VIS CONNECTIONS

 Summer 2012

We are happy to provide you our publication for nonprofit risk managers, as part of our service to you. The titles in the contents section link directly to their articles. If you need to change the email address to which this is sent, please contact us. Be sure to include your name, organization and address. You also are welcome to call us at 800.222.8920 for assistance.

In this issue…

Charity Fraud Is Huge…But Shrinkable

By Gary Snyder

Editor's note: This article is contributed to *VIS Connections* by Gary Snyder, founder and principal of *Nonprofit Imperative (NI)*, a national forum for nonprofit information. As a noted expert on issues facing philanthropy, Mr. Snyder has been a guest lecturer and has been consulted by Congress, and his work has been cited by hundreds of media. He has authored *Nonprofits: On the Brink*, the often-quoted guide to best practices and key concepts. His latest book, *Silence: The Impending Threat to the Charitable Sector*, is an investigative work about misdeeds in charitable organizations. He is the publisher of the *Nonprofit Imperative* newsletter and blog, and has twice authored the Governance Chapter of the *Michigan Nonprofit*

Management Manual (fourth and fifth editions). He can be reached, and subscriptions requested, at gary.r.snyder@gmail.com. VIS appreciates Mr. Snyder's contribution to our publication.

* * *

The vast majority of donors do not want to believe it. Many in the charitable sector leadership continue to deny it. Most regulators are incapable of doing anything about it. By all documentable accounts it is rising astronomically.

It is nonprofit fraud.

The Problem

Research by Mark Kramer, author of *Do More Than Give: The 6 Practices of Donors Who Change the World*, shows that theft in the nonprofit sector accounts for 13 percent of annual donations, or about twice the rate of fraud in the for-profit sector. These findings are consistent with a 2008 study, published in *Nonprofit and Voluntary Sector Quarterly* and reported in the *New York Times*, suggesting that $40 billion is stolen annually.

More recently, Bart Beavers, who regulated nonprofits as Texas attorney general, estimates that charities lose about $51 billion a year to thefts from employees and others, with approximately one out of six being affected to one degree or another. That represents a huge chunk of the nearly $300 billion nonprofits collect annually from private donors.

The 2012 Global Fraud Study conducted by the Association of Certified Fraud Examiners listed corruption cases by industry. Religious, charitable or social services accounted for 22.2 percent of cases, according to the study.

Charity fraud is big money.

Let's look at the factors that have allowed this fraud to grow so much, then turn our attention to ways we can shrink it – ways that will help the individual nonprofit reduce its own risk.

An environment of vulnerability

- Many charities (as well as for-profits) rely too heavily on their chief executives. This is dangerous. The ultimate decision-maker is the board. The executive needs to be monitored, not feared.
- Most organizations are devoid of internal controls that have been adopted by the board and understood by all.
- Employees and volunteers closest to the money often are too trusted. Even if there are controls in place, those controls are not followed.

- Too many organizations fail to focus on the agency's mission. Every activity must relate to the mission.
- Lack of financial oversight leaves the organization weak. The board must provide governance of its resources, and that means leadership must have financial strength and literacy within its ranks.
- Program strength should not be built at the expense of financial controls. If there are no controls, programs become unprotected.

Risk management, for a healthier environment

Now that we have determined that there is a problem and that there are systemic weak spots, how can we address them?

The temperature of the organization is set from the top. The transference of *ethical administration* must be generated from the board to management and then to staff members. Performance must be monitored, and failure to follow standards must be met with severe consequences. Honesty and vigilance must be the watchwords.

The standards that are set should have *checks at every level*. Dividing tasks helps prevent fraud. With small organizations, involve the board membership in these tasks.

Although I am in the minority on this issue, I believe credit cards should be limited *to a very few*. Prompt reimbursement of submitted receipts is a safer control. Under no circumstances should debit cards be used, because protections are limited and missing money can be difficult to recoup.

Set up a meticulous accounting system that records every transaction. A clear paper trail, even for the smallest transactions, shows who, what and when. Internal controls that require multiple signatures and cash controls will dissuade fraud.

