



Complete. On Demand. Affordable.

Red Flags Rule: The FTC Regulation and Solutions to Prevent Identity Theft

Kevin Prince
Chief Technology Officer
Perimeter eSecurity

The Red Flags Rule was developed pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The rule applies to creditors and financial institutions. Federal law defines a creditor to be:

- Any entity that regularly extends, renews, or continues credit.
- Any entity that regularly arranges for the extension, renewal, or continuation of credit.
- Any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

Accepting credit cards as a form of payment does not, in and of itself, make an entity a creditor. Some examples of creditors are finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies, and non-profit and government entities that defer payment for goods or services. Financial institutions include entities that offer accounts that enable consumers to write checks or to make payments to third parties through other means, such as other negotiable instruments or telephone transfers.

A comprehensive identity theft program will include:

- Identifying processes, systems, and procedures that add to, interact with, or store sensitive customer information.
- Creating a program that looks for patterns practices or other activities to identify, detect, and respond to behavior that could lead to identity theft including:
 - The modification of human behavior with regard to business processes. Much of Red Flags falls within the area of modifying procedures of employees to help detect and respond to behavior that can lead to identity theft.
 - Implement technologies that can identify system and human behavior that can lead to identity theft.
 - Ongoing training of these policies, procedures, and best practices including the monitoring and reporting of red flags.
- A response plan for when red flags are triggered.

GLBA is centered around the protection of sensitive information to limit fraud and identity theft. Red Flags goes beyond GLBA and calls for a specific plan to identify, detect and respond to suspicious activity that could indicate identity theft. Red Flags encompasses all organizations that must adhere to GLBA, but also applies to many other organizations as well.

Organizations that are currently compliant with GLBA have a bit of a head start. Current policies and procedures combined with information security solutions can all be applied to Red Flags compliance. Minor modifications to policies and procedures combined with the implementation of a few key technologies and solutions will likely push these organizations very near full compliance. Special care should be taken for procedures that deal with the creation of new accounts, extending credit,

modifications of data, and abnormal use of data or accounts. For these institutions, solutions that help mitigate the risk of a data breach have long been employed. These solutions include a firewall, an intrusion detection and prevention system, etc. However, there are additional solutions that will specifically help achieve the requirements of Red Flags that many of these organizations do not use.

- **Host Based Intrusion Detection and Prevention (HIDS/HIPS)** is a software solution that is designed to be loaded directly on the systems you want to protect at a higher level. The software generates alerts for any abnormal behavior based on a set of predefined rules.
- **End User Security Awareness Training** is a formal training program for employees. 12 courses are available online - each of which is designed to address a different aspect of information data security. For example, the Social Engineering course helps train employees to not give out sensitive information. There are courses around a clean work area, password use, Internet use, and more. Employee training is a critical part of any identity theft program.
- **User Access Auditing** creates alerts on suspicious activity as it pertains to user authentication on the network. For example, if one user id is logged into multiple systems, an alert is generated. If an account is logged in after hours or has several missed login attempts, alerts can be generated.

Organizations that have not historically fallen under GLBA may have a longer road to travel to become fully compliant with the Red Flags Rule. Perhaps no written or formal risk mitigation plan (let alone an identity theft prevention program) has ever been completed. The Red Flags Rule states that a program should be based on the size and complexity of your organization. It is essentially up to company what that program should include. In addition to complete policies and procedures to help detect and respond to identity theft, many technology solutions can be utilized to help detect and stop a data breach that could lead to fraud and identity theft.

- **Managed Firewall** can block unwanted traffic from entering your network from the Internet. Being managed by a qualified security professional can reduce errors and keep systems up-to-date to offer the best security possible.
- **Network Based Intrusion Detection and Prevention Systems (IDS/IPS)** should be employed to help identify and stop attacks that can lead to the compromise of systems where sensitive data resides.
- **Web Content Filtering** is a method to restrict employee and other insiders access to inappropriate web sites via your network. The written policies and procedures should identify which groups of users have access to which categories of web sites. This will curb the chances of an employee accessing a malicious or compromised web site that could install Trojan horse or other malware on the user's system. This software can be used to capture and send sensitive information.

An identity theft prevention program would be strengthened by additional risk mitigation technologies. Any technology that can reduce the chances of a data security breach will ultimately reduce fraud and identity theft. Additional technologies that you may want to consider include:

- **Email Defense Solutions** such as **Content Filtering**, **SPAM Filtering** and **Anti-Virus** can all help protect sensitive information. Phishing emails are an example of a SPAM message that may attempt to lure an employee out to a malicious web site where they can be compromised or enter sensitive information.
- **Remote Backup and Recovery** services can be used to reduce the risk of media being lost or stolen. Backup tapes, CDs and DVDs become high targets for criminals because they usually store our most critical data. A remote backup and recovery service allows you to securely store the data off-site using encrypted tunnels on the Internet, eliminating the opportunity for someone to mishandle, steal, or lose this sensitive data.
- **Policy Compliance** services scan individual servers and desktops for the status and configurations of specific policies. For example, policy compliance can check to see if your users are changing their passwords frequently enough, that passwords meet a desired length, and they are complex enough. Enforcing and auditing policies can reduce the risk of systems being compromised, which can lead to the compromise of data that can be used for identity theft and fraud.
- **Vulnerability Management** can also help reduce the risk of identity theft. Cyber criminals often use the exploit of vulnerabilities to compromise systems and data which can lead to identity theft. Identifying these vulnerabilities using internal and external vulnerability assessments, and then mitigating those vulnerabilities with a robust patch management system is one of the best ways to keep identity thieves out of your network.

Technology solutions are only one part of a comprehensive identity theft prevention program. However, when solutions are combined with enforced policies and procedures, Red Flags compliance can be achieved. Whether you are under GLBA now and well on your way to Red Flags compliance, or this is all brand new to you, Red Flags is a way that we can all work together to reduce the prevalence and severity of identity theft.

Kevin Prince
Chief Technology Officer
Perimeter eSecurity
KPrince@perimeterusa.com

ABOUT THE AUTHOR

Named Chief Technology Officer of Perimeter in 2009, Kevin Prince spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise.

With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk. Mr. Prince has trained federal examiners for several years.

ABOUT PERIMETER ESECURITY

Perimeter is the trusted market leader of information security services that delivers enterprise-class protection and compliance for businesses of any size. Through its cost-effective security-as-a-software platform, Perimeter offers the most comprehensive compliance, security and messaging services that include but aren't limited to: hosted email, encrypted email, firewall management and monitoring, vulnerability scanning, host intrusion and prevention, email antivirus and spam, remote data backup and email archiving.

As companies struggle with the increasing cost, complexity and stringent compliance requirements associated with their information intensive businesses, Perimeter is the only provider that can simultaneously reduce the cost, manage all of the complexity and meet all of the compliance requirements from a single platform.

Headquartered in Milford, CT, with seven geographically distributed technical operations centers and three redundant datacenters, Perimeter's on demand services, which are offered both on a Network (in-the-cloud) and CPE (customer-provided equipment) basis, are validated by TruSecure and guaranteed for current and future regulatory compliance. If you would like to speak with us or view a product demo, please don't hesitate to call at 800.234.2175 Option #2 or visit our web site at www.PerimeterUSA.com.