



# Identity Theft Red Flags Rule Security Program Implementation

*Reid Fudge*

Director IT Security  
Pulte Homes, Inc.

*Shawn Malone*

Vice President, Business Compliance  
Radian Guaranty Inc.

*Heather Czermak*

Senior Product Manager, Automated Compliance  
Wolters Kluwer Financial Services

*RJ Schlecht*

Director, Industry Technology Security & Compliance  
Mortgage Bankers Association

*The OCC, Board, FDIC, OTS, NCUA and FTC (the Agencies) are jointly issuing final rules and guidelines implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act. The rules implementing section 114 require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.*

Rules contains two main areas:

## 1. ID Theft Red Flags

- Assess, written results & plan, approved, implementation, training, continued support and inclusion of Service Providers

## 2. Address Discrepancies

- Identity verification (reasonable procedures)
- Data furnishing (reporting to CRAs)

November 1, 2008 compliance date

- Complementary or an extension to existing programs
- Risk based program
- Involves people, processes and technology
- Administrative Effort
  - Assessment
  - Written result
  - Approved by senior management
  - Periodic review
  - Address Service Providers

# A Lender's Perspective

**Reid Fudge**

**Director of Information Security**

**Pulte Mortgage, LLC**

What did our initial assessment show?

We were already adhering to the Spirit of the rule...our overall risk was low...however, we had some minor gaps that were related to address validation and administration/ documentation of the “Red Flag” program.

- Identification of covered accounts was straight forward
- Many of the red flag indicators were in our existing Loan Processing SOPs
- Basic governance and compliance processes for enforcement were in place

We did encounter several challenges related to:

- Address validation/notification
- Clarification of GLBA/Security vs. Red Flag/Fraud Detection
- Service Provider responsibilities
- Tracking and reporting of “Red Flag Ruling” violations

Our next steps required the formalization of a Red Flag program to:

- Perform a risk assessment
- Document the program and obtain governance approval
- Enhancement of Red Flag procedures
  - Identify relevant Red Flags (Source and Categories)
  - Incorporate any missing flags/address validation into ongoing processes for detection
  - Develop a response plan
  - Track and Report Red Flag exceptions
- Establish oversight requirements for Service Providers
- Perform ongoing administration and training

What ongoing maintenance is required?

- Detect, log, escalate and resolve
- Periodically monitoring the program for changes in scope and effectiveness
- Report to the Board
- Monitor transactions (including address changes) on existing accounts
- Education and training
- Third party/service provider compliance

# A Mortgage Insurer's Perspective

**Shawn Malone**

**Vice President, Business Compliance**

**Radian Guaranty Inc**

- Address Discrepancy (§ 681.1)
  - Conduct discovery to determine extent of user of credit report agencies across the organization
  - Identify discrepancy remediation process based on user activity
  - Several existing business processes already check this area
- Detection, Prevention, & Mitigation of Identity Theft (§ 681.2)
  - Understand scope based on “Creditor” and “Covered Accounts” definitions in Rule
  - Identify applicable red flags based on current business processes
  - Assess Information Security Program relative to Rule
  - Understand likely expectation from business partners
  - Access governance, compliance review process, and training needs

- Address Discrepancy (§ 681.1)
  - Ascertaining credit reporting agency “user” status across business
  - Determining remediation based on ADI type and severity
- Detection, Prevention, & Mitigation of Identity Theft (§ 681.2)
  - Determination of scope as it applies to Mortgage Insurer
    - Creditor
    - Covered Accounts
  - Development of policies and processes versus existing business practices
  - Training and effective monitoring practices
  - Anticipating / responding to requests from business partners
    - Viewed as Service Provider
    - Additional focus area for annual due diligence

- Address Discrepancy (§ 681.1)
  - Conduct discovery / risk assessment process on credit report usage across business
  - Define business rules for ADI remediation
- Detection, Prevention, & Mitigation of Identity Theft (§ 681.2)
  - Comparison of security program versus Red Flags
    - Capitalize on information security program elements
    - Develop program document and complementary governance policies
  - Process/procedure development that serves various business functions
  - Develop effective monitoring to ensure on-going awareness and compliance
  - Incorporate into service provider / third party vendor assessment process

