EMPLOYERS; PROTECT YOUR EMPLOYEES AGAINST IDENTITY THEFT

As more and more Americans are becoming victims of identity theft, many employers are increasing their level of security to protect their employees. A recent General Accounting Office report estimates that as many as 750,000 Americans are victims of identity theft every year. So, what can you do to protect your employees? Here are some ideas.

Employee files
HR (Human Resources) professionals will generally have a set of standard operating procedures when dealing with employee information. Make sure employee files, both active and terminated, are under lock and key. More importantly, make sure that only the Human Resources office has access to this key. In normal cases, the Human Resources office will be the only department who has any reason to access the employee files.

Information Release
Unless an officer of the court provides you with a subpoena, your company should have a strict policy not to ever release employee information to any individual except the employee him/herself.

Clean Desk Rule
Does your company have a clean desk rule? If not, you'd better make sure one is instituted. This rule ensures that any employee who deals with any type of sensitive employee data clears their desk and files and that this information is under lock and key whenever they leave their workstation. Many financial and housing institutions already practice this rule.

Social Security Masking
In the past, entire social security numbers were used to identify an employee. With the increase in identity theft, (and the methods by which thieves acquire this information), employers are now using number masks. In other words, instead of identifying John Doe as 123-00-4567, he is now identified as Doe XXX-XX-4567. This is what is used when sending information via mail or email and has dramatically helped employers reduce identity theft.

Use It Then Lose It
After an employee processes data containing sensitive information, and if it is not required to be refilled, information should be destroyed. A common paper shredder can be purchased for about $50.00 at any office supply store and can be another weapon in your arsenal to protect your employees. Documents should be shredded either immediately after use or at the very least, the same day before the end of the work day. This avoids storing hundreds of documents that can cause your employees' information to be stolen.

Identity theft causes months of grief and potentially thousands of dollars to fix. It's up to employers to do their part in protecting them at the workplace. For more information, contact your Human Resources office or visit the social security administrations website at http://www.ssa.gov/