

- [Affirmative Action Programs](#)
- [Background Checking](#)
- [Drug and Alcohol Testing Policies](#)
- [Employee Handbooks](#)
- [Employee and Supervisory Training](#)
- [Hire By Design](#)
- [HR Audits](#)
- [Job Descriptions](#)
- [Labor Relations](#)
- [Managed Separations](#)
- [On-Site Director of HR](#)
- [Performance Appraisal Programs](#)
- [Personnel Forms](#)
- [Public Sector HR Consulting](#)
- [Recruiting and Hiring Programs](#)
- [Safety Programs](#)
- [Unemployment Insurance Claims and Hearings](#)
- [Wage & Salary](#)
- [Workers' Comp](#)
- [360°](#)



Did You Know...

Customer and employee records have become a prime target for identity theft?

Employer Risks and Exposures

Identity theft has become one of the top consumer fraud complaints in the country. Unfortunately, this crime is no longer just a concern for individual consumers. In recent months, several large U.S. companies have made headlines in the news due to security breaches of employee and customer data.

In some of the cases, confidential employee and customer records were lost in transit, while in others, employees stole their employers' sensitive data for personal gain. A large financial services company recently notified 3.9 million customers that computer tapes containing their personal information got lost while being transported to a credit bureau. In January, a computer technician was found guilty in the largest identity theft case in U.S. history for stealing passwords used by clients of his employer's customers, resulting in millions of dollars in fraud losses. In another case, an employee who handled customer accounts allegedly downloaded customer information to her personal laptop. After the employee was terminated, her employer learned that she had previously been convicted of insurance fraud.

Employers are increasingly becoming targets of identity theft because of the large amount of sensitive customer and employee information in their possession, including personnel files, payroll records, and employee benefits information.

When these types of security breaches occur, employers can suffer serious financial losses as well as negative publicity, loss of business, and poor employee morale, let alone the effects on the customers and employees whose information was stolen. As of June 1, 2005, employers that obtain consumer reports from a consumer reporting agency must comply with the Fair and Accurate Credit Transactions Act (FACTA). The Act requires employers to take reasonable steps when disposing of consumer reports and personal information derived from these reports in order to protect against unauthorized access or use of this information. Failure to do so can result in statutory damages of \$1,000 per employee. If an employee's identity was stolen, the employer could also be liable for actual damages.

Avoiding Disaster

Consider implementing the following practices to reduce the risk of workplace identity theft:

- Verify employment references before making a job offer;
- Conduct criminal and/or credit checks, as appropriate, on final applicants who will have access to confidential information;
- Implement sound policies and procedures for collecting, maintaining, transmitting, and disposing of sensitive customer and employee records;

- Store confidential paper records in locked file cabinets in a secure location;
- Designate an employee or as few employees as possible to maintain personnel records and other sensitive information;
- Allow supervisors access to individual personnel files only if there is a business reason to review them;
- Keep the amount of sensitive employee and customer data maintained to a minimum. The rule of thumb is to obtain employee information only if needed for a business reason;
- Consider alternatives to using social security numbers and other personal identifiers on insurance cards, paycheck stubs, time records, etc.;
- Shred and properly dispose of confidential records that are no longer needed or hire a document destruction company;
- Make access to confidential computer files password-protected and require employees to change their passwords frequently;
- Disable employee access to computer files immediately upon separation;
- Install firewall protection;
- Consider using encryption software, especially before transmitting or physically moving sensitive records to another location;
- Do not store confidential information on a computer that's connected to the Internet; and

Limit the confidential information that employees can remove from the premises.

If you have questions or for more information about protecting your organization from identity theft, contact *AMTEK's* Human Resource Hot Line at **1.800.457.8829.**

This HR eNews is not intended to render legal advice but is meant for general informational purposes only.

CLICK HERE www.amteKHR.com FOR A DIRECT LINK TO OUR WEB SITE

Copyright © 2005 by *AMTEK Management Services Corp., East Syracuse, New York*

HR eNews dated 6/16/05