- Address Discrepancy (§ 681.1)
  - Monitor reporting agency ADI reports and respond to substantial discrepancies based on approved policy and associated procedures
  - Verify compliance with company policies and processes
  - Utilize change management process to create compliance record
- Detection, Prevention, & Mitigation of Identity Theft (§ 681.2)
  - Identify appropriate Red Flags based on business functions / process
  - Increase awareness and focus of this Rule along with Information Security Program
  - Develop tracking and reporting mechanism; use of existing channels
  - Monitor Service Providers / third party vendors
  - Recurring training / awareness campaign

# A Technology Provider's Perspective

**Heather Czermak**

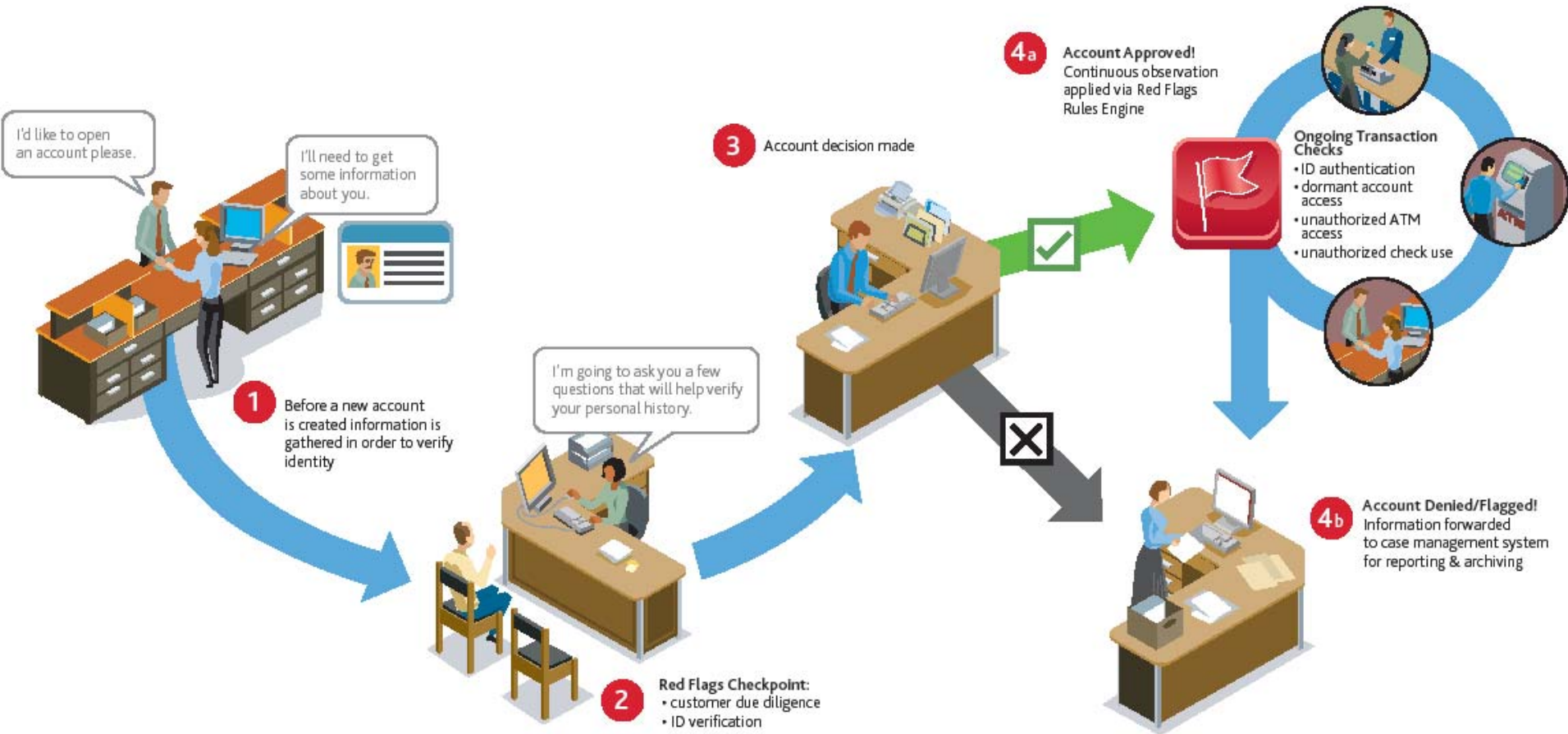
**Senior Product Manager, Automated Compliance**

