

# Managing Risk

THE  
**ENCORE**  
RISK  
MANAGEMENT  
GROUP INC

*More than a Policy  
— A Partnership!*

**MEDIA**  
PLUS  
INSURANCE  
SERVICES

Post Office Box 36219 Birmingham, AL 35236  
Toll Free: 888.204.4364 or Fax: 205.444.3035  
www.mediaplusins.com



Risk Management

Fall 2008

Volume 18 • Number 4

## What Smart Insurance Buyers Need to Know

In tough economic times, you want your money to go as far as possible, including on your business insurance. Here are some pointers to help you get the best possible coverage at the best price.

**Brokers vs. agents.** In some ways, buying insurance is like buying a car. When you need a new car, you don't go to Detroit: you go to a dealer, who acts as an intermediary to help you get the car you want. Insurance agents and brokers also act as middlemen to help consumers navigate the insurance-buying transaction.

Both agents and brokers are licensed by the state; however,

(in most states) they have different roles. Agents are employees of an insurer and (in most cases) offer only the products of that particular insurer. Examples of agency companies are State Farm and Farmer's. A State Farm agent, for example, will sell you State Farm products. A broker, on the other hand, can offer products of many insurers. Brokers who are "appointed" by an insurance company can market that company's products. Brokers usually

also have access to products of other insurers through managing general agents and other sources, giving you a wider variety of options in coverage features and price.

**Marketing.** One of the most important services a broker provides is marketing your business to insurance carriers. This involves selecting from hundreds of insurers the several that will most likely provide the coverage you need at a reasonable price. Your broker will then work with underwriters at those carriers to get quotes on your business. During a "hard market," when demand for coverage exceeds availability (as after 9/11), you might not be able to get all the coverage you need from a single carrier, so your broker will attempt to "layer" coverage. During a "soft market," your broker will look for those insurers who balance available capacity and good pricing with good underwriting practices to ensure the carrier's future solvency.

### This Just In

**I**T professionals say smart phones are more likely to cause security breaches than laptops, according to a survey by Credant Technologies. As cell phones get "smarter," they appeal to more knowledge workers, who like their portability. However, that portability also makes a smart phone easier to lose than a laptop. If your employees use PDAs for work, caution them to use their password-protection features to protect valuable data.

**C**ompanies can reap significant benefits by identifying and effectively treating depressed workers, according to a recent study published in the *Journal of the American Medical Association*. The study, funded by the National Institute of Mental Health, found that such programs yield advantages in hiring, training, productivity and salary costs that far outweigh the cost of outreach and treatment. The researchers estimated the cost of the program at \$100 to \$400 per worker, while the productivity boost from more hours worked yielded \$1,800 per employee.



BUYERS—continued on Page 3



# Driving the Road to Safety

A 2003 study by the National Highway and Transport Safety Administration found that the average car crash costs an employer \$16,500. When a worker has an on-the-job crash that results in an injury, it costs the employer an average of \$74,000. Costs can exceed \$500,000 when a fatality occurs. And unfortunately, occupational vehicle accidents account for one of every four worker fatalities nationwide, according to the National Bureau of Labor Statistics.

**E**very company is exposed to the dangers of unsafe driving – even if only in the commuter trips its employees make. However, numerous strategies and programs can significantly improve driver safety for all your employees, from the harried delivery driver to the casual commuter. According to recent survey, driver safety programs provide a return on investment of at least 3 to 1.

One of the most widely used programs is run by an alliance of OSHA (the U.S. Occupational Safety and Health Administration), the NHTSA (National Highway Traffic Safety Administration) and NETS, the Network of Employers for Traffic Safety. The program's participants include transport giants such as UPS and Amerifleet, as well as GM and An-

heuser-Busch. "Our affiliations with NETS is invaluable. At UPS, we put nearly 87,000 drivers on the road every day. NETS helps us to stay current on important traffic safety issues," says Charles Halfen, corporate fleet safety manager, UPS.

## The NETS Ten Step Program

- 1 Senior Management Commitment and Employee Involvement** – The involvement of top-level managers and employee representatives underscores the importance of traffic safety.
- 2 Written Policies and Procedures** – A clear and enforceable set of traffic safety policies is the cornerstone of the education effort. They should be disseminated widely and encouraged with incentives.

