



COMPLY WITH RED FLAG RULES

Tom Oscherwitz, chief privacy officer/VP of government affairs, ID Analytics
September 01 2008

By Nov. 1, creditors must comply with Federal Red Flag rules designed to combat identity fraud. Banks and credit issuers will be impacted, as will those unaccustomed to regulations. Some organizations face uncertainty with compliance programs. To avoid pitfalls, remember these principles.

First, companies are accountable for ID theft on their watch. These rules change creditor's roles in combating ID theft. ID management practices are requirements, as a result.

Second, compliance starts at home. Companies must look at unique risks and not assume the rules are met. Self-assessment is critical.

It's also imperative to start now. Doing risk assessment takes time (and once done, take credit for what you're doing). As well, it's important to build a long-term program and enact a system that evolves with fraudster threats. Regulators expect a flexible program.

Resolving risks is another priority. Red Flag rules require companies to not only identify risks, but address and resolve them.

It's also vital to design a program sensitive to business processes. Poorly drafted compliance programs interfere with customer experience and slow business processes.

You should care about these matters because companies that fail to comply face penalties and other enforcements.

So, viable Red Flag programs must: identify relevant ID theft risks, detect flags during operations, resolve detected flags, and evolve with changing risks.

Red Flag rules give flexibility. The price is that companies must design anti-fraud programs that demonstrably work.

Tom Oscherwitz is chief privacy officer/VP of government affairs, ID Analytics.