

WATCH OUT FOR RED FLAG RULES

By Thomas Oscherwitz
WirelessWeek - October 27, 2008

As if the wireless industry isn't dealing with enough change these days, companies in this space are about to face a new regulation that some of them may not even know about. They are called the [Red Flag Rules](#), and companies that issue credit—including those in the wireless space—will need to be compliant by Nov. 1, 2008.

The Federal Trade Commission (FTC), the federal bank regulatory agencies and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring companies to implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must provide for the identification, detection and response to patterns, practices or specific activities – known as “red flags” – that could indicate identity theft.

Although these rules may have been issued without much fanfare, don't let this trick you into thinking the new regulations won't affect your company; they will, and your company will need to comply. By Nov. 1, any time a wireless carrier opens or manages an account for a customer that involves multiple payments—e.g., a 1- or 2-year membership plan—it will need to be in compliance with these major new Federal regulations.

For the first time, wireless companies will now have enterprise-wide responsibilities to address identity theft risks. These businesses must address identity theft risks through every channel they 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 up-to-date as fraudsters' schemes evolve.

For instance, if a wireless carrier signs up a customer for a new account, that wireless carrier is responsible for flagging any potential indicators of identity fraud and then having a system in place to deal with them.

Understandably, the scope of these rules is daunting. To avoid compliance pitfalls, wireless companies should keep the following principles in mind:

1. **Compliance starts at home:** Companies cannot simply paste a vendor compliance solution and expect that they've met the rules. Companies must do a self-assessment of unique identity theft risks.
2. **Start now, don't wait:** Doing a meaningful risk-assessment takes some time and can't be completed properly a week before the compliance deadline. If you're already behind, don't wait any longer. Start today.
3. **Take credit for what you are already doing:** Many companies have fraud prevention systems in place that can satisfy many of the Red Flag requirements.



Oscherwitz: *The compliance date is Nov. 1.*

4. **Companies are now accountable for the identity theft that happens on their watch:** Data security has gone beyond protecting against corporate vulnerabilities and includes ensuring the identity security of customers.

5. **Build a Red Flag program for the long-term:** Compliance systems must evolve along with ever-changing fraud threats. Regulators expect companies to have programs that can be regularly updated.

6. **Resolving Risks:** Companies must not only identify risks, they also must resolve them—as cost effectively as possible.

7. **Design a program sensitive to business processes:** Poorly drafted compliance programs can interfere with the customer experience, and slow business processes.

8. **Yes, you should care:** Companies that fail to comply face penalties and other enforcement actions. Naiveté is not an excuse for non-compliance.

At the end of the day, while Red Flag Rules give companies extraordinary 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 their analytical tools to ensure they can actually resolve flags in an operational environment; and design Red Flag programs so they can be easily updated.

Keeping the above principles in mind will point all wireless companies in the right direction.

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

Oscherwitz is vice president of government affairs and chief privacy officer for ID Analytics.