- 3 Driver Agreements** – Adherence contracts should be signed by all employees who drive for work purposes, whether in company cars or their own vehicles.
- 4 Motor Vehicle Record (MVR) Checks** – Companies must screen out poor drivers before they cause accidents. Check driving records prior to assigning driving duties and periodically thereafter.
- 5 Crash Reporting and Investigation** – All crashes – even minor ones – must be reported. Establish guidelines of how to behave in the aftermath of a crash and thoroughly investigate the cause of each accident with the goal of eliminating future occurrences.
- 6 Vehicle Selection, Maintenance and Inspection** – Make the passive and active safety features of vehicles key criteria when purchasing company vehicles. Whenever possible, choose best in class vehicles. Schedule regular maintenance and safety checks. If private vehicles are used for company business, encourage employees to adopt the same policies.
- 7 Disciplinary Action System** – The company should have a clear policy to punish and deter dangerous drivers by assigning points after a moving violation or preventable crash. The system should adopt a progressive discipline approach if a driver begins to develop a pattern of incidents. Define the number of violations an employee/driver can have before losing the privilege of driving for work.
- 8 Reward/Incentive Program** – Safe driving contributes directly to your bottom line. Recognize it with prizes, awards and incentives.





**BUYERS**—continued from Page 1

**Risk analysis.** Your broker needs to know your likely risk exposures to know what types and amounts of coverage you will need. A broker experienced with your type of business can analyze your risks using tools such as inspections, checklists and surveys to compare your firm's risks to industry benchmarks. He/she will then estimate possible frequency and severity of those risks. Cooperating to provide your broker with all the information he/she needs to make a complete risk submission will help ensure you get the best possible insurance program. This can include payroll (for workers' compensation), claims history, lawsuits filed or threatened, situations (injuries and the like) that could lead to lawsuits, regulatory compliance programs, regulatory actions against your company, loss control procedures, disaster response plan, copies of your annual report (if publicly traded) and marketing/product information brochures.

**Insurer ratings.** Although pricing is important, you want to be sure your carrier will be able to pay your claims. Various companies rate insurers' solvency and claims-paying ability, including Best's, Standard & Poor's, Moody's and Fitch Ratings. Your broker will consider an insurer's ratings as well as its policy terms and pricing in making recommendations.

**Insurer services.** Brokers know which extra services carriers provide for their policyholders. These can include loss engineering services, legal services and more. Ask your broker which carriers might specialize in providing these services for firms like yours.

**Specialty markets.** Sometimes "standard" carriers will not write coverage for certain types of business that present unusual or large risks. A good broker knows and has access to the specialty markets that cover your industry. Often, "admitted" insurers (those licensed to do business in your state) will not

write these types of risks, so your broker will have to go to the surplus lines (or nonadmitted) market.

**Broker claim services.** A good broker's service does not end after the sale. Brokers can help their clients file claims and negotiate with the carrier on their behalf. Look for a broker with the systems and staff to help you handle claims. A broker might also help you develop a crisis management plan after a catastrophic loss.

**Communications.** Your broker should keep you informed of news that affects your insurance program on a regular basis. He/she should also check in with you on a regular basis, not just at renewal time, to see if your operations have changed in a way that might affect your coverage needs.

For more information on how we can help you negotiate the tricky world of insurance coverage, please call us. ■

**PRIVACY**—continued from Page 4

information about other employees? Do you include this requirement in all job descriptions for employees handling personal information? (yes)

- ✓ Do you train customer service, IT and other staff who have access to customers' personal information (particularly credit card numbers) not to disclose this information? Do you make this a condition of employment? (yes)
- ✓ Do you do background checks on any employee who will have access to others' personal information? (yes)
- ✓ Do you use employee Social Security numbers as ID numbers? Do you print Social Security numbers on paychecks? (no)

**Laws catching up on privacy issues**

HIPAA, the Health Insurance Portability and Accountability Act, has required health insurers and providers to protect the privacy of individuals' health information for several

years. California, which often leads the nation in areas of consumer rights, has several privacy protection laws. Of most interest to our audience are SB 1633 and AB 1950.

SB 1633 protects medical information by prohibiting businesses from trying to obtain medical information from an individual for marketing purposes without consent and without disclosing how it will use and share that information. AB 1950 protects individuals' personal information by requiring specified businesses to safeguard the personal information of California residents. The law defines "personal information" as name plus Social Security number, driver's license or state ID, or financial account number. It also requires businesses with access to this information to contractually require any third parties they do business with to protect this information.

