NonProfit Financial Managers

A Resource for the areas of Finance, IT, Human Resources, and Office/Facilities Management

Volume Seventeen, Number Two Oct 2009

For information, go to **npfm.org**, or contact Mitzi Fennel at 617-547-1063 x235 or Jessica Zander at 617-850-1752.

Mark Your Calendars

All of our meetings take place on the **last Tuesday** of each month. No pre-registration required. Upcoming dates:

- **Oct 27 Technical aspects of the same law (note: the implementation for this law has been moved to 3/1/10)**
- **Dec 1 (due to Thanksgiving) Using volunteers in the current economy**

NPFM Membership Information

The annual membership fee of $100 covers monthly mailings and other operating expenses. The membership period is from September to August. A part-year membership for $60 is offered for those joining after January 1st, which covers membership through August. Full-time students are welcome to join at any time without paying a fee.

In addition to attendance at monthly meetings, members receive a monthly newsletter and access to the NPFM e-mail forum. Lunch is provided for all attendees at meetings. There is a $12 meeting fee for non-members, and since membership is by organization, there is no limit of individuals from any one organization who may attend the meetings.

R.S.V.P's for the meetings are not required.

For renewals or new membership fees, please make your check out to:
NonProfit Financial Managers
C/O Child Care Resource Center
130 Bishop Allen Drive
Cambridge, MA 02139

Contact Mitzi Fennel at 617-547-1063, x235 for more information.

The Next Meeting

Topic: Technical aspects of the Privacy law, presented by All Covered

Date: Oct. 27, 2009

Location: United South End Settlements
566 Columbus Ave., Boston

Time: 12:00 PM – 1:30 PM

Last month we heard about the legal aspects related to the new Privacy Law taking effect on 3/1/2010. This month we will be delving into the technical requirements. The law, designed to prevent identity theft, attempts to regulate how companies are permitted to store, and how they monitor personal/private information. Therefore, companies are required to establish security protocol, including which employees have access to what information, and whether the proper protection has been applied to sensitive information. All Covered, Inc., will present.

Recap of September Meeting

Complying with the new Massachusetts Data Security Regulations *

** PLEASE NOTE: This information was prepared in late September 2009 and is current in light of the law at that time. It is expected that modifications to the law will continue to occur. Each organization should perform its own due diligence to ensure compliance with the law.*

In September Sam Hudson, Counsel for Foley Hoag LLP, spoke with the NPFM group about the upcoming Massachusetts Data Security Regulations. As the first law of its kind starting on March 1, 2010, Massachusetts is requiring that all businesses which have access to personal information of a Massachusetts resident have a comprehensive written information security program. This regulation will be monitored by

the Massachusetts Attorney General and penalties may include fines of up to $5,000 per violation, as well as costs of investigation and litigation.

"Personal information" is defined as a person's first and last name as well as ONE of the following:

- Social Security Number
- Driver's license number or other state issued I.D. card number
- Financial account number – including credit cards, debit cards, bank account, et al

It is expected that the Massachusetts Office of Consumer Affairs will provide a sample policy to assist organizations in establishing one of their own. Organizations will be held to the standards that they set forth in their plan so make sure that your organization can live up to its own policy. An organization increases their liability risk by adopting a policy that they do not follow.

Suggested elements of a written information security program should include:

- Designation of someone within the organization to act as the security officer.
- Policies that outline systems, practices and expectations for storing, accessing and transporting personal information on all electronic devises.
- Protocols related to personal information that are integrated into the employee handbook including general expectations, disciplinary steps for those who violate policies, and procedures surrounding employee separation.
- Expectations of third party service providers regarding their own capacity to protect personal information
- An incident response plan including actions which should be taken in the event of a data breach as well as a review of the breach to mitigate future risk.
- Dissemination written security policy to all employees in a way that ensures everyone receives it – best method, have them sign off on having read it!

Suggestions for mitigating risk within your organization:

- Understand where personal information lives within your organization as well as with their third party vendors.
- Conduct an assessment to consider the foreseeable risks associated with your particular business.
- Identify the minimum amount and type of personal information that needs to be collected by the organization and limit access to this information as much as prudently possible.
- Ensure that personal information is either stored under lock and key, password protection and/or by electronic encryption.
- Establish expectations and protocols throughout your organization and create processes for monitoring and identifying security violations.
- Ensure that stringent IT computer security standards are in place (malware protection, anti-virus, firewalls, passwords, etc.).

This law has been evolving over the past 1-2 years and will likely be modified before its final adoption and launch date of March 1, 2010. Please refer to the following websites for additional information:

- OCABR website at www.mass.gov
- Foley Hoag Privacy Blog at www.securityprivacyandthelaw.com

Job Openings…

The NPFM group has a section on their website for job postings. Check out our website at www.npfm.org for a complete list of jobs. Contact David Richardson at dr44@verizon.net with questions or postings.

NPFM E-mail Forum

One of the benefits of membership in NPFM is a subscription to our e-mail listserv. We encourage members to post questions, announcements and new developments in finance and administration. All new members who provide e-mail addresses are automatically subscribed. To post messages send to npfm@topica.com

NPFM Steering Committee

The Steering Committee consists of several members who are responsible for the meeting topics, speakers, and other details surrounding the group. If you are interested in joining the steering committee, or in submitting ideas for future sessions, please contact any of the existing members, by e-mail or in person at a meeting.