HEFFERNAN INSURANCE BROKERS
Because You're Different

News You Can Use

Nov. 2013 Volume 2, Issue 1

RISK MANAGEMENT

Forgiving Employee Theft May Void Coverage

IF YOU FORGIVE an employee who has stolen from your company and then that person steals again, you may be voiding any potential insurance recoveries.

That's according to speakers at a panel of risk management professionals at a recent insurance seminar. The problem of not being able to recover any losses through your fidelity coverage would typically stem from not reporting to your insurer the original instance of theft.

You may also void coverage if you suspect theft and do not conduct an internal investigation.

If the insurer, upon investigation, finds out that you forgave the employee and kept them on after the first instance of theft, it would likely argue that failure to report would void the coverage, according to the speakers – Andrew Kautz, national claims manager for Central Risk & Insurance Management Services Ltd. based in Vancouver, Canada; and Ross McGowan, a partner at Borden Ladner Gervais L.L.P., also based in Vancouver.

They pointed out that employees that steal, will typically not steal just once. If they get away with it the first time, they will likely steal more the next time around.

Prior dishonest acts generally terminate coverage if the insured knew about them.

An insurer's subsequent investigation after a theft report would focus mostly on coverage issues and whether the employee was responsible for other theft at the company.

Under the terms of their fidelity policies, employers have a duty to give timely notice to the insurer in writing after first discovering the loss.

The same would likely not hold true in the case of employee negligence that caused a loss and the employee tried to cover it up to keep their job. In such cases, the original loss may not be covered, but the subsequent losses (actual theft) might be covered.

You may also void coverage if you suspect fraud or theft, but do not investigate. ❖

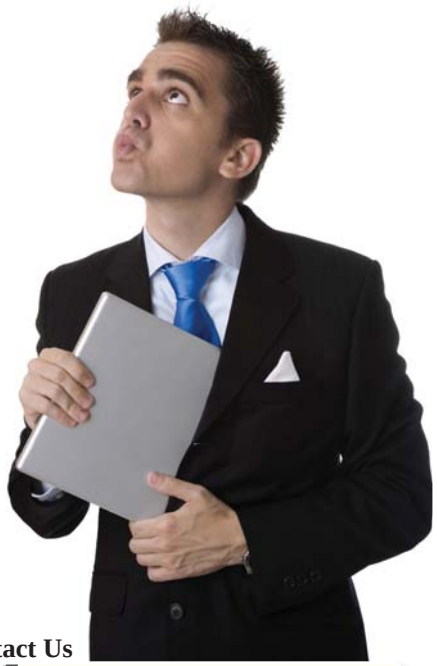
Take the right steps if you suspect theft

If you suspect employee theft, take the right steps to not only catch the thief, but also avoid wrongly accusing an employee (which could lead to a lawsuit for libel, slander or wrongful discharge).

The steps are:

- **Conduct an investigation to determine if an actual theft occurred.**
- **Figure out the extent of the theft and the methods used.**
- **If you discover a theft and can pinpoint the employee doing the stealing immediately, eliminate his or her access and/or remove him or her from the workplace.**
- **Try to recover the money or property.**
- **Take preventative actions to avoid theft from happening again.**

Remember, if the loss is very large and complex, you should immediately seek legal advice, which can assist you in evaluating the case and calling in additional experts, including forensic accountants and investigators.



Contact Us

HEFFERNAN INSURANCE BROKERS

If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek	Petaluma
San Francisco	Los Angeles
Menlo Park	Orange County
Portland	New York
St. Louis	

Sales: 877-731-7905
Service: 800-234-6787

Cal License No. 0564249

EMPLOYEE BENEFITS

FSA 'Use It or Lose It' Rule Partially Eliminated

THERE IS good newsfor your employees if you offer medical flexible spending accounts (FSAs), which allow them to put aside pretax funds to pay for medical-related expenses through the year: "Use it or lose it" has been partially eliminated.

The IRS and the Treasury Department have issued new regulations that will now allow employees to carry over up to $500 in unused account balances into the following year.

Up until now, any remaining funds in these accounts were forfeited at the end of the year if unused or, if the employer adopted one, at the end of a grace period that lasted up to 2½ months into the following plan year.

Under the grace period, unused account balances can be carried over and used to pay health care expenses incurred in the first 2½ months of the next plan year.

An FSA allows you to contribute money to the account for costs not covered by insurance: deductibles, copays and coinsurance. In addition, you can use your FSA to pay for health care costs that health insurance doesn't cover.

The "use it or lose it" caveat has always been a sticking point for some considering opting into an FSA, and the new regulations should increase participation.

The modification "cuts back on wasteful year-end FSA health care spending by limiting the risk of forfeiture and in turn reducing the incentive to spend down as year-end approaches in order to avoid the losing unused funds," the Treasury Department said.

The new regulations allow employers to choose either to allow employees to carry over up to $500 into the next year or offer a 2½ month grace period to spend the remaining account funds.

An estimated 14 million American families now participate in health care FSAs, according to the Treasury Department.

This year, employees can contribute a maximum of $2,500 per year to their FSA.

