

FACTA Red Flags

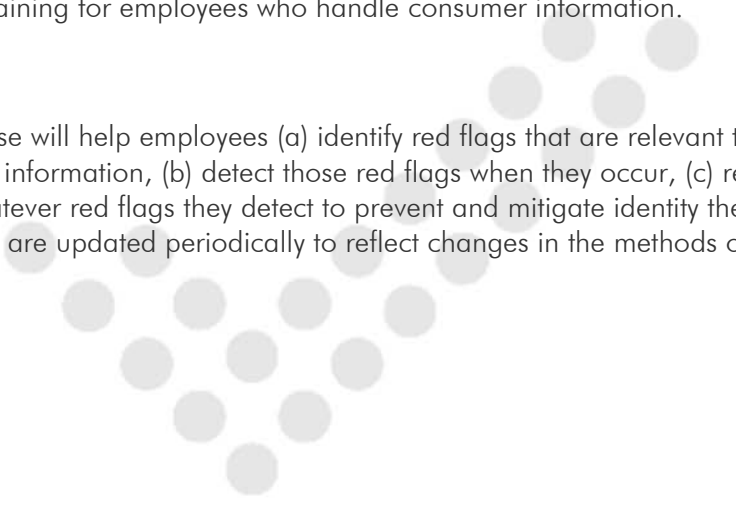
Identity theft is a huge problem for consumers and the companies that serve them. In the U.S. alone, five percent of adults — about 10 million — are victimized each year, with total losses of about \$50 billion. U.S. companies spend another \$50 billion a year on identity-theft-prevention measures.

Companies that handle personal and business account information are a common target of identity thieves. If these companies aren't careful with this information, they can be used as instruments of identity theft by clever criminals. But if they are alert to the "red flags" of identity theft, they can do much to prevent it, detect it early if it does occur, and mitigate the damage it can cause.

New Federal Trade Commission (FTC) regulations under the federal Fair and Accurate Credit Transactions Act (FACTA) require companies to have an Identity Theft Prevention Program that includes "red flag" training for employees who handle consumer information.

Course Summary

This 40-minute course will help employees (a) identify red flags that are relevant to their handling of account information, (b) detect those red flags when they occur, (c) respond appropriately to whatever red flags they detect to prevent and mitigate identity theft, and (d) ensure that red flags are updated periodically to reflect changes in the methods of identity theft.



FACTA Red Flags (cont'd)

The topics covered in the course include —

- What is identity theft?
- Fighting identity theft with FACTA
- Identifying and detecting red flags
- Warnings from consumer reporting agencies
- Suspicious documents
- Suspicious personal identifying information
- Suspicious account activity
- Notice or alerts of identity theft
- Low-tech red flags
- Responding to red flags
- Other information-security practices
- Address discrepancies
- Change of address requests
- Identity theft — a moving target