Wise risk managers won't wait until privacy protection becomes law—inaction that causes a breach of privacy could potentially

cost you your good reputation and lost business. For more information on minimizing your company's privacy exposures, please call us. ■

**DRIVING**—continued from Page 2

- 9 **Driver Training/Communication** – Teach and remind drivers continuously about the importance of safety. Courses should cover such issues as securing materials for transport, using seat belts, limiting use of cell phones, the danger of alcohol and drug-impaired driving, driving while fatigued, aggressive driving, driving while under stress and the increased dangers facing young drivers.
- 10 **Regulatory Compliance** – Ensure compliance with highway safety regulations and clearly establish which, if any, local, state, and/or federal regulations govern your vehicles and/or drivers. For more information on driver safety programs, please contact us. ■



The information presented and conclusions within are based solely upon our best judgment and analysis. It is not guaranteed information and does not necessarily reflect all available data. Web addresses are current at time of publication but subject to change. This material may not be quoted or reproduced in any form without publisher's permission. All rights reserved. ©2008 Smart's Publishing. tel. 877-762-7877 • www.smartspublishing.com

Please recycle this newsletter



# Your Growing Privacy Exposures

As businesses store more information on computers and networks, their privacy exposures also grow. Just think about all the personal information you store on employees alone: Social Security numbers, addresses, names of spouses and dependents, and possibly even medical information. Then there are your customers—what information do you have on them? Names, addresses, credit card numbers and expiration dates? If any of this information falls into the wrong hands, whether through error or theft, you have a liability exposure.

Identity theft is only one part of this growing problem—but a significant one. In 2003, the Federal Trade Commission (FTC) logged 214,905 identity theft complaints. ID theft topped the FTC's list of consumer fraud complaints, accounting for 43 percent of the complaints lodged in the FTC's Consumer Sentinel database. The dollar loss consumers attributed to reported fraud grew from \$160 million in 2001 to \$343 million in 2002. Congress further estimates that identity theft costs American industry \$3.5 billion per year.

Identity theft occurs when someone uses an individual's personal identifying information—name, address, credit card or Social

Security number—without authorization to open new charge accounts, order merchandise or borrow money. When the bills pile up, the thief disappears. Victims of identity fraud lose money, their good reputation and their credit rating, which can hinder their ability to borrow money or find a job.

The FTC defines "identifying information" as "means of identification" in the federal criminal statute defining identity theft. Businesses that store any individuals' "means of identification" have an obligation to protect it. How vulnerable is your company to privacy-related exposures? The following questions will help you spot areas of vulnerability.



How secure are your documents containing personal information on employees? Compare your answers to the ideal to uncover potential problem areas.

- ✓ Are they in locked file cabinets? (yes)
- ✓ Are these cabinets in an office with a locking door, inaccessible to unauthorized persons? (yes)
- ✓ Do you store the key to these file cabinets in the top desk drawer? (no)
- ✓ Do you always shred any documents containing personal information before discarding? (yes)
- ✓ Do you train human resources, payroll and benefits staff not to disclose personal

*PRIVACY—continued on Page 3*

## GINA Adds to Employers' Compliance Burdens

GINA will make it an "unlawful employment practice" to take discriminatory employment actions against an individual because of genetic information. The Act specifically prohibits failing to hire or discharging an employee on the basis of genetic information. It also prohibits any employer or related entity from requesting, requiring or purchasing an employee's genetic information, unless they are using it (1) to comply with certification requirements of family and medical leave laws; (2) for monitoring the biological effects of toxic substances in the workplace; or (3) for DNA analysis for law enforcement purposes or for purposes of human remains identification, when the employer is a forensic lab.

The law also allows employers to request genetic information for health services, such as under a wellness program, when the employee provides prior written au-

thorization. In all instances, the employer must treat genetic information as confidential and maintain it in separate medical files.

Employees who believe an employer has used genetic information to discriminate against them may file a claim with the Equal Employment Opportunity Commission (EEOC). If the EEOC finds evidence of discrimination, it might file a lawsuit on behalf of the plaintiff in federal court or give the plaintiff a "right to sue" notice. If the employee prevails, possible damages include compensatory damages, back and front pay, and equitable relief.

For information on how GINA will affect your company's human resource administration, or for information on protecting employees' confidential genetic and other health information, please call us. ■