Checking backgrounds of prospective employees (and volunteers, if they handle money) seems to be an elementary process. Unfortunately, the perceived urgency to make a hire, or just plain neglect, has resulted in misconduct that has embarrassed and damaged the mission of many organizations.

Developing a budget can be an enlightening exercise for both board members and staff. The budget-setting process can hone realistic expectations. Try to stick to the budget, with as few alterations as possible. Each line deserves careful attention of all those responsible for the organization's financial well-being. With this commitment to budget control, over time volunteers and staff alike will polish their skills and insight.

From my experience, *audits have not been the savior that many believe*. Since most charitable organizations are small, full-blown audits usually do not warrant the expense. Too frequently, malfeasance is missed by the outside set of eyes. Even at larger nonprofits, we have seen audits fail to notice vital issues.

With the right practices in place, and commitment behind them, you have a great opportunity to make sure the problem of fraud does not affect your organization, and that you contribute to reducing the larger problem that is afflicting the nonprofit sector.

Editor's note: VIS makes available to its members a two-page document with suggested techniques for preventing acts of dishonesty by employees and volunteers. It complements the valuable suggestions Mr. Snyder has provided. For a copy of *Preventing acts of dishonesty by employees and volunteers*, please contact VIS Executive Director William Henry by email, or by phone at 800.222.8920.

Let us help you honor your volunteers

"Volunteerism is both an expression of patriotism in a pure sense and the means by which a democratic society remains 'by the people.' – excerpt from *A History of Americans As Volunteers,* by Susan J. Ellis and Katherine H. Campbell (available at www.energizeinc.com).

When you think of your volunteers, it's likely that you think immediately of your best – those who love their work and your organization, and are always there for you. We'd like to help you tell others within the Volunteers Insurance Service community how great those individuals are. With the redesign of our Website (www.cimaworld.com), we will be making use of social media such as Facebook and YouTube to share resources, stories, successes, and profiles of volunteers.

What is it that makes a particular volunteer special to you? Is it the many years she has served? The way he helps others in a way he himself once was helped? The distance she drives a client, in all kinds of weather, for the services the client needs? We encourage you to send us a short profile and photo of the volunteers you are proud to recognize and to honor publicly. Or consider doing a short video interview with them. There is no limit on how many volunteers, or how often you would like to share. Just email VIS Executive Director William Henry with the information, and include your phone number in case he needs more information. We will let you know when the volunteer's profile is ready for viewing.

And please be sure to "like" us on Facebook! – www.facebook.com/cimaworld.

New document available from VIS – *Insurance basics*

Organizations participating in our Volunteers Insurance Service (VIS) program often have questions pertaining to other types of insurance, in addition to volunteer insurance. In response, we have developed a document called *Insurance basics for nonprofit organizations*.

This five-page document is intended as general and abbreviated guidance. Sections include general liability, directors and officers liability, workers' compensation, auto coverage for organizations that own vehicles and those that do not, umbrella liability, employee/volunteer dishonesty coverage, property, and other coverages.

The document also explains how the accident medical insurance, volunteer liability and excess automobile liability coverage available through VIS integrate with other insurance policies the organization might have, or wish to consider.

Please contact VIS Executive Director William Henry by email or at 800.222.8920, and he will be happy to email you a copy of *Insurance basics for nonprofit organizations* at no charge.

Social media – rules of the road for nonprofit organizations

Editor's note: Kenneth Liu (*kel@gg-law.com*) is an attorney specializing in intellectual property and Internet issues, with Gammon & Grange, P.C. (*www.gg-law.com*), a law firm serving charities and other nonprofit organizations throughout the United States. Following are excerpts from an article Mr. Liu published recently in the Law For Change newsletter (*www.lawforchange.org*). The entire article can be found at *www.tinyurl.com/socialmedialegalrisks*. The article primarily addresses risks involving employees' use of social media; we asked Mr. Liu to comment on any differences that might exist with respect to volunteers' use of social media. Here is his response:

"The status of volunteers is an ambiguous aspect of the law because it depends on the specific circumstances, the area of the law at issue, and which state the organization is located in. In some circumstances they can be considered as employees but in other circumstances they are not. As for the *respondeat superior* doctrine (see #2, below), a key factor will be how much control the organization has over the volunteer's activities and whether it is fair under the particular circumstances to hold the organization liable for the volunteer's actions."

