

# HUMAN RESOURCE CONNECTION MONTHLY NEWSLETTER

VOLUME I ISSUE IV SEPTEMBER 2008

## Table of Contents

*(Click on any title below to jump to that page)*

Greetings.....	1
2 NM Hospital Workers Fired for Taking Photos..	2
7th Circuit - FMLA's 1250 Hour Eligibility Requirement is Absolute .....	2
Background Investigations Keep Getting More Complicated.....	3
California Bans "Texting" Behind the Wheel; California Employers Should Update Personnel Policies.....	5
Disability Act Amendments to Take Effect January 1, 2009 .....	6
Massachusetts Data Security Regulations Effective 2009.....	8
Nabbing Workplace Thieves .....	10
OFCCP Issues New Form I-9 Inspection Procedures .....	11



Steven E. Gall  
President  
Bio

**Gall & Gall Company, Inc.** was founded in 1987, with corporate offices in Dayton, Ohio. We presently partner with customers in 19 foreign countries and all 50 states in the United States.

**Gall & Gall** was founded by **Beverly Gall**, Ohio's first female Police Chief and the third female Police Chief in the nation and **Steven Gall** a former Police Officer with over 27 years in Human Resources.

Together, their background is varied and extensive in information gathering and Human Resources.

Gall & Gall has always been looked to as a leader in Employment Background Screening Services.

### Contact Information:

E-Mail - [sgall@gallgall.com](mailto:sgall@gallgall.com)  
Toll Free 1-800-759-4255  
[www.gallgall.com](http://www.gallgall.com)

## GREETINGS

Welcome to the all New...

### Human Resource Connection Monthly Newsletter

Our aim is to reduce your HR headaches by providing the information and tools you need to make life easier! We will provide you with up to date Human Resource Information that will help you in your day to day operations.

If there is information that you are interested in seeing in this newsletter, please let us know by email at [sgall@gallgall.com](mailto:sgall@gallgall.com).

If you have a HR question email us and we can do a blind post (you will not be identified) in the newsletter and others can answer by email and we will do a blind post to you answer in the next months Newsletter.

Thank You, Steven E. Gall

## QUICK LINKS

(CLICK ON ANY LINK BELOW TO VISIT THE SITE)

**Below is a list of websites you may find useful:**

**SHRM ([WWW.SHRM.ORG](http://WWW.SHRM.ORG))**

**OHIOSHRM ([WWW.OHIOSHRM.ORG](http://WWW.OHIOSHRM.ORG))**

**MVHRA ([WWW.MVHRA.ORG](http://WWW.MVHRA.ORG))**

## 2 NM Hospital Workers Fired for Taking Photos

By HEATHER CLARK – Sep 22, 2008

ALBUQUERQUE, N.M. (AP) — Two University of New Mexico Hospital employees have been fired for using their cell phone cameras to take photos of patients receiving treatment and then posting the images to a social networking Web site.

Director of Public Affairs Sam Giammo said Sunday the photos — mainly close-ups of injuries being treated in the Albuquerque hospital's emergency room over the past few months — were posted on an employee's private MySpace page.

Giammo said he's never heard of a similar incident at the University of New Mexico Hospital or any other hospital.

A few other hospital employees were disciplined and the investigation is ongoing, he said.

UNMH values patient privacy "very, very highly and we will do everything we can to protect them," Giammo said. "We just won't tolerate unprofessional actions by any of our staff. We just won't stand for that."

The photos were discovered after a hospital supervisor received an anonymous tip about them Tuesday and launched an investigation.

Hospital managers personally oversaw the removal of the photos from the Web site and from the employees' cell phones, Giammo said.

"We have to rely on the people telling us that they don't have any others," he said.

The patients in the photos could not be notified that their pictures had been taken because their faces and personal identifying features had been removed from the photos, Giammo said.

Giammo said the MySpace page could only be accessed by the employee's online friends, not the general public.

Giammo said the employees who were fired violated a hospital policy that bans the use of cell phone cameras in patient areas. The other employees were disciplined for not bringing the photos to the attention of managers, he said.

The hospital is treating the matter as an employment issue and law enforcement has not been involved, Giammo said.

The use of cell phone cameras in hospitals have caused breaches of patient privacy or concern about such violations in California, Arizona and South Dakota in recent years.

