



**Identity Theft . . . A New Challenge for Companies and Their Employees  
A Seminar by Nationally Renowned Speaker John P. Gardner, Jr.**

- There was a twelve million percent growth in computer spyware attacks in 8 months!
- The industry is expecting a 5 million percent growth in attacks on cell phones in the next 36 months!
- If you, as a business, contribute to losing someone's identity, new laws will make you pay BIG TIME!
- As of June 1<sup>st</sup>, the penalties of FACTA took effect, and HIPAA as of April 21<sup>st</sup>.
- All of your personal information can be had for free on the Internet!

There are 3 types of privacy statement wording:

1. We will share your information unless you tell us not to.
2. We will not share your information except as provided by law, which means we will share your information unless you opt out.
3. (For doctors): We will not share your information except to our subsidiaries (who will share everything unless you opt out.) [However, HIPAA conflicts with this.]

- According to the Wall Street Journal, 51% of all identity theft occurs at work!
- At AOL, a single employee stole a database of over 92 million identities!
- For 4 years, bank managers at 10 different banks were selling 30-40 names per day for \$10 each to identity 'brokers', who were re-selling them for \$60.

According to FACTA, up to \$3,500 of combined Federal and State fines are levied for each name lost by a company.

- The average monetary loss to an individual victim of identity theft is \$92,000.
- The average number of hours to fix your credit, etc., is 600 hours.

By March, 2006, **anyone** handling medical information is covered by HIPAA rules.  
Breaking HIPAA rules can result in a 10 year sentence and a \$250,000 fine!

## WHAT ARE THE 5 TYPES IDENTITY THEFT?

1. Driver License (someone gets a DUI, and evades the law in your name)
2. Social Security Number (someone gets benefits or evades taxes in your name)
3. Medical Info Bureau ID (someone has an AIDS test in your name, someone might steal your benefits, your mortgage might get called due if you have cancer, drug stores sell your information daily)
4. Character (someone commits a crime in your name)
5. Money/Credit – NOTE: you have 2 days before you start losing money. If you don't notify creditors within 60 days, you owe all the fraudulent charges, and bankruptcy no longer eliminates them!
  - Only 26.5% of ID theft is monetary!

As of this year, all cell phones are required to have a GPS in them. If you have a cell phone, you can be found!

HIPAA requires by law:

- That you have a written policy regarding employee misuse of data, and automatic computer log-off times,
- That you have a confidential information contract.
- That you provide training on HIPAA security, which is mandatory as of April 21, 2005.
- That you have a Chief Security Officer.
- That you have a plan in place for early warning of credit fraud, and for damage mitigation.
- That you have a plan for document destruction and computer hard drive destruction.

Prepaid Legal provides:

- On-going background/credit monitoring.
- Restoration (they put in the hours it takes to recover your identity and credit).
- Emergency access to counsel, document review, and letter-writing.

Insurance doesn't cover losses! It only covers the cost of recovering your identity!

It is recommended that we set up a time for the Prepaid Legal people to come in for training and to help us comply with these laws.