FSAs should not be confused with HSAs (health savings accounts), which are tax-advantaged medical savings accounts available to taxpayers who are enrolled in an HSA-qualified high-deductible health plan.

Funds contributed to an HSA are not subject to federal income tax at the time of deposit. Unused amounts in one year can be carried over to following years and added to subsequent contributions.

In order to qualify for an HSA, the policyholder must be enrolled in an HSA-qualified high deductible health plan (HDHP), and must not be covered by other non-HDHP health insurance or Medicare, and cannot be claimed as a dependent on someone else's tax return.

The annual contribution limit for HSAs is $3,330 this year for individuals, and $6,550 for family coverage.

There was no exemption until the Affordable Care Act, which bars reimbursement for over-the-counter medicines, with the exception of insulin, without a prescription. ❖

Bill Would Repeal Ban on FSA Spending on OTC Meds

NEW LEGISLATION introduced in the U.S. Senate seeks to repeal a controversial portion of the Affordable Care Act that bars employees from using their flexible spending accounts (to pay for non-prescription over-the-counter medications.

The ban caused a stir largely because many people opt for over-the-counter medications when they have common ailments, and particularly when the reason for the purchase is clearly medical-related.

The new bi-partisan legislation – S. 1647 – would again allow FSA funds to pay for over-the-counter medications such as allergy treatments and pain relievers.

The provision barring FSA funds for such use "takes away choice and flexibility from individuals about how to manage their health care expenses and adds yet another burden to physicians," Sen. Pat Roberts, (R-Kan), who introduced the legislation with Lousiana Democrat Mary Landrieu, said in a prepared statement.

"Rather than promoting cost-effectiveness and accessibility, this provision directs people to potentially more costly, less convenient and more time-consuming alternatives," he said. ❖

WORKPLACE SAFETY

Employers Fail to Report Worker Hospitalizations

A NEW STUDY based on Cal/OSHA targeted inspections has found "large-scale under-reporting" of hospitalization cases to the safety agency.

Cal/OSHA uses reports by employers of workplace injuries that result in hospitalization to initiate workplace inspections.

Rand Corp., which conducted the study for the Commission on Health and Safety and Workers' Compensation, found under-reporting mostly in Southern California, as well as in rural areas.

While the employers may not be reporting these injuries to Cal/OSHA as required by law (or suffer a penalty of up to $5,000), the study did not indicate whether they are also not reporting the injuries to their workers' comp carriers (which is also against the law).

Rand wrote in its report that the "failure to report appears to go undetected often. The Appeals Board is now more committed to levying the full [$5,000] penalty, but even that threat is probably unlikely to have a major effect in the absence of better methods of detection."

Rand made its conclusions based on the fact that employers in Southern California counties saw fewer accident-related inspections than their counterparts in the north of the state. While at first glance that would seem to indicate safer workplaces in the south, the ratio of accident investigations for fatal incidents per 1,000 workplaces was lower in Northern California.

"We are not treating this pattern as evidence that construction safety practices are better in the north or even that fatality rates are lower there," the working paper says. "However, these figures do provide very strong evidence that the quality of reporting of hospitalization cases ... varies greatly among counties and is lower in Southern California."

Rand found glaring discrepancies in reporting by employers to Cal/OSHA.

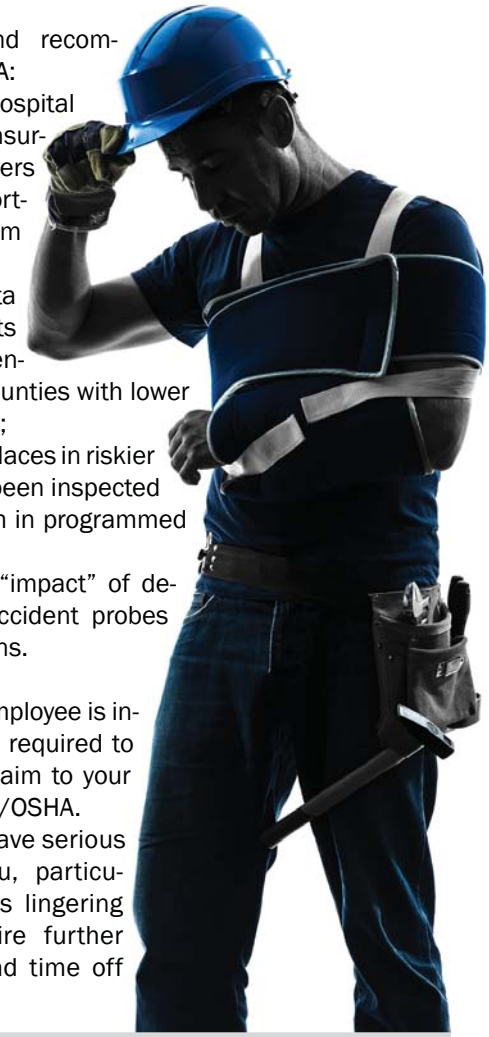
For example, while San Francisco had 10 non-fatal reportable cases to every fatality, a ratio "much closer to what most experts would expect," in Kings County in the Central Valley, the ratio was one non-fatal reportable case to three fatalities.

