

Businesses Are Held Responsible For ID Theft

By Robert Listerman,
CPA, CITRMS*

*Certified Identity Theft Risk
Management Specialist

Businesses of all sizes need to learn more about their responsibilities for preventing identity thieves from gaining access to the information they maintain on customers, employees, prospective employees, contract workers, and vendors. Ignoring recent laws may cost the owner thousands in fines and civil suits.

In 2007 the Identity Theft Resource Center reported 448 identity breach incidences placing over 120 million records on the street. Business was responsible for only 131 of those incidences but over 105 million of the 120 million records resulted from their breaches. The most recent local incidence occurred on January 5th when New

Jersey's Horizon BCBS lost control of 300,000 records. More specific information on each breach may be downloaded from www.btr-security.com.

There are at least five Federal Laws that specifically address a business' responsibility for protecting identities they maintain. The Federal Trade Commission (FTC) enforces these laws. Each state has their laws as well. Without getting into the specifics of each law there are "reasonable steps" the FTC expects the business to implement.

Each business needs to appoint, in writing, an Information Security Officer, develop a written policy to protect non-public information on employees and customers, and hold mandatory training for employees who have

access to non-public information.

Businesses need to evaluate their handling of data as it enters their business, is maintained, and eventually disposed. They should also consider what data they really need to collect or maintain. For example, it is generally not necessary to obtain social security numbers for every job applicant. Wait until you have decided to hire the person and then obtain it for background checks, tax records, etc.

Companies currently involved in litigation with the FTC or involved in class action law suits include: ChoicePoint, LexisNexis, DSW Shoes, Equifax, Veterans Administration, Providence Health Systems, AOL, Tri-West Healthcare, Ohio University, BJ's

Wholesale CardSystems Solutions, Bank of America, Prince William County Hospital, Wachovia, Petco, and many more.

The ABA Journal, March 2006, reported that according to Betsy Broder of the FTC. . "We will act against businesses that fail to protect their data ... all businesses must be able to show they have a written security plan in place. We're not looking for a perfect system... But we need to see that you've taken reasonable steps to protect your customers' and employees' information".

For more information regarding identity theft in the workplace you may contact Bob Listerman at 610-444-5295 or visit www.btr-security.com for more information.