



Red Flags Rule

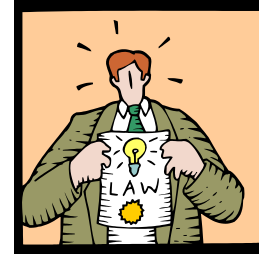
Fair and Accurate Credit Transactions Act of 2003

Lisa Klika

Vice President, Compliance & Quality Assurance
Guild Mortgage Company

What is the Red Flags Rule?

- One provision contained within the Fair and Accurate Credit Transaction Act (aka FACT Act) of 2003, which amended the Fair Credit Reporting Act (FCRA).
- It requires financial institutions and creditors to create an Identity Theft Prevention Program that:
 - Detects,
 - Prevents, and
 - Mitigates Identity Theft
- Requires certain actions be taken by a user of a consumer report when a notice of address discrepancy is reported by a consumer reporting agency (CRA)
- **Mandatory compliance is required by November 1, 2008**

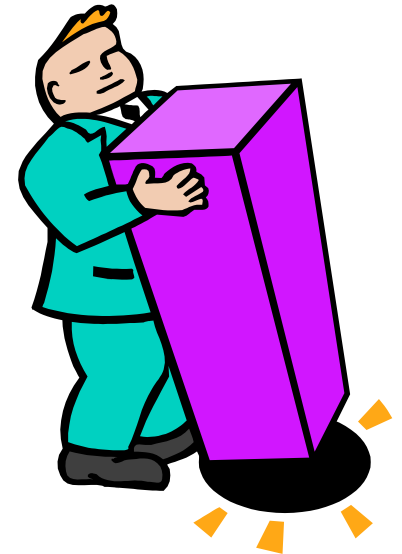


Who must have an Identity Theft Prevention Program?

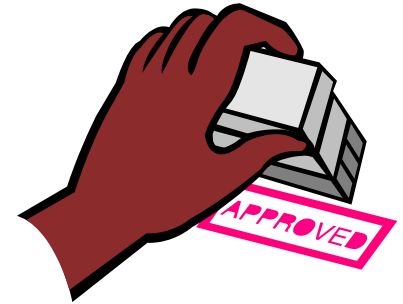
- Financial Institutions and creditors that offer or maintain a “covered account”
 - A covered account is an account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions such as a mortgage loan, credit card account, auto loan, cell phone account, or utility account.
 - Can also include other accounts (such as business accounts) if there is a foreseeable risk to the safety and soundness to the consumer or financial institution.

Establishing your company's Identity Theft Prevention Program

- It's not a "One Size Fits All" approach!
 - Consider the size and complexity of your company
 - Consider the nature and scope of it's activities
- Draw from what you already have in place:
 - Customer Identification Program/Patriot Act
 - Information Security Procedures
 - Privacy Rules
 - Other existing company policies/internal procedures



Administering Your Program



- Board of director approval
- Designated committee or senior management employee to administer and provide oversight of program
- Train staff as necessary
- Appropriate oversight of third party service providers

Elements of Your Program

- Identify red flags
- Detect red flags
- Respond appropriately when they are detected
- Report results & effectiveness
- Update periodically



Identify Red Flags

- Identify what red flags are relevant to the types of accounts covered by the program:
 - The ways in which the company offers to new accounts
 - Retail vs. wholesale
 - Application practices
 - The ways in which the company offers access to established accounts
 - Company experiences with identity theft
 - Changes to methods of identity theft

Red Flag Categories

- Alerts, notifications or warnings from the credit reporting agency or other services providers
- Suspicious documents
- Suspicious personal identifying information
- Suspicious activity by consumer
- Any notices received from identity theft victims, law enforcement, or other parties containing information relating to identity theft.
- See supplement A to appendix J of regulation for specific examples



Detect Red Flags

- Incorporate reasonable policies and procedures to detect the relevant red flags.
 - Acquire identifying information about the applicant
 - Review file for the existence of red flags in the ordinary course of action
 - Use of automated third party services



Respond to Red Flags Accordingly

- Upon identifying all red flags present, what action is required?
 - Consider:
 - How many red flags were detected?
 - Either individually or collectively, what degree of risk do the red flags pose?
 - What other factors might increase the risk?
 - Is there a risk of identity theft present?
 - What is the appropriate response?
 - Contact the consumer
 - Letter of explanation
 - Independent re-verification
 - Denying the loan
 - Report to law enforcement authorities
 - No response warranted based on circumstances

Periodic Reviews of Program

- Review your program periodically and make updates as appropriate
- Consider:
 - Experiences of the company
 - Changes to the methods of identity theft
 - Changes in the industry to detect, prevent, and mitigate identity theft
 - Changes in the company's business channels, affiliations, and operations
 - Do you begin to offer any other covered accounts?
 - Changes to the use of third party service providers
- Annual reporting to board of directors (or equivalent)
 - Evaluate effectiveness
 - Recommend changes

Receiving Notice of an Address Discrepancy

- First, form a reasonable belief that the consumer report relates to intended applicant:
 - Compare the information in the report to identification or other information provided by the applicant
 - Compare the information in the report to other third party resources
 - Verify directly with the consumer (i.e., interview or LOE)
- Second, furnish the consumer's address to the CRA that provided the address discrepancy notice if all of the following are met:
 - Consumer report relates to intended applicant,
 - Company establishes a continued relationship with customer, and
 - Company regularly provides information to CRA in ordinary course of business to the CRA that sent the notice of address discrepancy.

Thank you!

Lisa Klika

Vice President, Compliance & Quality Assurance

lklika@guildmortgage.com