1. Direct your employees not to post anything they would not want to see on the front page of *The New York Times* or to hear on the witness stand.

Even if you use a pseudonym online, there are ways that the public, including reporters, can discover who you are. Remember also that any data posted online is not only available worldwide, it can potentially remain forever. Even when privacy settings are restricted or a page is password-protected, there are still ways to retrieve data using cyber forensic tools, even after the data is "deleted."

Generally, information posted in social media can also be used as evidence in a court of law. And even what you delete from social networks can get you into trouble. In 2011, a lawyer in

Virginia told his client to remove several photos from his Facebook account for fear that they would prejudice his wrongful death case brought after his wife's fatal automobile accident. A judge chastised the lawyer for treating social media data differently from other forms of evidence, which litigants are prohibited from deleting once litigation is imminent. The judge ordered the lawyer to pay $522,000 for instructing his client to delete the photos, and the client to pay $180,000 for doing so.

2. Actions taken by an organization's employees can be held against the organization.

Under the legal doctrine of *respondeat superior*, employers can be held liable for the activities of employees. In the social media world, the line between one's personal life and professional life is becoming increasingly blurred. This ambiguity increases the risk of an organization being held liable for the online posts of its employees.

Many employees of charities and advocacy groups are passionate about their work, so they naturally speak out publicly on issues relating to their field. If an employee posts an offending statement against another organization on Facebook or another social network, the statement could be attributed to the employer, even if the employee posted on his or her own personal account. The risk is higher if the employee's profile clearly states his or her organization, his or her title as a senior staffer, and includes the logo of the organization.

Organizations can minimize such risk by requiring that personal postings and blogs of employees that relate to the employer's field be carefully distinguished from those of the employer, such as by including a disclaimer stating that the views and opinions expressed do not represent those of the employer. Prohibit employees from using the organization's logo on personal accounts.

3. If you're not allowed to do it in the "real world," you're probably not allowed to do it in a virtual world.

Although social media might often feel like a separate world, it is still subject to the laws of the real world. The context might be different, but the obligations to which a nonprofit is subject in the real world generally also apply online. Social media may be more casual, but that does not excuse illegal activity. Below are some sample legal issues implicated by social media use.

> ***Intellectual Property (IP).*** Nonprofits typically have two primary forms of intellectual property (IP): trademarks and copyright. Trademarks are words or designs that identify the source of a particular product or service, including organization and program names, logos, and slogans. Copyrighted works include any content expressed in a tangible medium, including Websites, books, reports, videos, music, photos, graphics, etc.
>
> Organizations need to prevent their employees from misusing IP in two ways: (1) misusing the organization's own IP in a way that jeopardizes the organization's rights, and

(2) infringing on the IP rights of others. An employee can misuse his or her employer's IP by, for instance, using the organization's trademarks without authorization to misrepresent the organization's position on issues, to provide false information, or to make defamatory remarks. This can happen if an employee uses the organization's logo on the employee's personal blog or other social media account.

An employee can violate others' IP by, for instance, copying and using others' trademarks or copyrighted works on social media without a proper license. Just because something is available on the Internet does not mean that it is free for anyone to copy. Unauthorized copying can result in bad public relations as well as significant liability.

Hostile Work Environment, Harassment, and Discrimination Claims. According to a 2011 Associated Press/MTV poll, 59% of young adults have experienced some form of harassment through social or online media. While most employers recognize they have a duty to maintain a workplace atmosphere free of illegal harassment, they often don't realize that they may face liability when employees use social media to make discriminatory statements, racial slurs, or sexual innuendos directed at co-workers. Recently, a California jury awarded $1.6 million to a juvenile corrections officer whose co-workers had ridiculed his severely deformed hand, in an unofficial blog.

