

# Red Flag Rules: How to Tame the Raging Bull

Keith Cheresko, VP, Privacy Associates International, LLC  
Mark Schettenhelm, Product Manager, Compuware

IAPP KnowledgeNet meeting June 15, 2010

# What is a Red Flag?



# First Auto Works Red Flag limo?



# What is a Red Flag?

- A method to further antagonize an already raging bull
- A device specified by Federal regulators to torture perpetrators of oil spills
- A sign of surrender resulting from the growing number of identity theft cases
- A method or means of warning others of potential danger
- A method or device alerting you or others that something is amiss, requiring further inquiry or action
- Or maybe it is a Federal red flag

# What is a Red Flag Under Federal Red Flag Rules?

Under Federal Red Flag regulations (or rule) adopted pursuant to section 114 of the Fair and Accurate Credit Transactions Act (FACTA) amending the Fair Credit Reporting Act (FCRA) a Red Flag is a

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

Conceptually simple --- in practice maybe not so simple.

# What is the Red Flag Rule?

- Regulation adopted by multiple Federal regulatory agencies (FRB, FDIC, NCUA, OCC, and OTS) published November 9, 2007 and effective January 1, 2008
- Presently enforced by all issuing Federal regulators except FTC – Delayed until December 31, 2010
- Requires **Financial Institutions** and **Creditors** to implement a written **Identity Theft Prevention Program** upon specified conditions (often referred to as the Red Flag Program or simply the Program).

# How is the Red Flags Rule Structured?

- Rule, Appendix (Guidelines) and Attachment
- Rule sets forth risk based obligations and requires use of the guidelines as appropriate and relevant
- Guidelines are factors that “should be considered”
- Guidelines are to be updated periodically by the Agencies
- Attachment provides additional information and examples

# Why a Red Flag Rule?

- Effectuates Congressional desire to find a way to reduce the ongoing incidents of identity theft
- Existing rules (e.g. GLBA's privacy and security requirements) address obligations to maintain security and privacy of personal data.
- Breach rules address disclosure and consumer notice if security fails.
- The Red Flag Rule helps close the data protection loop by seeking to prevent identity theft before it can happen

# What is a Red Flag Program?

A written and implemented Identity Theft Protection Program by **Financial Institutions** and **Creditors** that maintain one or more **covered accounts** designed

- to detect, prevent, and mitigate **identity theft** in connection with the opening of a **covered account** or any existing **covered account** and
- appropriate to the entity's size and complexity and the nature and scope of its operations.

# Who Must Implement a Red Flag Program?

- **Financial Institutions** – State and national banks, state or federal savings and loan institutions, mutual saving savings banks, state or federal credit unions, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer.
- **Creditors** – any person who regularly extends, renews, or continues **credit**; any person who 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**.

# Who Must Implement a Red Flag Program? cont'd

- in each case where the **Financial Institution** or **Creditor** offers or maintains one or more **covered accounts**.
- **Credit** - the right granted by a **creditor** to a debtor to defer payment of debt or to incur new debt and defer its payment or to purchase property or services and defer payment therefor.

# What is an Account ?

- A continuing relationship established by a **person** with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes.
  - Any relationship to obtain a product or service that an account holder or **customer** may have with a **financial institution** or **creditor**
  - The purchase of property or services involving a deferred payment
  - Deposit and checking accounts

# What is a Covered Account?

There are two types of **covered accounts** under the Rule:

- an account primarily for personal, family, and household purposes that involves or is designed to permit multiple payments or transactions (e.g. credit card, mortgage or auto loan, margin account, checking or savings account - *consumer accounts*)
- any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness to the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. (e.g. small business accounts, sole proprietors and others that may vulnerable to identity theft should be considered – *business accounts*.)

# What are the Elements of a Program?

The Program must include reasonable policies and procedures to:

- Identify relevant Red Flags.
- Detect Red Flags.
- Respond to prevent and mitigate identity theft.
- Update the Program periodically.

# How Do I Identify Relevant Red Flags?

- Identify the Red Flags of identity theft you're likely to come across in your business, the potential patterns, practices, or specific activities indicating the possibility of identity theft.
- Items singly or in combination
- Consider information in Appendix and Supplement
- Look to Supervisory guidance
- Consider your own entity's experience with identity theft
- Stay aware of methods of identity theft that reflect changes in risk

# What are Categories of Common Red Flags?

- Supplement A to the FTC version of Red Flags Rule lists five specific categories of warning signs to consider including in your Program.
  - Alerts, Notifications, and Warnings from a Consumer Reporting Agency
  - Suspicious Documents
  - Suspicious Personal Identifying Information
  - Suspicious Account Activity
  - Notice from Other Sources

# How Do I Detect Red Flags?

- Set up procedures to detect the identified Red Flags in your day-to-day operations.
- Different risk and procedures for in person or telephone, mail, Internet, or wireless system.
- Tailored to differing types of covered accounts
- Not one size fits all
- Use of verification and authentication techniques can help turn up Red Flags
- Where existing programs monitor transactions, identify behavior indicating possibility of fraud and identity theft, or validate changes of address incorporate them into your Program.

