

CS Week Bulletin

Brought to you by *Electric Light & Power*

COMPLYING WITH RED FLAG RULES: A RECIPE FOR UTILITY COMPANY SUCCESS

By Thomas Oscherwitz, ID Analytics Inc.

December 2, 2008

As if businesses aren't dealing with enough change, utility companies are about to encounter a regulation they might not even know about. It's called the Red Flag Rules, and companies that issue credit—including those in the utilities space—must comply by May 1, 2009. This date may seem far off, but companies must develop programs now to avoid Federal Trade Commission penalties for noncompliance next year.

The FTC takes this regulation so seriously that it delayed the original Nov. 1 deadline until next spring to give utility companies and other creditors more time to implement written identity-theft prevention programs.

Don't think the new regulations won't affect utility companies. They will. By May 1, utilities that have continuing credit relationships with customers—e.g., flat rate or deferred monthly billing—must comply. Given the enforcement delay, utility companies should expect the FTC to have zero tolerance for noncompliance.

For the first time, utility companies will have enterprise wide responsibility to address identity-theft risks. These businesses must address identity-theft risks through every channel used to communicate with consumers and with every type of customer credit account they maintain. In addition, companies must develop solutions to resolve the risks and keep their anti-fraud measures current as fraudsters' schemes evolve. For instance, if a utility company signs up a customer for a new account, that company is responsible for flagging any potential indicators of identity fraud and having a system to deal with them. The scope of these rules is daunting. To avoid compliance pitfalls, utility companies should follow these principles:

- Compliance starts at home. Companies cannot simply plug in a vendor compliance solution and expect that they've met the rules. Companies must do a self-assessment to uncover their own identity-theft risks.
- Start now, don't wait. Completing a meaningful risk assessment can't be done properly a week before the compliance deadline. If you're already behind, don't wait any longer. Start today.
- Take credit for what you're already doing. Many companies use fraud-prevention systems that can satisfy many Red Flag requirements.
- Companies are accountable for identity theft that happens on their watch. Data security has gone beyond protecting against corporate vulnerabilities and includes ensuring the identity security of customers.
- Build a Red Flag program for the long term. Compliance systems must evolve with ever-changing fraud threats. Regulators expect companies to have programs that can be regularly updated.
- Resolve risks. Companies must not only identify risks; they must also resolve them as cost effectively as possible.
- Design a program sensitive to business processes. Poorly drafted compliance programs can interfere with the customer experience and slow business processes.

- Yes, you should care. Companies that fail to comply will face penalties and other enforcement actions. Naiveté is not an excuse.

While Red Flag Rules give companies flexibility in designing their own anti-fraud programs, companies must be able to demonstrate that they work. To do this, companies should avoid systems that rely solely on manual flag reviews; test analytical tools to ensure they can resolve flags in an operational environment; and design Red Flag programs so they can be easily updated.

For more information on Red Flag Rules and compliance, visit <http://www.idanalytics.com/solutions/compliance.html>.