Political campaign activity. 501(c)(3) organizations are prohibited from participating in any political campaign on behalf of, or in opposition to, any candidate for elective public office. Violating this prohibition may result in excise taxes and possibly even revocation of tax-exempt status. Organizations can unwittingly violate this prohibition if their employees speak out in favor of, or in opposition to, political candidates through social media and their statements are attributed to the organization.

Charitable solicitations. Thirty-nine states require some type of registration for charities soliciting funds within their jurisdiction. In some states, the mere existence of a "Donate Now" button online can trigger the registration requirement. Use of social media to raise funds can also trigger the requirement, especially if the fundraising is directed toward people known to reside in a particular state. If your organization solicits funds online or through social media, be sure to comply with charitable solicitation laws in the appropriate jurisdictions. Failure to comply can result in significant fines.

Improper Disclosure of Confidential or Other Protected Information. Organizations must take care to prevent disclosure of confidential or proprietary information through social media. For instance, if an employee blogs about a donor or a constituent your organization has served, he must be careful not to reveal any personally identifiable information without authorization.

These and many other legal risks can be minimized by taking certain precautions, such as the following.

4. Implement a social media policy to govern use of social media by employees.

The foregoing concerns certainly do not warrant a ban on employee use of social media, not necessarily even within the office. If your nonprofit wants to get its message out and engage its donors and constituents, you not only want to permit employees to use social media, you may want to actively encourage it, depending on your organization's field and mission. However, it is crucial that organizations act prudently in guiding and training their employees in using social media appropriately.

One key step in protecting your organization is to have a written policy that provides guidance on what your employees can and cannot do in social media, both in their role as employees and in their personal use. Because every organization has a unique mission, purpose, and culture, each organization should develop a policy that addresses its own needs. For instance, groups working on sensitive matters may find it necessary to be more strict, while others that have a broader educational or advocacy mission may want to be more lenient in letting employees get the message out. Therefore, it is important to tailor a policy to the needs and goals of your organization.

5. Instruct employees to use only official organization social media accounts for conducting business.

Employees' use of personal social media accounts for official organizational business can not only cause confusion between employees' professional and personal online identities, it can also create problems when employees leave the organization. For instance, the organization can lose valuable history, content, and contacts if it can no longer access accounts used by a former employee. Also, organizations can end up in disputes with former employees about ownership of accounts and data. To minimize these concerns, require employees to conduct official business only through the organization's social media accounts, not through personal ones, and insist that the organization's accounts should not be used for personal affairs.

Editor's note: The National Labor Relations Board has taken a consistent position recently that employees' comments on social media regarding their employment are considered protected activity in many cases. You might want to read "They can't say that! Can they?" in the Fall 2011 issue of *VIS Connections*. To view the issue, go to www.cimaworld.com, click on the "Nonprofits" section, and see the menu on the left side of any page in that section for a link to *VIS Connections.* The article also includes guidance for developing a social media policy for your organization.

In May, the NLRB released a **report on social media**, describing what it considers acceptable, and not, in an employer's social media policy. According to the NLRB, a policy violates the National Labor Relations Act if it would "reasonably tend to chill employees" in their exercise of rights under the Act.

The NLRB's interpretations of the law apply equally to employers who work with collective bargaining agreements and those who do not.

The following article in this issue addresses another NLRB issue: its recent ruling limiting an employer's ability to require confidentiality regarding internal investigations.

NLRB limits confidentiality of internal investigations

The National Labor Relations Board (NLRB) has just ruled that an employer cannot require employees to refrain from discussing an internal investigation in which they are involved. In ***Banner Health System***, the board ruled that the employer's desire to protect the integrity of the investigation is outweighed by the employees' rights, under the National Labor Relations Act, to engage in concerted activity related to their compensation, benefits and working conditions.

