# New Identity Theft Red Flags Rule: What is New and How Leading Companies are Integrating Into Existing Processes

## The Privacy Symposium

Lydia E. Payne-Johnson

Peter A. Rabinowitz

PricewaterhouseCoopers, LLP

Harvard University

August 20, 2008

PRICEWATERHOUSECOOPERS

# Agenda

- Introduction: The New Identity Theft Red Flags Rule
- Who Will Need to Comply
- Compliance Benefits/Non-Compliance Risks
- Key Terms
- Building a Red Flags Rule Program
- Getting Started
- Our Point of View: Steps Towards Compliance
- Key Takeaways
- Questions?

# Introduction: The New Identity Theft Red Flags Rule

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

# Introduction: The New Identity Theft Red Flags Rule

- Issued by the FTC and banking industry regulators to help detect, prevent and mitigate identity theft by protecting corresponding customer, institution and creditor risks
- Covered companies are required to:
  - Conduct a targeted risk assessment based on specified criteria;
  - Identify “covered accounts” and activities that potentially may be at risk for identity theft;
  - Develop and implement a written Identity Theft Prevention Program;
  - Implement ongoing processes for monitoring covered accounts; and
  - Ensure “safety and soundness” of the organization from ID theft
- November 1, 2008 compliance date

# Who Will Need to Comply

- "Creditors," whether financial or non-financial, which include:
  - Banks
  - Credit/Debit Card Issuers
  - Mortgage Lenders
  - Utility Companies
  - Telecommunications Companies

# Key Benefits of Compliance

- Strengthens overall due diligence efforts
- Instills customer loyalty; confidence;  and trust
- Boosts employee morale
- Helps to “connect-the-dots” in your ongoing fraud detection and privacy compliance efforts
- Helps keep your organization off consumer-focused regulators’ radar

# Potential Risks of Non-compliance

- Reputation/brand damage
- Loss of revenue
- Loss of employee morale (employees may be customers/users, too)
- Civil liability arising out of identity-theft related damages to customers
- Significant regulatory fines and/or sanctions.

# Key Terms – “Creditor”

- “Creditor” is based on the definition under 15 U.S.C. §1691a as being any person who:
  - Regularly extends, renews, or continues credit;
  - Regularly arranges for the extension, renewal or continuation of credit; or
  - Any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

# Key Terms – “Covered Accounts” & “Transaction Processes”

- “Covered accounts”
  - Consumer-related transactional accounts offered by banks, credit and debit card issuers, and other creditors (such as mortgage lenders, telecommunications companies and utilities)
  - Accounts that potentially have a "reasonably foreseeable risk of identity theft" such as:
    > deposit accounts and extensions of credit, (i.e. purchase of property or services involving a deferred payment);
    > accounts used primarily for personal, family or household purposes; and
    > other accounts. i.e., small business and sole proprietorships
- “Transaction processes” associated with account opening, accessing and closing, and/or other related experiences with identity theft.

# Key Terms – “Identifying Information”

- “Identifying Information” is a any name/number used alone or with any other information to identify a specific person, including:
  - > Name, DOB, SSN, Driver’s License/State ID, Alien Registration #, Passport, Employee or Tax ID#;
  - > Unique biometric data (fingerprint, voice print, retina, iris image);
  - > Unique electronic ID #, address, routing code; or
  - > Telecommunication identifying information or access device.

# Additional Requirements – Monitoring Address Changes

- Companies must also monitor customers' address changes and/or discrepancies associated with the change:
  - Verifying the validity of change of address requests;
  - Authenticating your customer's identity; and
  - Ensuring accuracy of consumers' addresses when providing to a credit reporting agency (CRA) during the period of continuous customer relationship.

