

B|N|N BAKER|NEWMAN|NOYES_{LLC}

FACTA & Red Flag Requirements to Protect Against Identity Theft

Diana Thurston, CISA

April 8, 2009

Overview

- What are FACTA & Red Flags?
- Assessing Risk
- Detecting Red Flags of Identity Theft
- Preventing and Mitigating Identity Theft
- Administration and Reporting

Fair and Accurate Credit Transactions Act of 2003 (*FACTA*)

Requires financial institutions **and** creditors to develop and implement written “identity theft” prevention programs.



Federal Register

Friday,
November 9, 2007

Part IV

Department of the Treasury
Office of the Comptroller of the
Currency
12 CFR Part 41

Federal Reserve System
12 CFR Part 222

**Federal Deposit Insurance
Corporation**
12 CFR Parts 334 and 364

Department of the Treasury
Office of Thrift Supervision
12 CFR Part 571

**National Credit Union
Administration**
12 CFR Part 717

Federal Trade Commission
16 CFR Part 681

Identity Theft Red Flags and Address
Discrepancies Under the Fair and
Accurate Credit Transactions Act of 2003;
Final Rule

FACTA Written Program

Must provide for the identification, detection, and response to patterns, practices, or specific activities that could indicate identity theft.

Assess Risk

- Identify Covered Accounts
- Activities Allowed in the Accounts
- Interaction Methods for Activities
- Previous Experience with Identity Theft

Red Flags

A pattern, practice, or specific activity that indicates the possible existence of identity theft.

- Alerts, notifications or warnings from Consumer Regulatory Agency
- Suspicious documents
- Suspicious personal identifying information
- Unusual use of, or suspicious activity related to covered accounts
- Notice from customer, victims of identity theft or other authority

Detecting Red Flags

Policies and Procedures should include:

- Customer Identification Procedures for covered accounts and activities
- Authenticating existing customers
- Monitoring of transactions/activities
- Validating change of address request

Preventing and Mitigating

Policies and Procedures should include:

- Monitoring for evidence of ID theft
- Contacting the customer
- Changing of pass codes or security devices
- Closing or changing accounts
- Not opening account
- Notifying law enforcement

Card Issuers & Change of Address

- Address Validation Requirements
- Alternative Timing of Address Validation
- Form of Notice

Administration of Program

- Board of Director Approval
- Designated employee at the level of Senior Management in the oversight, development, implementation and administration
- Train Staff
- Oversight of Service Providers

Administration of Program

- *Documentation of detection, prevention and actions*
- Periodic review and updating of assessment and policies and procedures of program

Resources

www.ftc.gov/redflagsrule

www.rsa.com

www.fdic.gov

www.ncua.gov

www.bankinfosecurity.com

Diana Thurston

Baker | Newman | Noyes
280 Fore Street
Portland, Maine 04101