# How to Respond to Prevent and Mitigate Identity Theft?

- Respond appropriately
- Assess and evaluate whether detected Red Flag is evidence of identity theft risk
- Reasonable basis for concluding that detected red flag does not evidence risk of identity theft
- Monitor account, contact the customer, change passwords or access devices, reopen account with new access, not open a new account, close an existing account, notify law enforcement, not issue a new card, not attempt collection, etc .....
- Determine no response is warranted under the circumstances.

# Why Must I Update the Program Periodically?

- Periodic updates to the Program are required to ensure it keeps current with identity theft risks
- Reflect own experience, changes in methods of identity theft, changes in methods to detect, prevent, and mitigate identity theft, types of accounts offered, changes in business structures
- Consider annual updating to coincide with required senior management reporting.

# Why Periodic Identification of Covered Accounts?

- Determine whether offering or maintaining covered accounts
- Conduct risk assessment taking into consideration
  - The methods provided to open accounts
  - The methods provided to access accounts
  - Previous experience with identity theft
- Check for reasonably foreseeable risks of identity theft in connection with business accounts that may be opened remotely, without in person contact, by telephone, and over the internet.

# What are the Administration Requirements?

- Obtain approval of the initial written Program from the board of directors, a committee of board, or in some cases designated senior management
- Involve senior management in the oversight, development, implementation, and administration of the Program
- Train staff, as needed, to effectively implement the Program
- Exercise appropriate and effective oversight of **service provider** arrangements
- Include guidelines that are appropriate

# What is a Service Provider?

- A person that provides a service directly to the financial institution or creditor

# What Responsibilities are Involved With Use of Service Providers?

- Must exercise appropriate and effective oversight of service provider arrangements
- Take steps to ensure the activities of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risks of identity theft
- Service provider to multiple financial institutions or creditors may use own program as long as the program complies with the Rule
- Suggest specify requirements in written service contract you may outsource the work not the responsibility

# What is the FTC's Enforcement Posture?

- Rule in effect not being enforced by the FTC at this time
- FTC has issued five enforcement extensions
- Delayed enforcement relates to issues over creditor and credit provisions
- Professional Associations for lawyers, accountants, and doctors have each filed suits challenging application of the rule to professionals
- Lawyers won at trial and the FTC filed an appeal; court in the accountants' case issued a stay pending a decision on the lawyers' case; and the doctors suit was just filed recently

# What is at Issue in the Lawsuits?

- The definition of credit and creditor play a central role
- The procedural process followed by the FTC in adopting the rule
- Lack of an explicit congressional statement of intent to include activities traditionally regulated by the states

# Is There Action in Washington?

- There are bills in both houses of congress
- House bill H.R. 3763 passed the House 400 – 0 in October 2009
- Senate bill 3416 was introduced May 25, 2010
- Both bills provide exemptions to the Rule for small health care providers, accounting firms and law firms, subject to conditions.
- Also provides the FTC with authority to grant exemptions upon application of other businesses upon specified conditions.

# Helpful Resources

- "FIGHTING FRAUD WITH THE RED FLAGS RULE - A How-To Guide for Business" <http://www.ftc.gov/redflagsrule>
- "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule" Federal Register / Vol. 72, No. 217 / Friday, November 9, 2007 [ftc.gov/os/fedreg/2007/november/071109redflags.pdf](http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf)
- New "Red Flag" Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft [ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm](http://ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm)
- The "Red Flags" Rule: Are You Complying with New Requirements for Fighting Identity Theft? [ftc.gov/bcp/edu/pubs/articles/art10.shtm](http://ftc.gov/bcp/edu/pubs/articles/art10.shtm)

# Contact information

Keith Cheresko, Vice President

Privacy Associates International LLC

[kcheresko@privassoc.com](mailto:kcheresko@privassoc.com)

[www.privassoc.com](http://www.privassoc.com)

248 535 2819

Mark Schettenhelm, Product Manager

Compuware

[Mark.Schettenhelm@compuware.com](mailto:Mark.Schettenhelm@compuware.com)

313 227 6985