---

## 7th Circuit - FMLA's 1250 Hour Eligibility Requirement is Absolute

By Maria Greco Danaher, Ogletree Deakins (Pittsburgh)

The Family and Medical Leave Act (FMLA) provides that an employee is entitled to leave under certain circumstances, including a serious health condition that makes that individual unable to perform the functions of his or her job. Employers are prohibited from interfering with an eligible employee's right to take the leave associated with that act. Under the FMLA, an "eligible" employee is one who has been employed for at least 12 months at the company, and who has worked a minimum of 1250 hours during the 12-month period immediately prior to the leave request.

The 7th U.S. Circuit Court of Appeals recently addressed a situation in which an employee's working hours fell just below the 1250 hour requirement. In that case, the court found that the 1250 hour hurdle was absolute, and that any lesser number of hours removed the employee from eligibility to assert a claim under the FMLA. *Pirant v. U.S. Postal Service*, No. 07-1055 (7th Cir. September 4, 2008).

Antoinette Pirant was hired in 1993 by the U.S. Postal Service (USPS) to work as a mail handler. In the years of her tenure with the USPS, Pirant was regularly disciplined for attendance policy violations. In fact, she was "terminated" four times, and on each of the four occasions was able to convince her supervisors to reduce the termination to a suspension.

Continued on Page 3  
RETURN TO TABLE OF CONTENTS PAGE 2

In March 2001, Pirant was put on a Last Chance Agreement that specifically stated that further attendance problems would lead to termination, and that this was her “absolute last chance” on the issue. When Pirant subsequently was absent without excuse, she received a notice of termination, and her last day of work was set for October 28. However, on October 26, Pirant convinced her supervisor to extend her final day until December 10.

On October 5, Pirant’s supervisor ordered her to clock out two hours early, based upon an incident of alleged insubordination. Pirant did so, but complained to a USPS Dispute Resolution Specialist (Andrews) that she had been wrongfully accused. She was informed of her right to file a formal grievance on the issue, but did not do so within the allotted time.

On December 6, Pirant was absent from work, and did not provide a medical reason other than she “had not been feeling well.” On December 10, Pirant went to an emergency room and was examined for carpal tunnel syndrome and for arthritis in her knee. She was directed by a doctor not to work from December 10 to December 17.

On January 4, Pirant’s employment was terminated for her violation of the Last Chance Agreement. She filed a federal court complaint, claiming that the USPS violated the FMLA when it terminated her for missing work, since at least one of her absences was related to her “arthritis knee.” In an initial response to that complaint, the USPS admitted that Pirant was qualified for FMLA coverage.

However, after checking the official time records, and in light of the two hours that Pirant did not work because of the suspension imposed on October 5, the USPS amended its answer to state that Pirant had worked only 1248.8 hours in the preceding 12 months, and therefore was not eligible for FMLA leave. The district court dismissed Pirant’s claim. The dismissal was upheld on appeal.

The Seventh Circuit held that there was no factual dispute regarding Pirant’s eligibility, since the official payroll records showed a less-than-1250 hour work history – although barely less. Although Pirant argued that she should have been credited with the two hours missed while suspended, she was unable to show that she had appealed that suspension. Therefore, those two hours were not counted toward the 1250 hour minimum. In addition, the court held that Pirant’s time spent “donning and doffing” her uniform was not “work time” under the Fair Labor Standards Act, as it was not integral to her job. Therefore, that additional time did not count toward the FMLA’s 1250 work hour requirement.

The USPS’ ability to offer formal documentation of Pirant’s exact work hours was the factor that led to its success in this case. Although the shortfall between Pirant’s hours worked and the hours required for FMLA eligibility was a de minimus amount of time, the court was unwilling to act outside of the statutory mandate of 1250 hours. This case is a clear example to employers of the importance of complete and accurate payroll and work-time records.

## Background Investigations Keep Getting More Complicated

By Jennifer Brown Shaw and Matthew J. Norfleet

Employers increasingly are relying on credit and background checks in the hiring process. Employers want assurances that their employees are honest and trustworthy. Internal investigations of certain misconduct allegations are now required by anti-discrimination laws

and others, such as Sarbanes-Oxley. At the same time, surveys show resume fraud is rampant. Job references often won’t provide information about former employees other than “name, rank and serial number.” With a bad economy, huge student loan liabilities, and the mortgage crisis, potential employees may appear to be untrustworthy with credit.

Specific federal and state laws govern how employers may use credit and background reports prepared by third-party vendors. The California Legislature has sent to the Governor’s desk Assembly Bill 2918, a new law further limiting employers’ ability to use such information. It is unknown whether the governor will sign AB 2918, which would prohibit employers from relying on background checks performed by third parties, except in limited

Continued on Page 4

RETURN TO TABLE OF CONTENTS PAGE 3



circumstances.