**Wolters Kluwer Financial Services**

- Identify relevant patterns, practices, and specific forms of activity that signal possible identity theft
  - Requirements
    - Include 3 Regulations
      - Identity Theft Prevention Program
      - Address Discrepancy Requirement
      - Requirements for Card Issuers
    - Apply to new and existing accounts
- Detect 'red flags' that have been incorporated into the Identity Theft Program
  - Gather information from various sources: internal online applications and batch processes, alerts and reports from external sources, etc.
    - Identity Verification – initial applicant validation
    - ID Authentication – ongoing customer profiling
  - Maintain account profiles – ongoing activity monitoring

- Respond appropriately to any red flags
  - Generate alerts on suspicious events
  - Reporting and Case Management investigation documentation repository
- Update the program
  - Red flag library should be flexible and extendable
  - As fraud schemes evolve red flag rules must be enhanced

# Solutions for Red Flag Rules





# Approach

- Easy to use web-based tools that automates customer identification and authentication requirements
- Provides real-time Customer Due Diligence and risk scoring at account opening
- Contains embedded CIP process
- Automates list checking using multiple list sources
- Gathers information from various sources: internal online applications and batch processes, alerts and reports from external sources, etc.
- Maintains account profiles – profiling engine
- Generates alerts on suspicious events
- Facilitates reporting and case management
- Easily customized and adapted to customer environment



# Defining Expected Behavior – Examples of Red Flag Measures

- Deposits Volume Per Account Last 6 Months
- Deposits Volume Per Account Per Month
- No of Account Transactions Last 3 Months
- No of ATM Transactions in Last 3 Months
- No of Deposits in Last 3 Months
- Transactions Volume Per Account Per 6 Months
- Transactions Volume Per Account Per Month
- Withdrawal Volume Per Account Per Month
- Withdrawal Volume Per Account Per Month

# Examples of Red Flag Rules

- ATM Transaction of Dormant Account
- Deposits Increase Compared to Last 6 Months
- New Credit Account Credit Limit Exploitation
- New Request After Address Change
- Transaction Increase Compared to Last 6 Months
- Withdrawal Increase Compared to Last 6 Months

- Embeds Red Flag identification, detection, investigation and documentation in business processes
- Shifts the emphasis from reactive to proactive controls in support of existing workflow
- Justifies IT spend for AML/BSA and Red Flag purposes
- Facilitates ongoing adjustments to policies and procedures through flexible configuration
- Creates management visibility to measure the effectiveness of the program by summarizing these efforts through ad-hoc and custom reporting in order to show the complete Red Flag program detailing identification, detection, investigation and updating components

## Reid Fudge

Director, IT Security  
Pulte Mortgage, LLC  
7475 S. Joliet Street  
Englewood, CO 80112  
303-493-2031  
reid.fudge@pulte.com

## Heather Czermak

Senior Product Manager, Automated  
Compliance  
Wolters Kluwer Financial Services  
130 Turner St, 3<sup>rd</sup> Floor  
Waltham, MA 02453  
heather.czermak@wolterskluwer.com

## Shawn Malone

Vice President, Business  
Compliance  
Radian Guaranty Inc.  
1601 Market Street  
Philadelphia, PA 19103  
215-231-1667  
shawn.malone@radian.biz

## Robert (RJ) Schlecht

Director, Industry Technology Security  
and Compliance  
Mortgage Bankers Association  
1331 L Street, NW  
Washington, DC 20005  
202-557-2843  
rschlecht@mortgagebankers.org