logins and passwords and design back-up procedures for holidays and vacations of users and approvers.

Payment controls and best practices:

- Paper based transactions – checks:
  - Use an established check vendor, limit the check style and incorporate security features into the design.
  - Utilize a secure storage area with controlled access. The signer should not have access to the blank stock.
  - Elect check safekeeping at your bank and eliminate the need to receive and store cancelled checks, which are an opportunity for fraud.
  - Utilize Positive Pay Services at your bank including payee and teller protection at your bank. This solution will provide you with the ability to identify, review and reject altered and fraudulently replicated checks before they are paid.
- Electronic transactions - ACH and wires:
  - Utilize ACH blocks and filters at your bank. These services allow you to subscribe to daily reports to monitor, filter and authorize ACH transactions and reject those that are not approved.
  - Require dual approval for creation of user authority, transaction or file creation that will move money through your accounts.
  - Establish funds movement transaction limits by account and user in your online banking system.

Consider acting on these four critical objectives to make it difficult to commit fraud against your organization and the crooks will likely look for an easier target.

- Implement a sound separation of duties, policies and practices.
- Review your policies, controls and systems on a semi-annual basis.
- Conduct surprise audits during vacations and holidays.
- Seek banking tools to simplify the activities before your organization becomes a victim.

It is important to understand your financial transaction exposure. Those looking to commit fraud do not need to ask your permission to debit your account via the ACH. They can create fraudulent checks using your account information quickly and easily. Unless you implement safeguards and procedures, your accounts are a moving target for fraud. It is often assumed that financial institutions are responsible for losses resulting from fraud. However, an organization may be held responsible in some instances. Financial responsibility is determined on a case-by-case basis, depending on the facts of the case and applicable law. Fraud loss will more often be borne by the party who was in the best position to have prevented the fraud from occurring. Consult your legal counsel for more information about your liabilities.

###

We would be happy to assist you with any of your questions. Please call us at 941-365-4617 or email Rob Lane at [rlane@kbgrp.com](mailto:rlane@kbgrp.com) or Patricia Entsminger at [pentsminger@kbgrp.com](mailto:pentsminger@kbgrp.com).