Employers may wish to conduct their own research into employee backgrounds. Public records are more “public” than they were even 20 years ago. The internet has made it easy to obtain information that used to be available only in dusty courthouse basements. Additionally, employees provide a great deal of information about themselves to perfect strangers on social networking sites. When employers do their own research on employees’ backgrounds, they are subject to other laws, some of which may not be obvious.

### **What’s on the Horizon?**

Most employers are not required to perform credit or background checks on their applicants or employees. The law generally allows employers to choose to perform checks for evaluating applicants, selecting employees for promotion, and deciding whether to retain an employee.

In certain circumstances, federal, state, and local governments require criminal and other background checks as part of the application or licensing process. The 1993 National Child Protection Act authorizes states to create regulations to access the FBI’s National Crime Information Center (NCIC) for background checks for employees and volunteers who work with children, the elderly, and persons with disabilities. The California Attorney General manages access for law enforcement agencies, public and private schools, non-profit organizations, and in-home supportive care agencies. Authorized “applicant agencies” can access NCIC criminal background checks, but must not disclose criminal record history information. Release of information to unauthorized individuals can result in civil fines and a misdemeanor conviction.

Some employers, such as schools, must conduct background checks of all employees. Other organizations may choose whether to use NCIC background checks. Proposed Assembly Bill 2888 would require all organizations with employees, independent contractors, or volunteers who work directly and unaccompanied with minor children to conduct criminal background checks. Also, hiring a registered sex offender to work unaccompanied with minors would carry a civil penalty of \$10,000. Critics of the proposed law complain that it is not specific enough and unnecessary as long as the California Department of Justice provides NCIC information to employers whose employees work with children.

At the same time as the Legislature expands the obligation to conduct background checks, it is working to curtail permissible purposes for doing so. If signed, AB 2918 would prohibit employers from obtaining “credit” reports regarding employees unless it is “substantially job related,” required by another law, or obtained by an employer subject to “oversight” under the Fair Credit Reporting Act (such as certain banks). “Substantially job related” would be limited to credit checks obtained about applicants for “highly compensated,” managerial, or certain local government jobs. If the Governor approves the bill, it will prohibit employers from obtaining credit checks for employees handling cash or inventory.

### **Background Checks by Third Parties**

The federal Fair Credit Reporting Act applies to most credit and background checks conducted by third parties for employment purposes. California has similar laws, maintained in the Civil Code at sections 1785.1-36 for credit reports, and 1786-1786.60 for investigative consumer reports.

The laws cover “consumer reports,” which include not only credit checks but also criminal record history, verification of education, and personal interviews of friends and neighbors. These laws also control the use and procurement of “investigative consumer reports,” which are based on an “interview” that goes beyond simply verifying facts and dates. The Federal Trade Commission (FTC), which enforces the FCRA, considers investigative consumer reports “particularly invasive of a consumer’s privacy.”

Under existing law, employers generally are free to conduct background checks for covered purposes so long as they disclose their intent to do so, provide sufficient information under the law, obtain written consent, and provide sufficient information to applicants denied employment based on the results of the report.

A California employer that uses a third-party background investigator must explain the scope of the report requested, provide contact information for the investigator, explain the rights to see and copy any report, and allow the subject to receive a copy of any report. An applicant who requests a report must receive a copy within three days of receipt by the employer.

Under the FCRA, before any adverse action is taken based upon information in the report, the employer must provide the applicant or employee a copy of the report and the summary of consumer rights prescribed by the FTC. After an adverse action is actually taken, the employer also must provide an adverse action notice and a summary of rights under the FCRA. Complying with these requirements is a function that responsible investigative consumer reporting agencies can do for the employer.

### **Background Checks Conducted by Employers**

Employers that choose to conduct their own background checks are not subject to many of the requirements contained in the FCRA and the Civil Code. In California, for example, “investigative consumer reporting agencies” may not provide information about arrests, indictments, convictions, civil judgments, or tax liens that are more than seven years old unless state or federal law specifically requires the employer to check records for a longer period of time. However, employers are not limited from obtaining the same information in their own investigations. As a practical matter, of course, few employers are prepared to conduct that kind of thorough search without the assistance of an agency. Employers also cannot obtain a credit report without using a third party.

An employer that conducts its own investigation must notify the applicant or employee and, generally, must provide copies of any public records it receives within seven days of receipt. “Public records” include criminal files available to the public. However, if the investigation is ongoing, the employer may wait until its conclusion.

