



Brought to you by The TemPositions Group of Companies • www.tempositions.com

MINIMIZE YOUR LOSSES: PREVENTING THEFT OF CUSTOMERS, IDEAS, MONEY AND TIME

By Anne DeAcetis

Many employees abide by their agreements with employers in good faith. But every new hire represents a risk of some form of loss. There are many things employees can steal: confidential information, customers, product, money and even time. A worker who leaves may try to recruit former colleagues, essentially stealing employees. In the face of these risks, companies must have strategies for minimizing losses and recovering from them lawfully.

The FBI calls employee theft the “fastest growing crime” in the US. The American Society of Employers offers sobering statistics: businesses lose 20% of their income to theft and fraud; 20% of employees are aware that it is taking place (though they usually do not intervene); 44% of employees believe their employers could be doing more to reduce losses; and 55% of all offenders are managers—people the company trusts the most.

and crafting the right agreements and policies, employers can do much to reduce their risk.

Devora L. Lindeman, Esq. visited TemPositions’ HR Roundtable Series on December 10, 2009 to offer her guidance. Lindeman has 13 years of experience in employment law and is Senior Counsel at Greenwald Doherty LLP, a firm that represents management exclusively in this area. Lindeman lectures and publishes widely on the subject of employment law and is a regular contributor to www.humanresourcesIQ.com.

Per Lindeman, understanding how losses occur (and how to prevent them) is a timely priority. Employee turnover is much higher than it was in the past, especially among sales staff. Access to computers and company databases makes theft of information quick and easy. And more and more employees belong to social networking sites, which

Theft of physical and intellectual property

Companies suffer when employees take property, money, computers, supplies, product (or even product components) from the workplace. And loss of intellectual property—trade secrets, client lists, proprietary processes, formulas, blueprints, etc.—can harm the company for years to come.

The first thing companies must do, Lindeman stressed, is make reasonable effort to safeguard their property. If information is truly sensitive, it must be kept out of general circulation. Courts may rule that information does not have protection if it is too widely accessible, so access should be granted on a strict “need to know” basis.

If tangible property is valuable, it should also be accessed by fewer people. Cash is better safeguarded by decentralizing authority; separate signatures should be necessary to write checks or access petty cash. Such checks and balances limit the opportunities workers have to steal.

Non-compete agreements

Non-compete agreements have many components. Most restrict employees from going directly to work for a competitor. They prohibit former workers from contacting clients and taking trade secrets or other information. They state that whatever a worker produces will remain the property of the company, and there’s usually a clause prohibiting employees from recruiting their peers.

Surprisingly, many companies don’t have non-compete agreements on file for much of their workforce. They then have no recourse when former employees start their own enterprises or share proprietary information with new employers.

The FBI calls employee theft the “fastest growing crime” in the US. The US Chamber of Commerce estimates that employee theft costs companies from \$20 to \$40 billion per year.

The US Chamber of Commerce estimates that employee theft costs companies from \$20 to \$40 billion per year. And the consequences are real—when companies fail, employee theft is the cause one third of the time.

Many companies assume that if they have basic non-compete agreements on file, they’re protected from information theft. They may also believe that losses from property theft can be recovered by withholding wages (they can’t). The good news is that by anticipating losses

notoriously tempt users to take unofficial breaks from work—stealing time from companies that are paying for it.

Lindeman specializes in “preventative maintenance,” helping ensure that companies’ written policies (from handbooks to employee agreements) protect them adequately. At the HR Roundtable, she stressed the importance of customizing agreements based on the needs of each business and each role. “If a policy is non-specific,” she warned, “it will be non-enforceable.”

Those that do have non-compete agreements sometimes make them so broad in scope that they're unenforceable. Courts weigh a worker's ability to make a living against risk to companies, so it's critical that non-compete agreements be clear—and fair.

Lindeman recommended crafting agreements to be reasonable in terms of three factors: geography, duration and scope. Restrictions should always be based on what employees actually do, what information or technology they have access to, and how likely it is that sharing their knowledge would harm the company.

Surprisingly, many companies don't have non-compete agreements on file for much of their workforce. Those that do have non-compete agreements sometimes make them so broad in scope that they're unenforceable.

If a company is regional, there's no reason to restrict employees from working for competitors in other markets. Companies can't expect workers to leave the industry; a timeframe of 18 months is acceptable. (If keeping an employee away from competitors is vitally important, Lindeman recommended "garden leave," a paid severance period.) Companies also reach too far when they try to restrict employees from taking on different roles for competitors or in related industries.

Again, Lindeman stressed, the value of a non-compete agreement is in the details. If an agreement is full of restrictions that are irrelevant to a worker's daily activities, courts will tend to believe the worker's account of the employment relationship. If an agreement only addresses employees' actions after they leave, they could legally start competitive ventures while they're employed.

