**PIVOT**GROUP

Armed with Information Security Knowledge

# What Do Red Flag Rules Mean to Your Financial Institution?

Personally identifiable information (PII) is the pieces of information that can be used to distinguish or trace an individual's identity; name, social security number, bank account and PIN, etc. Information technology has significantly increased the collection of PII, and as a result, identity theft and fraud is running rampant. In response, the Federal Trade Commission, FFIEC, FDIC and NCUA sent the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 to the Federal Register for publication of the final rule. The preemptive "Red Flag" went into effect January 1, 2008, are designed to strike at identity theft in its earliest stages.

## Red Flag Rules

**Compliance is mandatory** beginning November 1, 2008 for all financial institutions. Do you know what this means for your organization? Will you be ready?

*Compliance is mandatory November 1, 2008 for all financial institutions.*

**The Red Flag Rules** require that each institution develop a written program that will:

- Identify relevant "Red Flags"; relevant patterns, practices, and specific activity that indicates possible existence of identity theft.
- Establish a mechanism to detect Red Flags that have been included in your program.
- Respond appropriately to detect Red Flag events to prevent ID theft and mitigate its effects.
- Update your program regularly to reflect changes in ID theft risks to customers/members and your institution.

Examples of specific events that a financial institution should monitor as possible indicators of identity theft include; suspicious or unusual account activity that is inconsistent with previous account activity, consumer fraud alert received from a consumer reporting agency, suspicious identification documents that appear to be altered or forged, and suspicious access to PII. A security breach can also occur if a financial institution's records are compromised by an unauthorized employee. Adequate notification is required once determination is made that this data is "in the wild", including verifying whether or not this data has been released to the public domain and its potential affect on customers/members.

As the November 1st deadline approaches, financial institutions should look for assistance from objective third parties to perform risk assessments and help develop effective identity theft programs. They must substantiate that they have developed a program sufficient enough to meet the Red Flag requirements.

Pivot Group LLC • 5555 Glenridge Connector, Suite 200 • Atlanta, GA 30342 • (404) 419 2160 • www.pivotgroup.net

**PIVOT**GROUP

Armed with Information Security Knowledge

**Pivot Group has outlined a Red Flag 4-phase roadmap for financial institutions:**

# look, plan, act, repeat

# Red Flag Rules

**look** – Risk Assessment of Your Red Flag Program

- o Identify procedures and policies to follow with regard to:
  - How Red Flags will be identified, implemented, and recorded
  - The incident response plans for mitigating and dentifying ID theft

**plan** – Build a Proactive Red Flag Strategy

- o Set up a framework with the approval of the board of directors or an oversight committee
- o Identify how to mitigate ID theft risks
  - Technical controls
  - Management controls
  - Operational controls
- o Draft or revise security policies to cover these risks
- o Select potential technologies
- o Education program for employees and customers

*Rely on Pivot Group to help you develop a Red Flag action plan.*

**act** – Take Action on the Red Flag Strategy Plan

- o Implement the processes, controls, and technologies
- o Revise security policies as required
- o Train customers and employees on security best practices

**repeat** – The Life Cycle of the Red Flag Program is a Process Not a Destination

- o Periodic analysis of what worked and what procedures need to be updated as ID theft attempts change
- o Ongoing basis – repeat it on a regular basis as security best practices indicate
- o Schedule regular risk assessments and update policies/controls regularly
- o If new technology is employed, schedule a risk assessment
- o If business requirements change, schedule a risk assessment

**Take action now - you can't afford to wait**.

As an independent information security consultancy, Pivot Group is committed to providing the services that best fit each institution's unique needs. Contact Pivot Group today to help your financial institution determine exactly what your plan of action should be to make certain you are in compliance with the Red Flag rules.

Pivot Group LLC • 5555 Glenridge Connector, Suite 200 • Atlanta, GA 30342 • (404) 419 2160 • www.pivotgroup.net