### **Internet Research**

At present, there are few restrictions on employers that merely search the internet for posted information about an applicant or employee. However, one potential information source available to any member of the public – the Megan’s Law website – is completely off-limits to employers. Megan’s Law created a database and public websites for members of the public to check on the whereabouts of registered sex offenders. The law and website are administered by the Attorney General. There is an express warning that the information on the site may not be used by employers to determine an employee’s fitness for duty. Ironically, employers are free to deny employment based on the conviction of the crimes themselves. Megan’s Law simply prohibits employers from relying on the website to obtain the information about the convictions.

Employers also may be tempted to search social networking databases such as “MySpace,” “Facebook,” and the like. Information available to the public is fair game to view. But employers nevertheless should not make decisions based on illegal criteria revealed on public websites, such as political beliefs, sexual orientation, or religion. Moreover, employers should not use trickery to obtain passwords to private web pages. Doing so could result in an applicant or employee successfully claiming an intrusion into privacy.

### **Conclusion**

Employers and the public have legitimate reasons to require the investigation of applicants’ and employees’ backgrounds. In some cases, the law requires careful vetting of applicants and employees exposed to children, confidential information, and other valuable or sensitive information or property. Other employers choose to implement background checks even though they are not required to do so. These employers must carefully follow the detailed procedures imposed upon them, and ensure the information obtained during the process is not misused.

---

## **California Bans “Texting” Behind the Wheel; California Employers Should Update Personnel Policies**

California has banned text messaging while driving, and employers need to respond promptly by updating policies.

SB28, signed by Governor Schwarzenegger on September 24, 2008, amends the California Vehicle Code to state: “A person shall not drive a motor vehicle while using an electronic wireless communications device to write, send, or read a text-based communication.”

As the governor sorted through 800 bills on his desk, he

said he was “happy” to sign this one. “Banning electronic text messaging while driving will keep drivers’ hands on the wheel and their eyes on the road, making our roadways a safer place for all Californians.”

What about fumbling with your PDA’s phone directory to dial out a call? That doesn’t count as texting under the new law: “For purposes of this section, a person shall not be deemed to be writing, reading, or sending a text-based communication if the person reads, selects, or enters a telephone number or name in an electronic wireless communications device for the purpose of making or receiving a telephone call.”

The penalty for violating the law is \$20 for the first violation and \$50 for subsequent violations. No violation points will be given as a result of the offense.

The new law closes a loophole left by Senate Bill 1613. Effective July 1, 2008, that new law provides that it is illegal to drive a motor vehicle while using a wireless telephone, unless a hands-free device for the cell phone is used. But the law did not expressly ban texting. (Separate legislation has already banned drivers under age 18 from using cell phones or any texting device while driving.)

California joins Alaska, Minnesota, New Jersey, Louisiana, Washington and the District of Columbia, where legislators have also recently enacted laws that ban sending text messages while driving. At least a dozen other states are currently considering such a ban.

Texting while driving is a frighteningly common occurrence, especially among younger drivers. According to a survey conducted by Findlaw.com, 47 percent of drivers between the ages of 18 and 24, and more than a quarter (27 percent) of drivers 25 to 34, admit to texting while behind the wheel. Seventeen percent of adults surveyed say they have texted while driving.

Studies suggest that texting while driving is more dangerous than driving while under the influence of alcohol or drugs.

The California Highway Patrol reports that statewide last year, 1,091 crashes with 447 injuries were blamed on drivers using cell phones. In accident cases, lawyers may argue that an employer is liable where an off-duty employee makes or answers a business-related call, or sends a business text message while driving.

Have you updated your employee handbooks? In order to minimize liability issues arising from employees using cell phones, PDAs, or other electronic communication devices on the road while in the course and scope of employment or while taking work-related calls, employers should implement a policy that requires all employees to refrain from texting and to use “hands free” devices while driving on company business or when making business calls on the road. Better yet, employees could be prohibited from using cell phones or PDAs while driving.

Submitted by:

Christopher W. Olmsted, Esq.

Barker, Olmsted & Barnier, APLC



**Gauntlet Awards** 1-800-541-2955  
Crystal Awards, Acrylic Awards, Clocks, Plaques, Trophies, Pet I.D. Tags, Corporate Logo Apparel, Thank You Gifts, Holiday Gifts and Much More!  
**WWW.GAUNTLETAWARDS.COM**

## Disability Act Amendments to Take Effect January 1, 2009

Both houses of Congress have approved the ADA Amendments Act (ADAAA), which will expand the definition of disability and overturn Supreme Court decisions that had made it more difficult for employees

**Continued on Page 7**

**RETURN TO TABLE OF CONTENTS PAGE 6**

to gain protected status under the Americans with Disabilities Act (ADA). The ADAAA, which President Bush has said he will sign, will become effective January 1, 2009.