Lindeman also recommended applying agreements mindfully. All employees should sign confidentiality agreements. Employees who have personal relationships with the company's clients should sign non-solicitation agreements, which prevent employees from taking clients to their new companies. And only key parties should sign non-compete agreements.

(Non-compete agreements in New York are somewhat unusual. Employees must abide by them if they quit a job or are terminated for cause. But if a company eliminates a position or otherwise lays off an employee, New York State may no longer consider the agreement binding.)

Avoiding lawsuits—a view from the other side of non-compete agreements

Companies tend to focus on non-compete agreements for their own employees. But they may neglect to protect themselves from being named in non-compete suits filed by competitors.

Employers should ask candidates if they are bound by prior agreements as part of the interview process. They should also instruct all new hires not to share confidential information from prior employers. The employee should sign a statement confirming they are not bound by prior agreements and agreeing that they will not share any information.

Existing agreements must be carefully reviewed. Based on the reasonableness of geography, duration and scope, the new employer may find that the candidate is not in violation. Or, they may discover that making an offer poses a business risk. If there's any question, Lindeman advised, the company should consult an attorney with employment law expertise.

Protecting computer systems

Employees routinely use workplace computers for personal use, and employers today are often frustrated by how much time their workers spend surfing the web, shopping, visiting social networking sites and working on personal projects. Especially on breaks and during lunch hours, employees feel entitled to use company computer systems for such activities.

But employment law regarding computer use mirrors the law on telephone use. These systems are company

property. The company is free to dictate how, when and why employees use them. They are entitled to monitor use of their property, within limits. (Companies must stop reading or listening to anything that is clearly personal, and may not use monitoring systems to learn personal passwords.) They're empowered to discipline workers for abuses, up to termination.

Again, Lindeman urged specificity. Policies should state that during the workday, employees are expected to work, and that excessive personal use of computers is a theft of company time. It should be made clear that computers are for work-related use only. There should be clear limits on personal email and the Internet. Employees should have no expectation of privacy, even during breaks. And lastly, determinations of "abuse" should ultimately be left up to the company (to protect against unforeseen behaviors).

For companies that don't have (or want) such a stringent image, policies can be relaxed. Most employers don't want to interfere with brief, necessary communications (e.g., checking on children). But most workers have personal cell phones. Smart phones enable employees to access personal email to take care of urgent needs. In some ways, it is more reasonable than ever to restrict company equipment use, with flexibility at the company's discretion.

Employees may see these restrictions as burdensome, but lifting them again involves risk. Even employees who think they're being careful can put company systems (and data) in danger. Downloads can contain malicious software. The simple act of visiting certain web sites can trigger downloads of adware, which can interfere with computer processes.

Computers may be used to violate discrimination or harassment policies. An employee may forward messages that they find funny, which others may find offensive. If the messages are sent on a company system, the company risks the perception that it condones the conduct.

Social media sites pose their own dangers, because they make private thoughts very public. It's frustrating enough when employees spend excessive time on these sites. But employees who "tweet" negatively about their

work, or post status updates that reveal too much about their companies' business, represent the company poorly and may offend clients as well as colleagues.

It's worth noting that not all online activity is harmful. Some businesses encourage employees to maintain private, professional blogs—this enables the company to make the claim that their employees are thought leaders. Others specifically assign employees to promote the company using social networking. Policies for these employees should reflect these permissions.

If policies are not already in place, Lindeman noted, employers can still take action against offending employees by focusing on their performance. (If an employee is online for much of the day, it's likely that their work does not meet professional standards.) Poor performance, whatever the cause, is always a justifiable reason to discipline or terminate an employee.

Monitoring outside-of-work activities

It's now relatively easy to track employee activities using company-owned technology (computers, cell phones, PDAs and even GPS-equipped vehicles). And there are many laws that support a company's right to monitor activities while employees are working. But there are few laws governing companies' right to use these technologies to track behavior outside of work.

Some monitoring may be appropriate. If a company restricts use of company cars on weekends, for example, they can discover that workers are violating that policy by noting cars' movements on Saturdays and Sundays. (Lindeman noted that it's always polite, though not required, to inform employees that monitoring will take place.)

But many personal online activities fall into a legal grey area. HR may not approve of saucy pictures on a personal web site or expletive-laden blog posts. But New York State in particular is protective of workers. Companies may reach too far if they make hiring decisions based on legal outside-of-work activities (however distasteful) that they discover online.

Lindeman noted that policies vary based on company tastes. An employer with a business-like image will favor stricter policies, prohibiting workers

from making any negative or unprofessional impression, online or off. More casual businesses may be far more permissive.

Again, she recommended reasonableness. What does the company need to know? How likely is it that outside-of-work activities would harm the company? Employees are more likely to respect guidelines that aren't unnecessarily intrusive into their personal lives.