In order to require employees to maintain confidentiality, the board ruled, the employer must "first determine whether…witnesses need protection, evidence is in danger of being destroyed, testimony is in danger of being fabricated, or there is a need to prevent a cover-up." In an analysis, the law firm Mintz Levin Cohn Ferris Glovsky and Popeo notes, "Essentially the Board is requiring employers to make a preliminary determination regarding confidentiality before they conduct any investigation." The analysis also notes that the ruling appears to conflict with the NLRB's own guidance regarding investigation of harassment complaints, and concludes:

"Regardless of the merits of the Board's decision, employers should review their existing investigation policies and procedures to determine whether confidentiality provisions are 'overbroad' under the Board's analysis. Employers should also strongly consider documenting their efforts to analyze the confidentiality issue before commencing any investigation (and to revisit the issue as necessary during the investigation). We suspect that, in many cases, the employer can sufficiently document a need to protect the complainant (or other witness) and a separate need to promote witness candor and/or prevent witness dissembling in order to require confidentiality."

Developing leadership on the job

Studies by organizations including the Annie E. Casey Foundation, Meyer Foundation, Idealist.org and recently The Bridgespan Group have found that nonprofit organizations often fail to develop potential leaders within their ranks, or otherwise plan adequately for leadership succession. For example, according to the Bridgespan Leadership Development Diagnostic Survey, only half of the 225 nonprofit leaders surveyed evaluate leadership potential, as well as current performance, of staff. In only one out of three organizations are the current leaders made

accountable for developing new leaders, and of those organizations that have leadership development plans in place, only 23% actually track progress.

"Failure to invest in leadership as well as services puts the entire mission at risk. And based on our research, it's a risk that's unnecessary," the study's authors say.

Bridgespan followed that survey with a 98-page report, available as a free download at www.bridgespan.org. "Plan A: How Successful Nonprofits Develop Their Future Leaders" includes recommendations on how to engage senior leadership, how to understand future needs, how to develop future leaders, hiring externally to fill gaps, and monitoring and improving practices. Each chapter includes specific steps, with case histories, checklists and questions that can help expose specific needs.

Leaders are made, not born

One of the key points of the "Plan A" study is that on-the-job leadership development is more valuable than simply sending someone to a class. "The most effective kind of leadership development happens on the job, every working day, driven by line managers whose words and actions can stretch the leadership potential of their people – or stifle it."

IRS: Link between good governance and tax compliance

In a recent speech at Georgetown Law School, the IRS director for tax-exempt organizations said that the IRS is developing data to show a direct correlation between good governance practices and compliance with the agency's requirements for nonprofits. Lois Lerner said that the IRS is more likely to find the Form 990 acceptable if it contains the following:

- Written mission statement
- Use of comparability data in determining compensation of staff
- Written procedures for use of the organization's assets
- Review of the Form 990 by the entire board of directors

One common mistake Ms. Lerner mentioned was the inclusion – usually inadvertent – of Social Security numbers within the Form 990. Those cannot be deleted, and the Form 990 is available online for anyone to view, so identity theft is a real risk.

Resources

www.irs.gov/charities and www.stayexempt.irs.gov

In the event of a volunteer claim…

Questions sometimes arise about the procedures to follow in the event of a claim involving a volunteer. In the "CIMA Volunteers Insurance" section of www.cimaworld.com, you will see a "Forms" link to the complete instructions and the proof of loss form. There also is a downloadable brochure for volunteers, with instructions. Here is an overview of the steps:

For injury to a volunteer

1. The organization should complete page one of the proof of loss form, have the injured volunteer complete the second part, *make a copy*, and fax the form to CIMA at 703.739.0761 right away. Even if there are no medical bills yet, please do not delay submitting the form to CIMA. If the volunteer is unable to complete the second part of the form immediately, just write "signature to follow" where the volunteer is to sign, and fax the form. Then, whenever the volunteer is able to complete his or her part, just fax the completed form to us.