The ADAAA preserves the basic framework of who is considered “disabled” and therefore protected under the ADA, but expands the meaning of terms used within that definition. The term “disability” continues to mean: (A) a physical or mental impairment that substantially limits one or more “major life activities” of such individual, (B) a record of such impairment, or (C) being regarded as having such an impairment. The ADAAA expands the scope of covered individuals by adding a definition of “major life activities” that is more inclusive than the interpretation federal courts had given that phrase.

By statute, the definition of major life activities will now include “caring for oneself, performing manual tasks, seeing, hearing, eating, sleeping, walking, standing, lifting, bending, speaking, breathing, learning, reading, concentrating, thinking, communicating, and working.” This list is illustrative, not exhaustive. Major life activities are also expanded to include “major bodily functions,” including but not limited to “functions of the immune system, normal cell growth, digestive, bowel, bladder, neurological, brain, respiratory, circulatory, endocrine, and reproductive functions.”

The effect of this expanded definition is significant. With this change, employees will likely be considered “disabled” if they have, for example, insomnia (impaired in the major life activity of sleeping), dyslexia (learning), stuttering (speaking), and attention deficit disorder (concentrating). Bending and lifting are now deemed major life activities as well. Individuals with digestive diseases or incontinence are now covered, if their impairment substantially limits them in these areas. The reference to “reproductive functions” may mean that employees undergoing infertility treatments are covered. Note that the major life activity affected need not have any relationship to working.

Before these changes, the ADA did not define “major life activities.” Interpretive guidelines set forth by the EEOC had provided some examples but the guidelines were less authoritative than the statute itself and were less expansive in scope than the new ADAAA definition. Courts had been left to interpret the phrase without a clear statutory definition and issued decisions that interpreted the term

too narrowly, according to findings set forth by Congress in the enacted bill. The new definition of “major life activities” overturns the narrower interpretation by the Supreme Court in *Toyota Motor Manufacturing, Kentucky, Inc. v. Williams*, 534 U.S. 184 (2002).

These changes do not mean that every impairment that has any effect on these functions automatically qualifies as a disability, and an impairment must still “substantially limit” a major life activity to qualify. However, Congress has conveyed its intent that the phrase “substantially limits” should be interpreted less strictly, and has instructed the EEOC to issue interpretive guidelines consistent with this intent. The more liberal interpretation of this phrase will also overturn portions of the *Williams* Supreme Court case which, according to language in the bill, “created an inappropriately high level of limitation necessary to obtain coverage under the ADA.”

The ADAAA will also require that the determination as to whether someone is disabled be made without considering mitigating measures. Thus, a person whose condition is controlled by medication, prosthetics, hearing aids, assistive technology, or other medical equipment or aids can no longer be excluded from the definition of disabled because of these mitigating measures. Rather, if a person’s condition would qualify as a disability without these aids, the person is considered disabled. This change overturns the Supreme Court’s decision in *Sutton v. United Air Lines, Inc.*, 527 U.S. 471 (1999).

The ADAAA provides an exception, however, where ordinary eyeglasses or contact lenses are used to correct poor vision. Poor vision that is corrected through ordinary eyeglasses or contact lenses is not a disability. This exception to the requirement that mitigating measures be ignored is limited to vision. It does not extend, for example, to hearing impairments, even where a hearing aid is used. Therefore, a person whose poor vision is corrected by eyeglasses is not disabled, but a person whose poor hearing is corrected by a hearing aid may be disabled.

Consistent with its special treatment of corrective lenses, the ADAAA prohibits any employment test or qualification standard that tests applicants based on their uncorrected vision, unless a certain level of uncorrected vision is required by the job and is a business necessity. In most instances, therefore, applicants required to take a

vision test must be permitted to use corrective lenses.

Other important clarifications to the ADA include the following:

- Individuals whose disability is in remission or is episodic are still considered disabled if the condition would qualify as a disability when active.
- The “regarded as” portion of the definition of disability does not apply to impairments that are “transitory and minor,” which is defined to mean “an actual or expected duration of 6 months or less.” This 6-month limitation applies only to the “regarded as” portion of the definition. There is no 6-month limitation applicable to individuals who actually have a disability.
- No claim of “reverse disability discrimination” may be made by a non-disabled person.
- These changes apply to definition of disability used in the Rehabilitation Act as well. The Rehabilitation Act is a sister statute to the ADA, prohibiting discrimination on the basis of disability in programs conducted by federal agencies, in programs receiving federal

financial assistance, in federal employment, and in the employment practices of federal contractors.

