Identity Theft "Red Flags Rule" – November 1 Compliance Date Nears

By Elizabeth B. Meers and Daniel S. Meade

Late last year, the Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the Red Flags Rule [link to Nov 9 2007 FTC rule in FR Update] intended to reduce the risk of identify theft. Mandatory compliance with the Red Flags Rule for "creditors" or "financial institutions" that provide "covered accounts" begins on November 1, 2008. Parts of the rule likely cover many colleges and universities, and as discussed below, the FTC has stated that nonprofit and government entities can be subject to parts of the rule. Institutions should consult with their legal counsel on applicability of the rule and should consider establishing a security program consistent with it.

Background on Red Flags Rule

The FTC issued the Red Flags Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act), which amended the Fair Credit Reporting Act (FCRA). The rule requires "financial institutions" and "creditors" that hold "covered accounts" to develop and implement an "Identity Theft Prevention Program" for new and existing accounts.

The Red Flags Rule is actually three different, but related rules, one or two of which apply to many colleges and universities:

> (1) Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. *(This provision is likely not applicable to colleges and universities, because, as discussed in the preamble to the Red Flags Rule, the definition of "debit card" specifically does not include stored value cards. However, this provision could implicate student ID's that also can be used as part of a national debit card network, such as Visa or MasterCard.)*
>
> (2) Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency. *(This provision applies to colleges and universities when they use consumer reports to conduct credit or background checks on prospective employees or applicants for credit.)*
>
> (3) Financial institutions and creditors holding "covered accounts" must develop and implement a written Identity Theft Prevention Program for both new and existing accounts. (*This provision likely applies to many colleges and universities*).

Application of Red Flags Rule to Colleges and Universities as Creditors
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 [instead of footnote hyperlink to doc], the FTC stated "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."[1]

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.

Under the rule, if an institution is a creditor, the institution must determine if any of its extensions of credit are "covered accounts." Basically, a covered account is a consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly. The Red Flags Rule and the FTC's guidance on it indicate that covered accounts include certain types of arrangements in which an individual establishes a "continuing relationship" with the enterprise, including billing for previous services rendered. Certain payment arrangements, such as payment of tuition in full at the beginning of each semester either by the student's family or through a third-party student loan provider, likely does not meet the "continuing relationship" standard in the "covered account" definition. Any type of account or payment plan that involves multiple transactions or multiple payments in arrears, however, likely is a "covered account."

Steps to be Taken by Colleges and 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;

[1] *See* "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft", available at http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

- 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.

The board of directors (or appropriate board committee) must approve the initial written Program. Board approval may be necessary only for the first written Program if the board delegates to appropriate senior management further responsibility. If an institution has not yet done so, it should promptly develop an Identity Theft Prevention Program for board (or board committee) approval, as the Red Flags Rule goes into effect November 1, 2008.

Content of Identity Theft Prevention Program

The Red Flags Rule allows for flexibility in the scope of the Identity Theft Prevention Program, depending on the creditors' activities and level of identity theft risk associated with the relevant covered accounts. In developing Identity Theft Prevention Programs, institutions should assess whether they have "covered accounts." This analysis and an initial risk assessment will enable the financial institution or creditor to identify accounts the Program must address and identify the risks the institution faces, based in large part on the institution's previous experiences with identity theft. The FTC has stated this risk-based approach will enable organizations to tailor their Programs appropriately. An appropriate Identity Theft Prevention Program may not need to be detailed or complex, but should be written, duly approved, and implemented.

Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation [link to Guidelines doc], published as an appendix to the Red Flags Rule, provides an outline for developing a Program. In a supplement to the guidance, the FTC and federal banking regulators identified 26 "red flags" that may be useful to incorporate into an Identity Theft Prevention Program. Examples include:

- address discrepancy

- name discrepancy on identification and insurance information

- presentation of suspicious documents

- personal information inconsistent with information already on file

- unusual use or suspicious activity related to a covered account, and/or

- notice from customers, law enforcement or others of unusual activity related to that covered account.

In addition to addressing relevant "red flags," an institution covered by the Red Flags Rule must "train staff, as necessary" to implement the Identity Theft Prevention Program effectively. According to the preamble to the rule, institutions need train only "relevant staff" and only insofar as necessary to supplement other training programs.

The institution must also exercise "appropriate and effective oversight" of service provider arrangements. According to the preamble to the rule, this provision is intended to remind creditors and financial institutions that they remain responsible for compliance with the rule even if they outsource operations to a third party. The provision is also intended, however, to provide "maximum flexibility" to creditors and financial institutions in managing their service provider arrangements. Thus, a service provider that provides services to multiple creditors and financial institutions may do so in accordance with its own identity theft prevention program, as long as that program complies with the rule. Among other steps, a creditor or financial institution could require a service provider by contract to have policies and procedures to comply with the rule.

Application of Red Flags Rule to "Financial Institutions"

The Red Flags Rule also applies to "financial institutions," generally defined as banks, thrifts, credit unions, and other institutions that offer transaction accounts.[2] Colleges and universities that offer students the option of having their student ID also operate as a Visa or MasterCard debit card should coordinate with the bank through which such services are offered to ensure that the bank has an adequate Identity Theft Prevention Program in place.

FTC Enforcement

Under the FCRA, the FTC may impose civil money penalties (up to $2,500 per violation) for knowing violations of the rule that constitute a pattern or practice. If the FTC finds violations of the rule to be unfair and deceptive, the FTC may also use its adjudicatory authority to issue cease and desist orders and other enforcement actions. Although there is no private right of action for noncompliance with the Red Flags Rule under the FCRA, victims of identity theft may be able to bring claims under other theories of liability such as private torts.

Conclusion

Many colleges and universities currently have procedures in place to flag some address discrepancies or other "red flags." The Red Flags Rule requires covered institutions to systematize these procedures, and develop a written plan, approved by the board of directors or equivalent, by November 1, 2008.

***

Elizabeth Meers is a partner and Daniel Meade is an associate at Hogan & Hartson, LLP, and practice in its Education and Financial Institutions groups, respectively.

[2] A transaction account is a deposit or other account from which the account holder may make payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts. See 12 U.S.C. § 461(b)(1)(C).