Advisory

MARCH 2009

celebrating 75 years

WIGGIN AND DANA

founded 1934

Compliance with New Laws on Identity Theft and Protecting Personal Information

This advisory provides information about a federal regulation that the Federal Trade Commission (the "FTC') will begin enforcing on May 1, 2009, and about a recent Connecticut data privacy statute, both of which will likely affect colleges and universities. Both laws require individuals and institutions that handle personal information to adopt certain policies and procedures and impose civil fines for non-compliance.

I. THE "RED FLAGS RULE"

On November 9, 2007, the Federal Trade Commission (the "FTC'), in coordination with several other federal agencies, issued the Red Flags Rule (the "Rule") in an effort to prompt the adoption of policies and procedures concerning identity theft. While the Rule became effective on November 1, 2008, the FTC has announced that it will not enforce compliance until May 1, 2009. Thus, any institution subject to the Rule will need to adopt appropriate policies and procedures by May 1.

Who must comply?

The rule likely applies to colleges and universities, because it applies to any "creditor" that has a "covered account," and those terms are broadly defined. The FTC has also indicated in informal guidance that it considers those who provide services in exchange for future or deferred payment to be creditors. A college or university must comply with the Rule if it: (1) offers credit or permits deferred payment, (2) for the purpose of selling products or services for personal, family, household, or business use, (3) to a person with which the institution has a continuing relationship. Thus, colleges and universities that extend credit to students through student loan programs or offer tuition payment plans likely must comply with the Rule.

What is required?

Colleges and universities that are subject to the Rule must prepare and implement a written "Identity Theft Prevention Program" (the "Program") to detect, prevent, and mitigate identity theft when they open or maintain accounts covered by the Rule. The content and scope of the Program must be tailored to the school implementing it, taking into consideration its particular risks, size, and the nature of its activities.

The Program must be approved by the school's Board of Directors (or a committee thereof), implemented with training for appropriate staff, and periodically updated. The Board or one of its committees must assign specific responsibility for overseeing the Program to an employee in senior management. In addition, colleges and universities that are subject to the Rule must require their subcontractors and vendors who deal with the school's covered accounts to comply with the school's identity theft Program. At least annually, the school must provide the Board (or a committee thereof) with a report on the Program.

It is advisable to review your draft identity theft prevention program with your counsel to ensure compliance with the Red Flags Rule.

What are red flags?

Red flags are items of information that suggest the possibility of identity theft. Examples of red flags are:

- a warning from a reporting agency that a fraud alert exists in a consumer's file;
- documents provided by a consumer that appear to be forged or fake;
- information provided by a consumer that is internally inconsistent; and
- mail sent to an address for an active consumer that is returned undeliverable.

There are suggested red flags in the appendix to the Rule. The FTC encourages institutions developing a Program to be creative and identify other possible red flags.

What must be done once a red flag is detected?

If a school identifies a red flag in a transaction with a person opening or holding a covered account, that school must take appropriate steps to respond. The FTC has advised that an appropriate response depends upon the nature of the red flag detected. The response could require conducting an internal investigation to determine whether the red flag was an administrative error, contacting law enforcement authorities, or waiting to provide credit until an investigation reasonably confirms the applicant's identity. The Rule requires that the institution respond in an appropriate manner under the circumstances to address the risks posed.

How will the Rule be enforced?

As mentioned above, the FTC will begin enforcing the Rule as of May 1, 2009. The Connecticut Attorney General also has enforcement authority under the Rule. The Rule provides for penalties of up to $2500 per violation, but it is not yet clear what the FTC will consider to be a violation. Informal guidance from FTC staff suggests that, at a minimum, a covered school that completely fails to adopt and implement the required identity theft prevention program, or fails to make a good faith effort to adopt and implement such a program, will be found in violation of the Rule.

II. CONNECTICUT PUBLIC ACT NO. 08-167: AN ACT CONCERNING THE CONFIDENTIALITY OF SOCIAL SECURITY NUMBERS

A 2008 Connecticut statute governing the handling of Social Security numbers ("SSNs") and other personal information may also affect colleges and universities in the state. Effective October 1, 2008, Public Act No. 08-167, codified as section 42-471 of the Connecticut General Statutes, requires any person or business that collects or possesses "personal information" to (1) safeguard the information from misuse by third parties, (2) ensure proper disposal of the information, and (3) adopt and make public a policy that specifically addresses the protection of SSNs.

"Personal information" is defined as information, whether in paper, electronic, or other form, that is capable of being associated with a particular individual through one or more identifiers, such as a SSN, driver's license number, state identification card number, account number, credit or debit card number, or other identifying number. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

The Act imposes a civil penalty of $500 for each violation, with a cap of $500,000 for any single event. No fine is imposed, however, for unintentional violations.

The Act supplements section 42-470 of the Connecticut General Statutes, which also deals with SSNs. That law prohibits any individual or entity from using an individual's SSN in any of the following ways: publicly displaying it; printing it on a card required to access products or services; requiring transmission of SSNs over the Internet, unless via a secure connection or encrypted; and requiring SSNs to access a website, unless a password or unique personal identification number or other "authentication device" is also required to access the site.

As an employer, colleges and universities generally collect SSNs (and other personally-identifiable information) about their employees. Also, colleges and universities typically maintain similar information about students, and possibly parents (for example, in connection with financial aid). As a result of these activities, most colleges and universities likely are required to comply with the Connecticut privacy laws described above.

If your institution is not already in compliance, it should assess the types of information collected that are covered by these state laws and confirm that it is properly obtained, stored, and destroyed when it is no longer needed. There should also be a policy, posted on the school's website or otherwise made public, that specifically addresses the protection of SSNs maintained by the school.

If you have any questions or want guidance in your compliance efforts, please contact: Aaron S. Bayer at 860.297.3759 or abayer@wiggin.com or Sabrina Houlton at 203.498.4342 or shoulton@wiggin.com