While the changes enacted in the ADAAA undoubtedly expand the scope of individuals covered by the ADA, they do not limit employers’ ability to raise defenses, including defenses as to whether a requested accommodation is reasonable. Because of the expanded scope of coverage, however, the ADAAA may result in the defense of ADA cases becoming more difficult and expensive.

If you have any questions, please contact any member of our Employment & Labor Practice Team.

Baker & Hostetler LLP publications are intended to inform our clients and other friends of the Firm about current legal developments of general interest. They should not be construed as legal advice, and readers should not act upon the information contained in these publications without professional counsel. The hiring of a lawyer is an important decision that should not be based solely upon advertisements. Before you decide, ask us to send you written information about our qualifications and experience.

[Florida Rule 4-7.2(d)] © 2008 Baker & Hostetler LLP

## **Massachusetts Data Security Regulations Effective 2009**

The Massachusetts Office of Consumer Affairs and Business Regulation has issued final data security regulations pursuant to the comprehensive data security law signed by Governor Deval Patrick on August 3, 2007. The regulations establish minimum standards for protecting and storing personal information about Massachusetts residents contained in paper or electronic format. The regulations apply to any businesses or individuals that own, license, store or maintain personal information about a Massachusetts resident. Therefore, they may even cover businesses or individuals having no presence in Massachusetts, as long as these entities possess the personal information of any Massachusetts resident. The regulations become effective on January 1, 2009.

General Requirements. Covered persons and entities must develop, implement, maintain and monitor a comprehensive information security program applicable to any records containing personal information. The

program must:

- (i) be in writing,
- (ii) be reasonably consistent with industry standards, and
- (iii) include administrative, technical, and physical safeguards.

Thus, addressing the data security requirement solely from an IT perspective will be insufficient to comply with these regulations.

While certain safeguards may be necessary and appropriate for any comprehensive program, the regulations list safeguards that must be a part of any comprehensive information security program. Covered persons or entities must:

- Designate one or more employees to maintain the program.
- Conduct risk assessments to gauge risks to the security,

confidentiality, and/or integrity of any electronic, paper or other records containing personal information. This must be followed by evaluating and improving the effectiveness of safeguards. The regulations include temporary and contract employees in the training requirements.

- Develop security policies concerning whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- Discipline employees for program violations.
- Ensure terminated employees no longer have access to personal information.
- Verify through reasonable efforts that outside vendors with access to personal information have the capacity to protect that information. The regulations require that before providing a vendor access to personal information, the covered person or entity must obtain a written certification that the vendor has a compliant comprehensive information security program.
- Collect, retain and provide access to personal information only to the extent it is reasonably necessary to accomplish the legitimate purpose for which it is collected, retained or accessed, or as is necessary to comply with state or federal record retention requirements.
- Unless a covered person or entity protects all records under a comprehensive information security program as if they contain personal information, it must identify paper, electronic and other records, computing systems, and storage media that contain personal information.
- Impose reasonable restrictions on physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted.
- Monitor the program to ensure it is operating as intended and make adjustments as necessary and appropriate.

- Assess the scope of the entity's safeguards at least once a year or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- Document steps taken to respond to a security breach and any changes in safeguards resulting from a review of the breach incident.

Specific Program Requirements for Electronically Stored or Transmitted Personal Information. Every covered person or entity that electronically stores or transmits personal information also must establish and maintain a security system covering its computers, including any wireless systems. The security system must be a part of the written, comprehensive information security program. Among other things, the system must implement protocols to authenticate users and restrict access. To the extent feasible, records containing personal information that is transmitted across public networks and wirelessly must be encrypted. All personal information stored on laptops and portable devices must be encrypted.

Complete and Timely Compliance. The regulations seem to contemplate and permit covered persons or entities to design an information security program that is appropriate to their particular circumstances. That is, when evaluating whether a particular program complies with the Massachusetts data security regulations, the following may be taken into account:

- size, scope and type of business obligated to safeguard the personal information,
- resources available to the person or entity,
- amount of stored data, and
- need for security and confidentiality of both consumer and employee information.

