



# RED FLAGS RULE

## Are You Ready for June 1st?



### RECOMMENDED RED FLAGS COMPLIANCE SOLUTIONS

- ▶ Host & Network Intrusion Detection and Prevention
- ▶ E-Security Awareness Training
- ▶ Managed Firewall
- ▶ Web Content Filtering
- ▶ Email Content Filtering
- ▶ Spam Filtering
- ▶ Email Anti-Virus
- ▶ Remote Data Backup
- ▶ Policy Compliance Audit
- ▶ Internal & External Vulnerability Assessments
- ▶ Consulting Services

Call Us Toll Free: 800.234.2175

**C W S D** Sales Sheet

### WHAT WILL HAPPEN ON JUNE 1<sup>ST</sup>?

This is the date when the Federal Trade Commission will finally start to enforce the Identity Theft Red Flags Rule, for which federally-regulated banks and credit unions have been tested for compliance since Nov. 1<sup>st</sup> of 2008. The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs - or "red flags" - of identity theft in their day-to-day operations.

### WHO IS IMPACTED?

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. A creditor is broadly described as anyone who defers payment on a debt, or anyone who defers payment on goods or services. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. But creditors do include organizations such as finance companies, healthcare organizations, automobile dealers, mortgage brokers, utility companies and telecommunications companies.

### WHEN WILL THE CHANGES OCCUR?

By identifying red flags in advance, you'll be better equipped to spot suspicious activity or a "Red Flag" before it turns into a costly case of identity theft.

### STEPS TO PREPARE FOR RED FLAGS RULE INCLUDE:

Key Features	Benefits
Develop & execute a more detailed information security program specific to preventing, identifying & mitigating "red flags"	Perimeter E-Security has created solutions built specifically to address the FTC, FFIEC, SEC, FINRA, Sarbanes-Oxley and GLBA requirements around secure messaging and compliance. We guarantee you will be compliant!
Required staff training	<b>Perimeter's E-Security Training Courses</b> help your business meet state, federal or standards body compliance requirements. Perimeter can better prepare your staff for the growing challenges of protecting customer and network privacy while reducing the threat of identity theft.
Conduct regular vulnerability testing	<b>Perimeter's Monthly Remote Network Assessment ("MRNA")</b> tests the effectiveness of your internal and external network security controls and identify associated weaknesses before malicious activity can take place.
Written procedures for responding to and communicating information on a data security breach	<b>Perimeter E-Security Consulting:</b> Perimeter offers a team of security experts. Our experts will meet with you regularly to discuss your network security concerns and recommend services to meet your needs.
Increased record keeping for policies and procedures	Through <b>ViewPoint</b> , our online portal, you can access information securely, 24/7. Reports are focused with an audit mindset, and executive summaries allow for easy interpretation by senior management.