

FTC Grapples with Endless Red Flag Problems

By Bridgette C. Roman

The goal was laudable: requiring businesses in the position to detect and prevent identity theft to implement procedures to identify it and take steps to mitigate it. The need was real: \$48 Billion Dollars in 2008 was lost due to identity theft. The execution: Well, in the words of Buffy the Vampire Slayer, “not so much.”

The Red Flag plague has its genesis in the vague terminology that runs rampant through the rules. Broad and ill-defined terms such as “covered account,” “transaction account” and “creditor,” have placed a Girl Scout troop that defers payment for a cookie order until the time the cookies are delivered at risk of being a “creditor” and the cookie order a “transaction account.” The legal community has not been spared. The most recent delay in the implementation of the Red Flag Rules may have arisen in part because the President of the American Bar Association made clear that unless the Federal Trade Commission exempted attorneys from the Red Flag Rules, a declaratory judgment action would follow.

These seemingly endless vagaries, and presumably the FTC’s desire to clarify them before making the rules effective, have led to mounting frustration with the FTC and the Red Flag Rules. The deadline for implementation of required identity theft prevention programs has shifted more times than the San Andreas Fault. The most recent extension occurred on July 29, just three days before the deadline of August 1. The newly established deadline is November 1, 2009. One published comment exemplifies the aggravation at the ever-shifting deadline:

It is actually laughable that the FTC sets guidelines and mandates and continuously changes them at the last minute. It is insulting and harmful to companies that try to meet the compliance guidelines and it rewards companies that have failed to meet the mandate. How are companies supposed to believe that the next deadline is any more realistic than the last? If I was a non-compliant company after the next proposed deadline I would argue that the deadline has been postponed so many times that no reasonable company could determine the validity of the newest enforcement date; therefore, I should not be subject to any real fines or regulatory action. Maybe the FTC should start reading parenting books for guidance on how to deal with establishing credibility in enforcement of rules. [Red Flag Forum on Linked In, posted July 31, 2009]

The foundation of the Red Flag Rules rests on Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”), 15 U.S.C. §1681 et seq. A group of six federal agencies then promulgated regulation to carry out these statutory provisions.

The “final” regulations were published on November 9, 2007, but the effective date has been the subject of recurring delays. The rules require the following:

- Each “financial institution” and “creditor” that holds a “covered account”¹ shall develop and implement an identity theft prevention program designed to prevent, detect and mitigate

identity theft in connection with new or existing accounts. This involves

- Identifying and incorporating into the program certain patterns, practices and forms of activities that are “red flags” signaling possible identity theft. In large measure companies are to audit their own experiences and build their program on those experiences.

- Once determined, the business is then required to develop policies and procedures to detect their pre-identified “red flags” on an on-going basis.

- The business then must appropriately respond to any “red flags” detected in order to prevent and mitigate identity theft.

- Then, periodically assess the effectiveness of and update the program to reflect changes in customer risk.

- Oversight by the company’s board of directors (or committee thereof) and reporting to the board.

- Training of staff on the rules.

- Issuers of credit or debit cards must develop policies and procedures to assess the validity of certain address change requests.

- Users of consumer credit reports must develop policies and procedures to respond to notices from credit reporting agencies regarding address discrepancies.

The very broad reach of these rules requires that every business make a determination as to whether they are a “creditor” with “covered accounts.” Given the concerns raised by the ABA that client accounts with their attorneys fall within these definitions, one cannot take lightly the question as to whether they are a “creditor” with “covered accounts.” The current deadline for enforcement gives ample opportunity for even the stragglers to assess the risk areas for identity theft and implement the required program.

¹ Due to space limitations here, the reader is directed to 15 U.S.C. §1681 et seq. and 12 CFR 14.90 for the definitions of these terms.



broman@checksmart.com

*Bridgette C. Roman,
Vice President & General Counsel,
Checksmart Financial Company*