The January 1, 2009, effective date imposes a short time frame for businesses to become compliant, particularly those that have significant amounts of personal information internally or maintained by vendors. While this measure may be good news for Massachusetts residents, the law significantly increases covered entities' obligations to safeguard personal information and their

exposure for a failure to do so. These regulations follow a nationwide trend — a number of other states, including California, Texas, New York, Oregon, and Maryland, have enacted similar measures. State regulations and the vast amount of employee and other personal information businesses own and maintain compel the need to develop comprehensive data security programs. Jackson Lewis attorneys are available to answer your questions about these new regulations and assist in developing your data security program.

This article is provided for informational purposes only. It is not intended as legal advice nor does it create an attorney/client relationship between Jackson Lewis LLP and any readers or recipients. Readers should consult counsel of their own choosing to discuss how these matters relate to their individual circumstances. Reproduction in whole or in part is prohibited without the express written consent of Jackson Lewis LLP. Jackson Lewis LLP represents management exclusively in workplace law and related litigation. Our attorneys are available to assist employers in their compliance efforts and to represent employers in matters before state and federal courts and administrative agencies. For more information, please contact the attorney(s) listed above or the Jackson Lewis attorney with whom you regularly work.

---

## **Nabbing Workplace Thieves**

By Carol Coultas , Business Writer

LEWISTON - In hindsight, there were red flags.

For Chip Morrison, president of the local Chamber of Commerce, it was an employee's personal financial troubles. For accountant Tom Robustelli, it was a client's reluctance to provide timely documents.

Both men shared their personal experiences with employee fraud and theft at a seminar at chamber offices Thursday. The problem, which analysts estimate costs American business \$40 billion a year, is remarkably common, said Morrison.

"After our issue with this topic, we had over 100 members call or e-mail and say 'It happened to us, too,'" said Morrison. "That's 10 percent of our membership. Don't feel like it can't happen to you."

The presentation fulfilled a promise Morrison made to members last year after a chamber employee was fired for allegedly stealing \$17,000 from the organization. Rather than hide the incident, Morrison and his board decided to use the experience to teach others about the problem.

"It is so rampant and common that I'm guessing at least half the people in this room are affected," Morrison told the crowd of about 25, many of whom nodded their heads in agreement.

Two essential ingredients leading to employee theft are need and opportunity. Morrison said he knew his

employee was in trouble when he started to field calls from creditors, but he never thought she'd steal to fix things. The situation was exacerbated by the chamber's capital campaign to move into its new building, which meant much more money was moving around the organization's books than normal.

Robustelli, a certified public accountant with Robustelli Rotz & Soucy, said he learned a valuable lesson after performing a routine audit on a nonprofit organization that had been his client for 10 years. He said he wasn't suspicious until he began asking the bookkeeper for canceled checks to reconcile with the bank statements.

"She said the treasurer had them," said Robustelli, whose multiple requests were stonewalled until he contacted the treasurer and bank directly. He discovered a 3-year fraud by the bookkeeper that netted her \$260,000.

"It was all there," said Robustelli. "She'd written a check to herself for \$20,000 the day before I began my field work."

Luckily for businesses, new laws in the wake of the Enron and Worldcom scandals have ramped up the intensity of audits. But it's still the responsibility of management to uncover fraud, said Robustelli. The easiest thing to do is prevent it in the first place, and that's possible with internal controls.

"The first thing to do, is set a tone in the organization," said Robustelli. "Make it a controlled environment."

He suggests: competent bookkeeping, a workplace

**Continued on Page 11**

**RETURN TO TABLE OF CONTENTS PAGE 10**

emphasis on honesty and integrity, knowing the boss is paying attention. The situation with the ripped-off nonprofit was made worse by an executive director who focused on the group's mission and was hands-off on managing the money, he said.

Robustelli also suggested people think like a thief to identify where the company is vulnerable. Procedures that provide good checks and balances - the employee who prepares the bank deposit shouldn't be the one to post customer accounts - offers protection, as do things like outsourcing payroll and installing surveillance cameras.

Lewiston police Detective Lee Jones, who investigates white collar crimes, said digital or video tape has been instrumental in prosecuting employee theft cases. He, too, presented at the chamber seminar, adding his voice to those who say they see a rise in workplace fraud.

"People that handle money do steal," he said, encouraging extensive background checks before someone is hired. "I try to prosecute 100 percent of the time."

In Robustelli's example, the thief was sentenced to nine years. The chamber case is still pending, but Morrison said the \$17,000 was restored through its insurance company, which is seeking restitution from the former employee.

Besides the legal and financial fallout, the emotional toll can be severe, as well. Robustelli said he was so angry - at himself, at the board, at the fraudster - that he donated \$12,000 in services to the nonprofit "to make it right." Morrison said every employee at the chamber felt violated by their co-worker's deceit.

