

- Come visit us at the 55<sup>th</sup> Annual Employee Benefits Conference in Orlando, FL on Nov 8-11, 2009. Booth #205

### Special Interest Articles on back:

- Computer Theft claims continue to rise.
- ERISA Bonds: An Overview

## Privately Offended

An off-hand comment or joke—one that has been often shared in the past—can leave an entire organization vulnerable to allegations of misconduct. Even the ethics of a seemingly earnest business decision can be called into question.

Often, the individuals offended by some action opt to move directly into litigation, leaving management and leadership feeling completely blind-sided. Consider a few examples of situations that might arise:

- *A female administrative assistant overhears a conversation between the President and Treasurer which includes some colorful language not intended for her ears...she is privately offended and decides to sue.*
- *A Latino business agent emails an in-depth joke exploiting Latino stereotypes to the entire office...a bookkeeper is privately offended and decides to sue.*
- *A retired business agent is allowed to keep his union vehicle since it is older and has many miles...due to a perception of poor financial management, A member is privately offended and decides to sue.*

It makes little difference if the alleged actions actually offend the accuser or if the individual is just greedy or opportunistic. What matters is that these individuals intend to sue to obtain compensation for internal distress. Long-term employees are not immune. Even those individuals who seem easy going may reach a boiling point. There are few limits to the possible offenses on which a lawsuit could be based.

For many of these issues, the union attorney may, ultimately, get the case thrown out. Nonetheless, the average employment practices liability case costs the defendant upwards of \$100,000. *Can your organization afford to pay that much in legal fees?*

A Union Liability policy is designed to cover the defense costs for the Local and the individual labor leaders. Adding this layer of protection just makes sense since you never know who will be privately offended.

## Identity Theft: How Vulnerable Are You?

Over 8 million U.S. adults discovered they were victims of identity theft according to a 2007 Federal Trade Commission report. 56% of the victims did not know how the information was accessed while 5% knew the breach occurred at an organization that maintained the personal information in their records.

As the guardian of your membership's sensitive personal data, it is your responsibility to ensure the information is protected from constantly-changing and increasingly malicious attacks.

Data security breaches can happen to any organization at any time or place. Your computer network can be hacked, agent's and organizer's laptops can be stolen, paper records can be lost or *misplaced*, and e-mails can be sent using incorrect or unauthorized distribution lists. The consequences of these security breaches are always costly.

The best way to protect yourself, your organization, and your membership is to obtain Data Compromise coverage. Fireman's Fund Insurance Company has added Data Compromise coverage to our labor organization program. The coverage includes:

- Legal review and recommendations on how to respond to a breach
- Forensic technology services to research the cause and the scope of the breach
- Notification of affected individuals
- Provides credit monitoring services for individuals whose personal info has been compromised with Access to one of the industry's leading security and identity recovery specialists

Are you protecting sensitive information as best you can? Too much is on the line for the answer to be "maybe."

Real Claims  
Examples:

- Stolen briefcase with retiree info; the cost for notifying approximately 350 people of potential identity theft and establishing 1yr credit monitoring.

Cost of claim:  
\$50,000

- Stolen PC with health plan participant data – notifying more than 1,000 people of potential identity theft and establishing 1 yr credit monitoring.

Cost of claim:  
over \$100,000

## ERISA Bonds – What You Should Know

### ERISA Bonds – The Basics

ERISA bonds are designed to protect employee benefit plans against losses sustained due to acts of “fraud or dishonesty” by persons whose positions require them to manage, handle, or otherwise exercise discretion over plan assets.

Fraud or dishonesty includes, but is not limited to, larceny, theft, embezzlement, forgery, misappropriation, wrongful abstraction, wrongful conversion, willful misapplication, and other acts where losses result though any act or arrangement prohibited by law.

### Watch Out For These Gotchas!

Most bonds have stipulations that, in effect, automatically cancel coverage for any individual known by plan officials to have engaged in a fraudulent or dishonest act *at any time prior* to his/her relationship to the plan.

Plan fiduciaries can be held personally liable under ERISA’s general fiduciary rules for any loss to the plan that should have been, but was not, covered by a bond.

An ERISA bond is not the same as Fiduciary Liability insurance. The ERISA bond insures the plan against losses due to fraudulent or dishonest acts. Fiduciary Liability insurance insures the plan against losses due to a breach of fiduciary responsibility.

### Who is Required To Be Bonded?

ERISA requires that all plan fiduciaries and *all* persons who handle plan funds / assets be bonded. Committees that make investment decisions for the fund which are not reviewed or approved by another party must be bonded regardless of their role in directly handling plan funds / assets; they are exercising discretionary control over the funds.

As for outside service providers, ERISA does not require that plan sponsors or the plan pay for the outside service providers’ bond, however, outside service providers who “handle” plan assets are required to be appropriately bonded.

It is crucial that plan sponsors seek evidence showing that outside providers are bonded and these entities should obtain a bond naming the plan as the insured.

In all cases, it is the responsibility of the plan sponsors to ensure the plan is bonded in compliance with ERISA; this includes any non-exempted service providers that handle plan funds or assets.

## Beware: Thieves Want YOUR Electronics

There has been a recent spike in claims filed for stolen electronics. Anyone who has become a user of high-tech computing and communication devices is a potential target. The following recommendations can help to protect your equipment from theft.

- **Do not leave your electronics visible in your vehicle.** Laptops and smartphones are very attractive items to thieves. If you cannot carry the device with you, find a way to conceal it. (Also, beware of heat damage to the device if you do leave it in your vehicle.)
- **Do not leave your bags unattended.** Thieves are crafty and know that briefcases and backpacks often contain valuable equipment. Carry your bags with you at all times.
- **Do not leave your personal electronics unsecured at the office.** Laptop locks that can secure your computer to your desk should be used when your computer is left unattended. Phones should always be kept in a pocket or on a belt clip.

Be sure to have the appropriate insurance coverage for electronics which includes making sure they are covered outside the office or in transit. Keep receipts for new purchases to confirm the value of the item.

Consider adding Electronic Data Protection to your insurance policy to protect against losses arising from missing data as that can be one of the most expensive consequences.