Employment law regarding computer use mirrors the law on telephone use. These systems are company property. The company is free to dictate how, when and why employees use them.

Until there are more laws on the books, companies should choose the approach that makes sense for their business, striking a balance between professional obligations and personal privacy.

Using hiring practices to minimize losses

With so much at risk, hiring good people is an essential starting point for minimizing losses. No system will catch every dishonest employee. But there are many concrete measures employers can take to ensure that they're hiring honest, professional and trustworthy people.

Lindeman recommended multiple interviews with different parties within the company, spreading responsibility for each hiring decision. As a rule, companies should always check references, confirm degrees, call previous employers to verify job experience, and run third-party background checks. All this should take place before an offer is made. (It is much more complicated to terminate an employee once they've been hired.)

Sometimes previous employers resist sharing details. This may be a bad sign. But it can also be simple company policy. Lindeman recommended engag-

ing HR with simple, direct questions. Would the company rehire the worker? Is there anything else a new employer should know?

If a past employer is overly evasive but the hire still moves forward, Lindeman recommended typing a memo about the attempt to check the reference and including it in the employee's file. This due diligence (evidence of having tried to vet the employee) provides some protection against charges of negligent hiring, which can be brought if the new hire harms other employees.

When the worst happens: how to discipline employees who steal

Lindeman recommended quick, clean termination once professional trust is broken. But she acknowledged that many companies have close relationships with employees and may be willing to take extenuating circumstances into account. An otherwise excellent worker who shows true remorse may be disciplined rather than terminated. It's ultimately the company's decision.

If a company is unsure what to do, Lindeman recommended considering how harmful the theft was, the likelihood that the employee will steal again, and the potential harm to the company. What is the worker's complete history? How valuable are they? Would taking simple precautions, like limiting access to property or data, prevent future losses?

Even terminations can be negotiated to be more or less punitive. A worker can be asked to resign, or can be "permitted to resign" (a clear red flag to future HR personnel). If the loss is significant, a company may well want to fire an employee. But Lindeman counseled against making an example of a worker by broadcasting the reason they're leaving. (Charges of defamation are usually not worth the risk, except under carefully scripted circumstances.)

When employees are terminated, they should not be left alone with their computer systems. They may be tempted to access and copy/email proprietary information—or even delete their work.

Lindeman recommended taking a "digital snapshot" of the worker's hard drive (before anyone else uses it). This can be invaluable if the employee tries to fight termination. A principal in

PLACE
POSTAGE
HERE

employment law called “after acquired evidence” gives broad support to terminations if companies discover more infractions (also punishable by termination) after a worker leaves.

And while employees are encouraged to give two weeks’ notice, employers are not obligated to keep them on staff during that time. Depending on the worker, it may be safer to thank them for their service and ask them to leave the office as soon as they’ve gathered their things.

Recovering losses

Once losses are discovered, companies have to decide if, and how, to recover what was stolen (or its value). Some companies carry theft insurance, but these policies often require a police report, and many companies are not interested in making a workplace spectacle out of a loss.

Employers can’t deduct from wages to recoup losses, though they can withhold outstanding expense report reimbursements. They also can’t threaten employees with criminal charges in order to coerce payment. (A company that decides to involve the police should inform the employee, but the decision must be

made independent of the worker’s willingness to repay.)

In general, Lindeman recommended moving on—unless losses are substantial and have the potential to harm the company long-term. If the employer wants to pursue the matter, the courts are the appropriate forum. And it’s important, she stressed, to be consistent. By handling all losses the same way, companies protect themselves from charges of discrimination.

The process of avoiding, dealing with and recovering from loss can be complicated and take valuable hours away from a company’s core business. But by being diligent in the hiring process, drafting detailed agreements and embracing a firm, common-sense approach, companies can do much to reduce their risk of loss—and act decisively when losses do occur.

Anne DeAcetis is a freelance writer based in New York. Reach her at anne.deacetis@gmail.com.

The HR Roundtable is a breakfast forum for human resources professionals in New York City sponsored by The TemPositions Group of Companies. TemPositions, one

of the largest staffing companies in the New York tri-state area with operations in California, has been helping businesses with their short- and long-term staffing needs since 1962. Visit them online at www.tempositions.com or email them at info@tempositions.com.



THE
TEMPOSITIONS
GROUP
OF COMPANIES

420 Lexington Avenue, New York, NY
(212) 490-7400

111 Broadway, New York, NY
(212) 689-2444

20 Broadhollow Road, Melville, NY
(631) 673-7100

10 Mott Avenue, Norwalk, CT
(203) 945-2099

118-21 Queens Blvd., Forest Hills, NY
(718) 544-3100

140 Geary St., San Francisco, CA
(415) 392-5856