

# SmartGuard Newsletter

## Is your employer doing everything possible to ensure your identity is safe? Maybe.

There are times when sharing personal information can't be avoided – financial transactions, credit agreements, employment applications, etc. Because you and the institution requesting the information are involved in a legitimate transaction, sharing the particulars of your identity seems logical and most of us do it without issue. The potential for identity theft lies, particularly in employment situations, in the unnecessary use and poor safeguarding of our personal information.

Most companies maintain employee files that include the employees' full name, Social Security number, home address, telephone number, salary and benefit information. It's easy to understand why Human Resource files are a gold mine for identity thieves. All it takes is a name and home address to assume an identity. When it comes to protecting employee information, there are several relatively simple security measures that can and should be done.

### File Access

Your personal information, whether it's in paper files or stored electronically, should be unquestionably secure.

- Personal information should be considered “classified”, requiring a well defined and clearly appropriate use and restricted access.
- Passwords should be both dynamic and confusing with traceable access.
- Temporary employees and those that haven't had a background check should not be permitted access to employee personal data. Employees that do have access to employee information should have their background screened on a regular basis to alert management to questionable activity and ensure their secure background status is maintained.
- Databases of personal information should not be stored on laptop computers. Several recognizable companies including Equifax, Hewlett- Packard, Verizon, and General Electric have had laptops containing employee personal information stolen in recent years.

### Use and Posting

Identifying information should only be used when absolutely necessary.

- Employers should only ask for/retain personal information that is absolutely imperative to the employment process and benefits.
- Social Security numbers should not be used for employee identification or file numbers. Unfortunately this continues to be a common practice and one that can make stealing a co-workers identity a simple process.
- Personal information should not be posted in readily available, public locations.

### Related News

45 million discount store customers had ID stolen

Underground Market for Stolen ID's Thrives

75,000 voter registration cards found in Fulton trash bin

# SmartGuard Newsletter

## Disposal

It is the responsibility of the employer to safeguard employee information even when it's no longer needed.

- Paper containing employee personal information should be shredded prior to disposal.
- Computer hard drives should be cleaned before reassignment or being discarded.
- CD's and DVD's that may have contained employee data should be sanitized prior to reuse or disposal.

Employers have beefed up their employee data security in recent years, but we continue to hear shocking news stories about employee data being found in dumpsters or on laptop computers that are being stolen from within the office environment or out in the community.

While we may not be able to control the measures our employers take to secure our personal information, we can make ourselves aware of potential misuse of our identity. By consistently monitoring the use of our personal information, we can take action on unauthorized changes and use before an identity theft becomes a fully executed and potentially costly identity assumption.

## Early Alert

This innovative detection and warning system utilizes AlertNow, our proprietary system, to scan over 1,500 data sources at various daily, weekly, bi-weekly and monthly intervals for address changes - a common link in identity theft cases. Should any address changes be detected, which typically signifies that there is a theft in progress, AlertNow™ issues a warning by email, phone or pda and to a designated emergency contact number.

This unique early detection system will either prevent theft or at least substantially limit the amount of damage done and time necessary to recover. By issuing alerts to potentially bogus accounts or fraudulent activity, consumers can maintain complete control of their identities with minimal effort.