Leave donation programs are a popular way for companies to allow employees to donate paid leave time for the benefit of other employees. But a company establishing a leave donation program must consider the tax consequences from the donating employee to the recipient employee, and the employer.

Under basic income tax principles, income is taxed to the donor employee. For example, Joe is entitled to a $500 paycheck at the end of the pay period. He tells his employee, “Instead of giving me $500, pay it to my coworker, Sally.” Although Joe never saw a penny of that $500, in the world of tax law, it is considered Joe’s income and taxed to Joe. The same applies if, instead of giving $50 to Sally directly, Joe decides to transfer some of his time off. Suppose Sally is ill for an extended period of time and has exhausted her sick leave, and Joe tells his employer, “I have some extra paid sick days, just give them to Sally.” Under general rules of taxation, the pay that Sally receives from Joe’s sick days will be taxable to Joe.

The IRS has specifically carved out two exceptions to these principles of taxation. Both exceptions allow the donor (Joe) to shift the tax liability for the donated leave to the recipient (Sally) who benefits from the leave. The first exception allows leave-sharing arrangements for medical emergencies. The second exception allows an employer to establish a leave bank for employees adversely affected by a major disaster declared by the President. In 2005, the IRS also provided some guidance on what the program should look like in Revenue Ruling 90-29:

- Be in writing.
- Create a leave bank for the deposit of donated leave, from which the leave will be distributed. A “one-on-one” plan, where one employee directly donates leave to a specific employee, is more likely to be viewed as income to the donor, followed by a gift to the recipient.
- Restrict eligibility to medical emergencies, such as a major illness or medical condition of the employee or a family member that requires prolonged absence of the employee from work.
- Have a formal application procedure. The applicant employee should be eligible to receive leave from the bank only after the application is approved and the applicant has exhausted all paid leave.
- Limit the amount of paid leave time that may be transferred by a given donor per year.

The leave transferred under the donation plan must actually be used as medical leave by the recipient. If the program simply liquidates the donated leave and pays cash to the recipient, when the recipient is not actually taking legitimate medical leave, the plan will not be viewed as a qualified program.

Presidential Declaration
Last year, the IRS issued Notice 2006-59 setting forth the tax consequences of programs that permit employees to deposit leave in an employee-sponsored leave bank for use by other employees who have been adversely affected by a major disaster as declared by the President of the United States. The leave-sharing plan must be in writing and if it meets eight specific requirements outlined in the notice, tax liability will shift from the donor employee to the recipient employee, the same as under a donation program for medical emergencies.

Wayne State University law student and WNN summer associate Thomas Amen contributed to this article.
In response to a recent case involving an individual being arrested for utilizing a coffee shop's unsecured computer network to hack into a local store's e-commerce system, from his car outside the shop, a number of our clients have asked us to provide some guidance. There are a number of reasons why one might be interested in securing one's computer network from such unauthorized access, and we believe that the case at hand provides an excellent opportunity to do so.

Employees' Criminal Liability
The employer, in such cases, is the only party generally responsible for unauthorized use of computer access. If the employer makes access available to a professional hacker then that hacker, if caught, could face criminal penalties.

An employer's violation of the act, however, could still have repercussions for the employee. In addition to the potential of negative public exposure, any computer security/ intellectual property breach could lead to civil liability for the employee.

As an employer, you need to ensure that you are following all appropriate policies and procedures to prevent unauthorized access. This may include implementing stronger security measures, such as firewalls and intrusion detection systems, to prevent unauthorized access. It is also important to ensure that all employees are trained on the proper use of computer networks and to establish clear policies regarding the use of such networks. In addition, it is important to establish procedures for handling complaints and incidents of computer misuse.

Civil Liability
There are certain circumstances in which employers can be held civilly liable for the actions of their employees. To date, however, there have been no civil cases brought under Michigan law regarding employer liability for employee misconduct.

The easiest example involves violations committed by a tenant or visitor. In such cases, employees access the wireless network without authority. The easiest example involves violations committed by an employee working for the employer. In such cases, employees access the wireless network with authority. It is likely that such an individual without authority access would be entitled to damages.

