
Red Flag Rules: An 800 Pound Gorilla?

Being exempt from Red Flag legislation doesn't mean exemption from exposure!

You may be thinking that the headline is a bit of a misnomer. How can something like Red Flag Rules, which many people are talking about, be the proverbial 800 pound gorilla in the room? The problem is not who is talking about Red Flag Rules, but who is NOT talking about Red Flag Rules. Companies that find themselves subject to the rules have no doubt spent time developing procedures to meet compliance requirements, while companies that are not subject have most likely moved on to other business issues. Unfortunately, the Red Flag Rules are important for those companies who are not subject to them and the exposure cannot be ignored any longer.

To summarize, the Red Flag Rules, which will be implemented 6/1/10, affect health care providers, financial institutions, auto dealers, and anyone else classified as a "creditor" or "service provider" with "covered accounts." Keep in mind these terms are defined by the law itself and may fall outside of the "common law" usage. Please consult the legislation or your attorney if you are unsure if you are subject to the Rules. Those affected are required to develop and implement a written "Identity Theft Program" to detect, prevent, and mitigate identity theft. Essentially, the FTC has turned good risk management practices into law (and attached a fine for non-compliance!). Unfortunately, many companies who are not subject to the rules will ignore the effective risk management practices outlined in the law. Even though these companies will not be fined for ignoring risk management, it does not make good business sense to ignore an exposure to loss.

While the Red Flag Rules outline a comprehensive guide to detecting and mitigating privacy losses, they fail to address the vital role insurance can serve in protecting your company's assets. In general, most Commercial General Liability policies (CGL) offer little coverage for security and privacy breaches resulting in lost information. At one time the CGL would provide broad coverage, but now a specialized policy like Cyber or Privacy Liability is most often needed. An example of a covered loss on a specialized policy is theft of confidential customer information such as names and social security numbers that are stored in a company's database or file cabinets. The related expenses incurred in notifying those customers about the breach, which is often required by law, can be covered as well. Without the proper policy, a company can be financially burdened paying these losses out of pocket.

Hopefully the best thing to come out of the Red Flag Rules implementation will be a renewed focus on Cyber and Privacy Liability by all companies. Just because the Red Flag Rules do not apply to your organization does not mean that the exposure to loss does not apply. While the rules may be new, the exposure is anything but new. As technology has become an integral part of most business, more and more companies have become exposed to loss. And, as consumers continue to become more aware of their rights when their privacy is breached, it becomes extremely important that companies take the steps to protect themselves. Talk to a professional; get rid of the 800 pound gorilla in your office.

*– Dustin DeJarnette, CIC and ARM
Commercial Compliance Specialist*