Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace

Experts in identity theft report that a number of cases can be traced back to dishonest employees in the workplace or computer hackers who obtain Social Security numbers (SSNs) of employees and customers and disclose that information to individuals involved in crime rings or other identity theft schemes.

One of the keys to preventing identity theft, therefore, is to safeguard sensitive personal information within the workplace, whether that workplace is a government agency, private business, or nonprofit organization. Everyone must get involved in protecting personal information such as SSNs, financial account numbers, dates of birth – in other words, the information used by identity thieves to impersonate individuals in the marketplace.

WORKPLACE INFORMATION-HANDLING PRACTICES

- Adopt a comprehensive privacy policy that includes responsible information-handling practices. Appoint an individual and/or department responsible for the privacy policy, one who can be contacted by employees and customers with questions and complaints.
- Store sensitive personal data in secure computer systems. Store physical documents in secure spaces such as locked file cabinets and when possible in a locked file room. Data should only be available to qualified persons. Know who has passwords, know who has keys.
- Dispose of documents properly, including shredding paper with a cross-cut shredder, “wiping” electronic files, destroying computer diskettes and CD-ROMs, and so on..
- Conduct regular staff training, including new employees, temporary employees, and contractors. Conduct privacy “walk-throughs” and make spot checks on proper information handling. Reward employees and departments for maintaining “best practices.”
- Put limits on data collection to the minimum information needed. For example, is the SSN really required? Is complete date of birth needed, or would year and month be sufficient?
- Put limits on data display and disclosure of SSN. Do not print SSNs on paychecks, parking permits, staff badges, time sheets, training program

rosters, lists of who got promoted, on monthly account statements, on customer reports, etc. Do not print SSN on mailed documents or require that it be transmitted via the Internet unless allowed by law., do not use SSN as customer number, employee ID number, health insurance ID card, etc.
- Restrict data access to staff with legitimate need to know. Implement electronic audit trail procedures to monitor who is accessing what. Enforce strict penalties for illegitimate browsing and access.
- Conduct employee background checks, especially for individuals who have access to sensitive personal information. Screen cleaning services, temp services, contractors, etc.
- Notify customers and/or employees of computer security breaches involving sensitive personal information.