# Building a Red Flags Rule Program

- Four primary components that require implementing processes to:
  - Identify Relevant Red Flags for Covered Accounts
  - Detect Red Flags
  - Prevent and Mitigate Identity Theft
  - Periodically Update the Program

Building a Red Flags Rule Program

# 1. Identify Relevant Red Flags for Covered Accounts

- Requires conducting an assessment to determine applicable risk factors, sources and categories of red flags to identify:
  - Covered accounts;
  - Associated account opening processes;
  - Account access mechanisms (i.e., in person, call center, website); and
  - Historical incidents/patterns of ID theft.

Building a Red Flags Rule Program

# 2. Identify Relevant Red Flags for Covered Accounts

## 5 Red Flag Segments define 26 Key Indicators

- > Alerts, notifications or other warnings from CRAs, Service Providers, Fraud detection services;
  - » i.e. fraud/active duty alert; credit freeze notice, inconsistencies in account activity
- > Presentation of suspicious documents (altered/forged);
- > Presentation of suspicious identifying information (inconsistent with your records);
- > Unusual/suspicious activity related to a covered account following change of address request (uptick in activity and users); and
- > Notice regarding possible ID theft related to covered accounts from customer, law enforcement, ID theft victim or any other person.

Building a Red Flags Rule Program

# 2. Detect Red Flags

Requires monitoring of new and existing covered accounts by:

> Strengthening how the identity of customers are verified;

> Authenticating customers;

> Monitoring transactions; and

> Verifying the validity of address changes, especially for existing covered accounts.

Building a Red Flags Rule Program

# 3. Prevent and Mitigate Potential Identity Theft

Implementing appropriate responses to heightened risks of identity theft:

- > Account monitoring;
- > Contacting the customer;
- > Changing any password, security codes or other security devices that permit access to a covered account;
- > Assigning a new account number to a covered account;
- > Not opening a new covered account;
- > Ceasing attempts to collect on a covered account or selling to a debt collector;
- > Notifying law enforcement; or
- > No action due to the particular circumstances.

Building a Red Flags Rule Program

# 4. Updating Your Red Flags Rule Program

Making relevant periodic changes to mitigate risks to customers or to the "safety and soundness" of the organization based on:

> Experiences with identity theft;

> Changes in identity theft methods;

> Changes in identity theft prevention methods;

> Changes in the types of accounts offered and/or information collected; and

> Organizational changes due to mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Getting Started:

# Leverage Existing Processes

- Existing risk assessment and compliance programs that may be leveraged may include:
  - Fraud Prevention
  - Information Security
  - Privacy
  - Enterprise Risk Management
- Proactive approach to compliance

# Our Point of View: Steps Towards Compliance

Five key phases:

- Conduct a high level review of key existing risk assessment and compliance programs
- Identify covered accounts, select a high risk / high priority account class for a pilot Red Flags Rule risk assessment, and execute a pilot/test program
- Based on the pilot's results, build a prototype Red Flags Rule risk assessment process that leverages and integrates existing processes
- Roll-out the Red Flags assessment to other covered accounts on a risk-rated basis
- Develop and implement an overarching, sustainable Red Flags Rule Identity Theft Prevention Program and governance process.

# Key Takeaways: The Identity Theft Red Flags Rule

- Applies to any covered institution or creditor that collects and uses consumers' confidential personal information, interacts with a credit reporting bureau, and/or maintains transactional accounts for individuals and businesses
- Includes both retail and business accounts
- May involve significant operational and systems adjustments
- Requires conducting an initial risk assessment
- Requires identification and implementation of appropriate identity theft red flags
- Requires implementing and sustaining an Identity Theft Prevention Program including on-going monitoring of and adjustments to red flags and program
- Mandatory compliance by November 1, 2008

# Questions?

# Presenters

Lydia E. Payne-Johnson
Privacy, Governance, Risk and Compliance Advisory Services
T: 646-471-4487
E-mail: lydia.e.paynejohnson@us.pwc.com

Peter A. Rabinowitz
Privacy, Governance, Risk and Compliance Advisory Services
T: 267-330-1780
E-mail: peter.a.rabinowitz@us.pwc.com

www.pwc.com



PRICEWATERHOUSECOOPERS