Similarly, lost profits would likely be small in the context of an attempted breach. For example, in the case where a potential client has already been lost, the individual's access to the wireless network will likely be small in the context of an attempted breach. The individual is likely to have access to the wireless network for a short period of time in order to gain access to the system. During this period, the individual is likely to have access to the wireless network for a short period of time in order to gain access to the system. If the individual is able to access the system, they will likely be able to do so without the employer's knowledge.

In the context of an attempted breach, however, it would be difficult to identify the injury. Even if a plaintiff could articulate injury, such as the overall value of the network, it would be difficult to quantify the damages for the injury in monetary terms. That said, it is still advisable to monitor any access to the network. (Note that you should also make sure that the individual is aware of the unauthorized access to the network.)

Arguably, a piggybacker is wrongfully entering over the owner's wireless network without the owner's permission. A violation of the Electronic Communications Privacy Act. This activity is often called “piggybacking.”

Piggybacking Policy
Although the likelihood of significant exposure is remote, employers who expect their employees to use wireless Internet access in carrying out their job duties should consider adding a policy against piggybacking. Such a policy will serve a couple of important functions.

First, it will make employees aware of the risk of individual criminal prosecution. This factor alone should decrease the number of employees engaging in piggybacking, and consequently decrease an employer's potential liability.

Second, such a policy can be shown to third parties, should the need arise. If an employee is caught piggybacking in the same manner as the applicant, the individual would be able to demonstrate that it took precautions to prevent such behavior.

The current regulations under 405(b) of the IRC were published around the time that the House floor traveled to the U.S. and appeared on the Edsel television show. As a result, these regulations were published in 2004, but final regulations didn't appear in the Federal Register until 2007.

Many of those changes reduce the differences between the rules governing 405(b) plans and those governing other arrangements that include salary reduction contributions (401(k) plans and plans for state and local governmental entities). In connection with these regulations, the IRS has also added additional information to the controlled group regulations surrounding 401(k) plans.

As detailed below, the final regulations confirmed some positions previously announced or interpreted by the IRS over the years. They also include a lot of new guidance.

Effective Date
The final regulations are generally effective for taxable years beginning after Dec. 31, 2008. Those regulations may be counted in establishing a plan year. While a plan may choose to follow the final regulations earlier, there are no restrictions that mandate an earlier effective date except that the plan must be effective as of the first day of the plan year and as of the plan's tax year.

Effective as of the first day of the plan year and as of the plan's tax year. For example, if the plan year begins on Jan. 1, 2009, the plan must be effective as of Jan. 1, 2009. Delayed effective dates are available for church, collective bargaining situations, and governmental entities. The regulations also permit the use of universal availability exclusions, and the removal of certain ascertainable exclusions for all universal availability provisions.

Plan termination
A 403(b) plan now must be maintained pursuant to a written defined contribution plan. All terms and conditions must be in the plan, specifically including eligibility, benefits and limitations. There is no requirement to have a single or multiple plans. A written or formal plan must outline the terms and conditions of the plan, including contributions and other documentation from the providers. There is no specific rule or requirement on the number or subject matter of component documents. For example, a salary reduction agreement could contain a separate document. Under a coordinated Department of Labor guidance, the existence of a written plan formally cause the 405(b) regulations to be subject to ERISA.

Voluntary
The final regulations confirm that a vesting schedule that contains a vesting or non-participation of employees who make a once-time election to participate in a qualified plan other than a 403(b) plan.

Non-discrimination changes
The final regulations incorporate the nondiscrimination standard for employer contributions to qualified plans. The final regulations, therefore, do not apply to insurance and fiduciary requirements available for collective bargaining employees, visiting employees, or employees who make a one-time election to participate in a qualified plan other than a 403(b) plan.

Distributions Restrictions
Distributions from covered accounts (mutual funds, IRAs, and similar accounts) are generally restricted to annuity (403(b) and 401(k) plans). Distributions will be governed by the 401(k) rules and safe harbor. Distributions are not allowed from individual accounts or from employer contributions and attributable earnings.

Universal Availability
Universal availability for defined contribution plans will be required for employer contributions and attributable earnings.

Civil Liability
If you would like any further information about this legislation, or any other activity in the Michigan legislature, please contact Troy M. Cumings at tuna@wnj.com, (517) 679-7411 or Jim Cavanagh at jcavanagh@wnj.com, (517) 679-7410 or Jim Cavanagh at jcavanagh@wnj.com. We are both located in Detroit's New Lansing office.