FTC RED FLAGS RULE

History

The Red Flags Rule was developed pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under the Rule, financial **institutions and creditors** with **covered accounts** must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

- Mandatory compliance was to begin on November 1, 2008.

- Enforcement of the new "Red Flags Rule" suspended until **May 1, 2009.**

Colleges & Universities

- The Red Flags Rule defines the terms "creditor" and "covered accounts" broadly.
- A "creditor" under the Red Flags Rule includes any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month.
- Although the FTC, in many contexts, does not have jurisdiction over not-for-profit entities, it has taken the position that not-for-profits are subject to FTC jurisdiction when they engage in activities in which a for-profit entity would also engage. In its July 2008 guidance, the FTC stated "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

Activities that could cause colleges and universities to be considered "creditors" under the Red Flags Rule may include, for instance:

- participating in the Federal Perkins Loan program,
- participating as a school lender in the Federal Family Education Loan Program,
- offering institutional loans to students, faculty, or staff, or
- offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

Steps to be Taken by Universities Covered by the Red Flags Rule

Under the rule, creditors that hold covered accounts must develop an identity theft prevention program that includes reasonable policies and procedures to detect or mitigate identity theft and enable a creditor to:

- identify relevant "red flags" (patterns, practices, and specific activities that signal possible identity theft) and incorporate them into the program;
- detect the red flags that the program incorporates;
- respond appropriately to detected red flags to prevent and mitigate identity theft; and
- ensure that the Program is updated periodically to reflect changes in risks.

Closing Thoughts:

- The Red Flags Rule provides the opportunity for financial institutions and creditors to design and implement a program that is appropriate to their size and complexity.
- Many (most?) Universities have not yet addressed this issue.
- FTC may impose civil money penalties (up to $2,500 per violation) for knowing violations of the rule that constitute a pattern or practice

Red Flag Rules are similar to FERPA, HIPAA, Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry (PCI) Data Security Requirements.

The RTC Red Flag Rules would seem to fall under the Information Security Policy 01.10

While MSU has an information security program, it is probably insufficient to address Red Flag Rules without modification.