"Other people are affected mightily," he said, noting that everyone went to voluntary counseling. "Some are still working out their anger."

---

## **OFCCP Issues New Form I-9 Inspection Procedures**

The Department of Labor's Office of Federal Contract Compliance Programs (OFCCP) issued a directive on October 2, 2008, effective immediately, regarding inspection procedures for an OFCCP compliance officer (CO) when reviewing Forms I-9 during an on-site compliance review.

The impetus for the new directive is the U.S. Citizenship and Immigration Services' revision last year of Form I-9, and President Bush's recent Executive Order requiring federal contractors to use an electronic verification system to confirm the employment eligibility of new hires and current employees working on the new federal contract. E-Verify, a web-based system currently operated jointly by the Department of Homeland Security Citizenship and Immigration Services (CIS) and the Social Security Administration (SSA), has been designated as the authorized electronic verification system until March 6, 2009.

The new OFCCP inspection procedures include these requirements: 1) federal contractors must use the new Form I-9 (Rev. 06/05/07) for all employees hired, rehired, or re-verified after November 7, 2007; 2) the

CO must ensure that any electronically reproduced or retrieved Form I-9 is legible and that there is no evidence of inserts or changes to the name, content, or sequence of the data elements; 3) the CO may request that the federal contractor retrieve and reproduce electronically stored Form I-9 and supporting documentation and associated audit trails showing who had access to the electronic system and activity within the system during a given period of time; 4) the CO may request that the federal contractor provide hardware and software, personnel and documentation necessary to retrieve, read and reproduce electronically stored I-9 forms and any supporting documents, associated audit trails, reports, and other data used to maintain authenticity, integrity and reliability of the records; and 5) federal contractors must provide, if asked, reasonably available electronic summary files (e.g., spreadsheets) containing all information electronically stored and the CO may use that summary to select certain Form I-9 for inspection.

The DHS has not yet issued regulations for the new Executive Order, but is authorized to do so. The OFCCP may revise its Form I-9 inspection procedures once the DHS issues implementing regulations. The Federal Acquisition Regulation Counsel (FARC) has not yet issued a final rule to implement the Executive Order, but comments to FARC's proposed rule closed on August 11, 2008.

**RETURN TO TABLE OF CONTENTS PAGE 11**

Steven E. Gall, President  
Gall & Gall Company, Inc.  
*The Information Source*



Contact Information:

Phone: 937-264-4900

Fax: 937-264-4903

[sgall@gallgall.com](mailto:sgall@gallgall.com)

### **Human Resource Management & Employment Law**

Prior to entering the private sector, Steven worked in law enforcement and personnel administration for over twenty-seven years. He has dealt with employers and assisted them in resolving a wide variety of personnel problems and issues. Steven provides instruction and consulting to many Associations and Companies annually. His programs focus on all areas of HR Management.

Steven has conducted training sessions for Miami Valley Human Resource Association, Kentucky State Chapter of the Society of Human Resource Association, The National Apartment Association, The Florida State Apartment Association, The United States Department on Senior Care & Aging, The Cooperative State Research, Education, and Extension Service (CSREES) an agency within the U.S. Department of Agriculture as well as many other Associations and Companies Nationally. One of his areas of expertise is Employment Law, The Fair Credit Reporting Act, and Due Diligence in Employment Background Screening, Workplace Violence and other areas of Human Resources. Steven also speaks on Technology in today's workplace, "The Good, The Bad & The Ugly."

### **Professional Associations and Community Leadership Activities:**

- SHRM Society of Human Resource Management – Professional Membership
- SHRM Ohio State Council – State District Director – West Central Ohio
- SHRM Chapter Miami Valley Human Resource Association, – Past President, Technology Director
- Miami Valley Military Affairs Association – Past President, Technology Director, Membership Chair
- Dayton Area Chamber of Commerce
- Huber Heights Chamber of Commerce
- Main Street Piqua
- Piqua Area Chamber of Commerce
- Tipp City Area Chamber of Commerce
- Trotwood Chamber of Commerce
- Troy Area Chamber of Commerce
- Vandalia-Butler Chamber of Commerce



Social Security Number Report, Employment Credit Report, County Criminal Records, Employment Reference Report, Drivers' License Record Search, Educational Credentials, Professional Certifications Reports, National Criminal Records, Statewide Criminal Records, US Patriot Act Search, Multi-state Sexual Predator and Violent Offender Search, Drug and Alcohol Screening and more!

[www.gallgall.com](http://www.gallgall.com) 1-800-759-4255