



DISPOSING OF EMPLOYEE INFORMATION (FACTA 2003)

By Vivian Dickerson, SDA
San Diego Chapter
Society of Design Administration

On June 1, 2005, a new Federal rule went into effect which requires employers to safeguard access to sensitive information derived from employees and requires that disposal of such information be accomplished by burning, pulverizing or shredding. Failure to comply with the new regulations may expose your firm to Federal or State fines or civil liability in individual or class action lawsuits.

The Fair and Accurate Credit Transaction Act (FACTA) was enacted to protect the confidentiality and integrity of personal consumer information and reduce the risk of identity theft and fraud. Sensitive employee information is identified as: the employee's name; address, telephone number, social security number, email address, insurance and/or annuity information (existence of same, payment for its provision, and its number), credit reports for employment, inquiries for mortgages or other such loans, child support obligations, and adverse actions (denial of employment, cancellation or reduction of insurance, and employee misconduct investigations).

FACTA permits an employer's reporting of sensitive employee information under certain circumstances including subpoena, license eligibility, and in accordance with the written instructions of the employee to whom it relates.

Additionally, FACTA sets a national standard for truncation of credit and debit card transactions to include no more than the last five digits of the card number, and Social Security numbers to include no more than the last four digits.

What must you do?

- Keep employee's information confidential— restrict access; segregate the sensitive information from general Human Resources records, monitor compliance.
- Ensure that your paycheck stubs (or those prepared by your specialist) or other such correspondence include no more than the last four digits of the payee's SSN.
- Establish policies for the disposal of employee records:
 - Burn, pulverize, or shred records containing sensitive employee information so that it cannot be read or reconstructed, monitor compliance;
 - Destroy or erase electronic files and media containing sensitive employee information so that the information cannot be read or reconstructed, monitor compliance. This includes erasure of the hard drives of those computers set for disposal or donation;
 - Conduct due diligence if you contract with an outside provider for the storage and/or destruction of records, review and evaluate their policies and procedures for compliance.

More information on FACTA is available at the Federal Trade Commission's website:
FACTA links - www.ftc.gov/os/statutes.fcrajump.htm