The takeaway

The study results could spur more aggressive policing by Cal/OSHA.

In its report Rand recommended that Cal/OSHA:

- Examine hospital bills submitted to insurers to detect employers that may not be reporting hospitalizations from workplace injuries.
- Maintain data on informal complaints and better serve potential complainants in counties with lower formal complaint rates;
- Identify workplaces in riskier sectors that have not been inspected for years. Include them in programmed inspections; and
- Evaluate the "impact" of devoting resources to accident probes versus other inspections.



Remember: If an employee is injured at work, you are required to not only submit the claim to your insurer, but also to Cal/OSHA.

Not doing so can have serious repercussions for you, particularly if the worker has lingering symptoms that require further medical treatment and time off from work. ❖

Gov. Brown Signs Bill Expanding Paid Family Leave

GOV. JERRY Brown has signed new legislation that significantly expands California's Family Medical Leave Act.

Under the current Paid Family Leave Act, employees can take up to six weeks of paid leave annually to care for a newly born or adopted child, or a seriously ill child, spouse, parent or domestic partner. The new legislation adds to the act employees who take time off to care for seriously ill grandparents, grandchildren, siblings and parents-in-law.

While on leave, employees receive payments from a state fund to replace 55% of wages.

SB 770, authored by State Sen. Hannah-Beth Jackson (D-Santa Barbara), takes effect July 1, 2014.

The new legislation will not increase costs to employers directly.

But,as an employer you need to be aware of the expanded pool of family members that an employee can take time off work to care for.

Leave taken under the new and current Paid Family Leave Act is counted against the 12 weeks of unpaid, job-protected leave employees are entitled to under the federal Family and Medical Leave Act.

California's law applies to virtually all employers in the state, unlike the federal FMLA, which exempts employers with fewer than 50 employees. ❖

CYBER SECURITY

Ensure You're Prepared in Case of a Data Breach

IF YOU'VE ever experienced a data breach, you will know just how difficult it is to deal with and all of the ensuing issues that come to the fore.

If customer or employee data was exposed, most states have strict notification laws that you must follow. You will no doubt be trying to figure out how to gird your network for a future attack, and also how to regain your company's perhaps sullied reputation.

Whatever the results of the breach, how you deal with the ensuing fallout can make or break your company's ability to get back on its feet. The online security and risk news website CSO recently published a list of the worst things you can do in the wake of a breach, a list it based on a presentation by Michael Bruemmer of Experian Data Breach Resolution.

Below are eight things you should strongly consider.

1. Use external agencies' services

Sometimes a breach is too big to deal with in-house, and the type of breach may make that option an unwise one. So it's best to have external help available if needed. Incident response teams, such as those offered by Verizon Business, Experian, Trustwave or IBM – to name just a few – should at least be evaluated and considered when forming a business continuity/incident response plan.

2. Engage a lawyer

"Enlisting an outside attorney is highly recommended," Bruemmer said.

"No single federal law or regulation governs the security of all types of sensitive personal information. As a result, determining which federal law, regulation or guidance is applicable depends, in part, on the entity or sector that collected the information and the type of information collected and regulated."

3. Designate a decision maker

"While there are several parties within an organization that should be on a data breach response team, every team needs a leader," Bruemmer said.

There needs to be one person who will drive the response plan, and act as the single source of contact to all external parties. They'll also be in charge of controlling the internal reporting structure – in order to ensure that everyone from executives to individual response team members are kept updated.

4. Have a clear communications plan

Miscommunication can result in you mishandling a data breach, as it delays action and adds confusion.

The decision maker should be the one who also is the main source of information, particularly for the attorney you are using.

Also, have a plan for communicating with customers, and if necessary the public and the media if you are large enough.

"Companies should have a well-documented and tested communications plan in the event of a breach, which includes draft statements and other materials to activate quickly. Failure to integrate communications into overall planning typically means delayed responses to media and likely more critical coverage," Bruemmer said.

5. Have remediation plans

There should be plans in place that address how to engage with customers and others once the breach is resolved, as well as the establishment of additional measures to prevent future incidents.

If you make new investments in processes, people and technology to more effectively secure the data, finding ways to share those efforts with stakeholders can help rebuild reputation and trust.

6. Provide a remedy to customers

Customers should be put at the center of decision making following a breach. This focus means providing some sort of remedy, including call centers where consumers can voice their concerns and credit monitoring if financial, health or other highly sensitive information is lost.

7. Practice regularly

Above all, a plan needs to be practiced with the full team, according to Bruemmer, who recommends regularly updating and revising your incident response plan.

"By conducting a tabletop exercise on a regular basis, teams can work out any hiccups before it's too late," he said.

8. Tap your cyber policy

If you have not purchased one, now is a good time to do so. The threats to businesses grow with each passing day as hackers shift from going after big companies to smaller ones with lower defenses.

A policy can cover the costs associated with a breach, including notification costs and any fines that the state may impose. Call Heffernan Insurance Brokers for more information. ❖