
Volume Six
Number Three
June 2009
Bimonthly

Meet

## Martin T. Biegelman

**Director, Financial Integrity Unit, Microsoft Corporation and**

## Daniel R. Biegelman

**Attorney-at-Law and Author**

PAGE 16

## Earn CEU Credit

VISIT: WWW.CORPORATECOMPLIANCE.ORG/QUIZ

OR SEE PAGE 11

## When the government calls: Corporate response to an inquiry

PAGE 20

*Special Issue!*

## Compliance & Ethics Institute

www.complianceethicsinstitute.org
September 13–16, 2009 | Las Vegas, NV

ALSO:

## College and university compliance with the FTC's Red Flag Rules

PAGE 34

# College and university compliance with the FTC's Red Flag Rules

***By Robert F. Roach, JD, CCEP, CHRC, CFE and Dorothy Murphy, Esq.***

*Editor's Note: Robert Roach is the University Compliance Officer at New York University, where he oversees the University's ethics and compliance program. He may be reached by e-mail at robert.roach@nyu.edu.*
*Dorothy Murphy is a New York-based corporate attorney currently engaged in legal research consulting and specializing in the area of data protection and privacy. She may be contacted by e-mail at dmurphyesq@optonline.net.*

In 2003, the US Congress sought to provide consumers with further protection from identity theft by enacting the Fair and Accurate Credit Act (FACTA), which amended the earlier Fair Credit Reporting Act (FCRA). FACTA directed the Federal Trade Commission (FTC) to issue regulations, now generally referred to as the Red Flag Rules (Rules), which require financial institutions and creditors to adopt policies and procedures that protect consumers from identity theft.

Not-for-profit institutions, such as most colleges and universities, are not generally subject to the enforcement jurisdiction of FTC. However, FTC has interpreted its jurisdiction to cover not-for-profits when they engage in activities that, if undertaken by a for-profit entity, would be subject to FTC jurisdiction. Accordingly, colleges and universities should become familiar with the Rules and, if they conduct activities covered by them, should institute policies and procedures to assure their institution's compliance.

College and university compliance officers should review the three relevant sections of the FTC regulations and evaluate their institution's activities to determine the applicability of the Rules to their organization. They can develop an effective compliance program following some of the practical suggestions offered below.

## The Red Flag Rules

In 2007, the FTC issued the Rules, which were intended to regulate the practices of financial and banking institutions and creditors. Effective compliance with the Rules requires a brief review of three regulations, each having a different scope as set forth in the following sections:

1. Users of consumer reports (16 C.F.R. § 681.1)
2. Financial institutions and creditors (16 C.F.R. § 681.2) and
3. Issuers of debit or credit cards (16 C.F.R. § 681.3)

**Users of consumer credit reports**

Many colleges and universities use consumer credit reports that are issued by a consumer reporting agency for purposes permitted under FCRA, such as employment or credit analysis. An institution that uses these consumer credit reports must establish policies and procedures that enable it to verify the identity of the subject of the report if the institution is notified by the consumer reporting agency that there is a discrepancy between the subject's address in the agency's records and the address that the subject provided to the institution.

Accordingly, college and university compliance officers should enquire whether their institutions use consumer credit reports and to what extent. Most typically, these reports are used by Human Resource departments when they conduct background screening for new faculty and staff and by Admissions and Financial Aid departments.

**Financial institutions and creditors**

Under the Rules, a financial institution or creditor who offers or maintains one or more covered accounts, must develop and implement a written identity theft prevention program that will identify, detect, prevent, and mitigate damages resulting from identity theft in connection with a covered account.

For purposes of this component of the Rules, a "creditor" is defined under FCRA as

> … [any] person who *regularly* extends, renews, or continues *credit*; any person who regularly arranges for the extension, renewal or continuation of credit; as any assignees of an original creditor who participates in the decision to extend, renew or continue credit. (Emphasis added) [15 U.S.C.A. §1691(a)(e)].

The term "credit" is defined as "… [the] right granted by a creditor to a debtor to defer payment or to incur debts and defer payment or to purchase property or services and defer payment therefore." [15 U.S.C.A. § 1691 (a)(d)].

"Covered accounts" are accounts "… [established] primarily for personal, family or household purposes that involve or

are designed to permit multiple payments of transactions, i.e. consumer accounts."

Such accounts specifically include transaction and credit accounts, "… [Or] any other accounts for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft." Under the Rules, identity theft prevention programs are only required for these covered accounts.

Colleges and Universities frequently engage in activities that qualify them as creditors with covered accounts for purposes of the Rules. These activities include student lending activities under either the Federal Perkins Loan Program or the Federal Family Education Loan Program. Additionally, any university that extends credit to students or their parents in the form of deferred tuition payments, or provides any services in advance of payment, or provides loans to faculty or staff that require multiple installment-type repayments will also be required by the Rules to establish an identity theft prevention program.

## Duties of card issuers regarding changes of address

Section 16 C.F.R. § 681.3 applies to creditors, as defined above, who issue debit or credit cards to consumers. The requirements state that a card issuer must establish and implement reasonable policies and procedures for validation of a change of address request from the consumer when there is a subsequent request from same consumer for an additional or replacement card.

Some colleges and universities issues identity cards that are also "stored value cards" on which students may store a cash value and use the card to make purchases in campus stores and food service facilities. Other colleges and universities issue identity cards that are also traditional debit cards that allow access to "transaction accounts," typically in conjunction with local banking institutions. A transaction account is an account that allows a depositor or account holder to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments to third parties or others.

Although stored value cards, as described above, are not covered by the Rules, if a college or university issues a debit card that allows access to a transaction account, under the Rules, it will have to establish reasonable policies and procedures to assess the validity of changes in account addresses and subsequent requests for additional or replacement cards.

## Compliance procedures

A college or university whose activities are subject to the Rules will need to develop an identity theft prevention program. It should be noted, however, that the program may be tailored to the institution's size, complexity, and nature of its operation. Although the program should be reflected in written policies and procedures, it need not be detailed or complex. Rather, the program should be based upon the institution's previous experience with identity theft associated with relevant covered accounts.

An appendix to the Rules provides guidelines for developing a program along with 26 potential red flags of identity theft. An effective program will contain mechanisms for the:

- identification of identity theft Red Flags applicable to the type of credit extended;
- detection of such Red Flags;
- prevention of theft, and
- mitigation of damages to the consumer.

For programs that respond to address discrepancies related to consumer credit reports, two sets of policies and procedures should be developed, neither of which is extraordinary or burdensome to the user:
(1) policies and procedures to help ensure that the person about whom a report is requested is the same as the subject of the report provided by the consumer reporting agency; and
(2) policies and procedures to provide the verified address of the subject back to the consumer reporting agency.

The program developed by a college or university must be approved by the institution's board of trustees or an appropriate committee of the board. Senior management must be engaged in the development, implementation, and oversight of the program, including regular monitoring and updating of the program, as appropriate. ■

*The views expressed herein are the authors' own and do not necessarily represent the views of New York University.*