



FACTA Red Flags Rule – Ten Steps to Compliance

(Document No. 0502830)

Solutions For Advanced IT Services

Altius Information Technologies, Inc.
Dedicated to the advancement of IT services
151 Kalmus Drive, Suite L-4
Costa Mesa, CA 92626
(714) 442-6670
www.AltiusIT.com

What is Required

The Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), known as the "Identity Theft Red Flags Rule", requires mandatory compliance by November 1, 2008. It requires certain institutions to adopt a written identity theft prevention program.

The identity theft prevention program must include policies and procedures for detecting, preventing, and mitigating identity theft. The regulation requires an institution to have:

- 1) A written program approved by the Board of Directors
- 2) Initial Risk Assessment
- 3) Policies and procedures for detecting, preventing, and mitigating identity theft
- 4) Regular compliance reporting
- 5) Oversight of service providers
- 6) Mandatory staff training
- 7) Ensure the program is reviewed periodically and is updated to reflect any changes.

Initial Risk Assessment

An initial risk assessment determines the entity type, scope of the prevention program, account offerings, and the amount of effort to create the program.

The following are key Risk Assessment tasks:

- 1) Determine Entity Type of the institution
- 2) Identify institution assets
- 3) Identify accounts offerings
- 4) Identify the type of consumer accounts
- 5) Determine methods to open accounts
- 6) Determine methods to access accounts
- 7) Assess previous issues with identity theft
- 8) Identifying supporting systems (i.e., network devices, servers, etc.)
- 9) Identify well-known risks and/or vulnerabilities
- 10) Risk analysis and documentation

Mitigate Identity Theft Risks

Ten Steps to Compliance

Altius IT recommends the following ten step approach to meet FACTA compliance requirements:

1. *Initial risk assessment* – reviews covered accounts, processes to open and access accounts, identity theft, supporting systems, and risks.
2. *Covered accounts* - identify all covered accounts. Inventory types of consumer accounts and loans. Identify identity theft risks associated with each type of account and service offering.
3. *"Red flags"* - Identify a pattern, practice, or a specific activity that triggers the belief that identity theft has occurred. Group into specific red flag categories.
4. *Detection* - implement detection policies and procedures to detect identity theft related to existing accounts, the opening of new accounts, or customers presenting information.
5. *Response* - implement response policies and procedures to respond to events of suspected or identified cases of identity theft, red flags, alerts, and other warnings.
6. *Written program* - develop and document a written identity theft prevention program based upon the size, complexity, the nature and scope of activities.
7. *Training* – develop and implement a staff education and training program to prevent and mitigate identity theft risks. Implement a testing process to ensure your staff follows management directives.
8. *Gap analysis* – periodic reviews of identity theft program, compare actual activities and compare with documented policies and procedures to identify "gaps". Identify impact on organization.
9. *Enhancements* - modifications and enhancements to the program to eliminate "gaps" and ensure compliance in the program. Enhance policies and procedures as necessary.
10. *Subsequent risk assessments* – review changes in service offerings, new covered accounts, policies and procedures to ensure on-going compliance.