2. The organization should give a completed copy of the proof of loss form to the injured volunteer, to give to his or her medical providers. If the volunteer has primary insurance (Medicare, Humana, etc.), the primary insurance must pay first, and our volunteer insurance will be secondary. Fax us copies of the primary insurer's Explanation of Benefits, itemized bills showing the treatment provided and treatment codes, and any other paperwork from the insurer. If the volunteers inform their providers that they do have excess coverage that can be billed for any balances due, once the primary insurance has paid, the providers will send bills directly to us, and the volunteer can be bill-free. Note that our accident coverage also will reimburse the volunteer for deductibles and copayments they have incurred. If the volunteer *does not* have any primary health insurance, give the completed proof of loss form to the volunteer (make a copy first), and tell him or her to inform the provider that our program is their primary coverage for this incident, and that bills should be sent directly to us.

3. Preferred Care, Inc. is engaged by CIMA as the third-party administrator for our accident medical claims and, as such, reviews and pays the claims on behalf of the underwriting company. Tell your volunteers they might receive information requests or other correspondence from Preferred Care regarding their claim.

Note: If you prefer to scan documents and email them rather than fax them, that is fine. You can email them to Joan Wankmiller (jwankmiller@cimaworld.com) or Vicki Brooks (vbrooks@cimaworld.com).

For volunteer liability claims and excess automobile liability claims

As soon as you become aware that a volunteer is, or *might be*, held responsible for injuring someone else or damaging someone's property, or is at fault in a vehicle accident while volunteering, please call or email Joan Wankmiller (jwankmiller@cimaworld.com) or Vicki Brooks (vbrooks@cimaworld.com) at 800.222.8920.

It is important to report the incident as soon as you become aware of it, and CIMA will handle the claim from there. Once you contact us, we will ask you to provide the following information as soon as you are able:

1. The volunteer's description of the incident

2. The volunteer's name, address, phone number, personal liability insurance company and policy number if any (such as homeowner's insurance or personal umbrella policy), claim number under that policy or policies, and contact information for that insurance company's claims adjuster. If there is no primary insurance, our coverage will be primary, from the first dollar.

CIMA service team for VIS® members

Volunteer insurance:
Victoria W. Brooks, Account Executive
Joan R. Wankmiller, Account Executive

Directors and officers liability:
Aaron Jones, Account Executive

Laurie S. Coleman, Senior Vice President

Toll-free: 800.222.8920 or 800.468.4200

We are always happy to serve our members. Please let us know, any time we can be of help!

VIS® Commitment

Volunteers Insurance Service is committed to providing its members a complete resource for the nonprofit organization's risk management needs. Our services include:

- Publishing ***VIS® Connections*** as one of our information resources for members;
- Maintaining for members' use a library of information relating to management of risks in the nonprofit organization;
- Researching available and appropriate insurance relating to volunteer activities;
- Designing and administering insurance programs, and compiling underwriting information;
- Providing consultation on risk management issues at no additional charge to our members, via a toll-free line (800.468.4200);

- Assisting members, on request, with matters relating to insurance.

Insurance and administrative services are provided to VIS® and its members by The CIMA Companies, Inc. and/or one of its affiliated companies.

VIS®'s Articles of Incorporation, Financial Information, and a list of the members of VIS®'s Board of Directors are available to VIS® Members upon request.

CIMA licensing information

The following licensing information is being provided in order to comply with state governmental regulations:

Volunteers Insurance Service Association, Inc. is a risk purchasing group formed and operating pursuant to the Liability Risk Retention Act of 1986 (15 USC 3901 et seq.)

Notice to Texas clients: The insurer for the purchasing group may not be subject to all the insurance laws and regulations of your state. The insurance insolvency guaranty fund may not be available to the purchasing group.

Notice to California clients: License #0B01377 and #0A06046, CIMA Companies Insurance Services

Notice to Minnesota clients: License #009285 and #07544084, The CIMA Companies, Inc.

CIMA, one of its subsidiary companies and/or an authorized individual is licensed in all jurisdictions. Please contact CIMA at 800.468.4200 if you would like information about our licenses.