Albany Law School

Red Flag Rule – Identity Theft Prevention Program

BACKGROUND

Final rules implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 were issued by the Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration ("NCUA"). A joint notice of final rulemaking was published in the Federal Register (72 FR 63718) finalizing *The Identity Theft Red Flag Rule* ("the Rule"). The Rule was issued with the underlying goal of detecting, preventing, and mitigating identity theft "in connection with the opening of certain accounts or existing accounts," referred to as "*covered accounts*."

Red Flags are defined by the Rule as "a pattern, practice or specific activity that indicates the possible existence of identity theft." Examples of "Red Flag" incidents include presentation of suspicious identity documents or frequent address changes.

The law requires that a written Identity Theft Prevention Program be approved by either the organization's governing board or a committee of the board.

This Program is to be considered in tandem with all other data security and privacy policies in place at the Law School.

DEFINITIONS APPLICABLE TO THIS PROGRAM

- Identity theft - a "fraud committed or attempted using the identifying information of another person without authority."
- Red Flag - a "pattern, practice, or specific activity that indicates the possible existence of identity theft."
- Covered Account –an account that a creditor holds that is designed to allow multiple payments or transactions, and will include all student accounts or loans that are administered by the Law School.
- Program Administrator - the individual designated with primary responsibility for oversight of the Program.
- Identifying information - "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

IMPLICATIONS FOR ALBANY LAW SCHOOL

This Program is intended to contain reasonable policies and procedures for Law School personnel to:

1. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from Identity Theft.

The Law School is impacted by the Rule in the following areas of operation (areas which may involve the creation or maintenance of Covered Accounts):

- Student tuition and fee payment plans
- The Federal Perkins Loan program
- The Trustee Loan program
- Bookstore advances
- Human Resources – benefits portal and requests for payroll/employee data

- Financial Aid – document verification and third party (UAS and collection agencies) compliance with Red Flag rules
- Registrar – requests for transcripts
- Admissions – changes to applicant information
- Information Technology Services (ITS) – password/system access

IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the Law School considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The Law School identifies the following potential Red Flags in each of the listed categories:

A. Alerts, Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Receipt of a notice of address discrepancy in response to a credit report request.

B. The Presentation to the Law School of Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information; and
4. Application for service that appears to have been altered or forged.

C. The Presentation to the Law School of Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the student.

D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the Law School that a student is not receiving mail sent by the Law School;
6. Notice to the Law School that an account has unauthorized activity;
7. Breach in the Law School's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others

1. Notice to the Law School from a student, Identity Theft victim, law enforcement or other person that the Law School has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, Law School personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student's identity at time of issuance of student identification card.

B. Current Students

In order to detect any of the Red Flags identified above for an existing Covered Account, Law School personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, or via email); and
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes.

PREVENT AND MITIGATE IDENTITY THEFT

In the event Law School personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Continue to monitor the Covered Account for evidence of Identity Theft;
2. Contact the student or applicant;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Not open a new Covered Account;
5. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report ("SAR"); or
9. Determine that no response is warranted under the particular circumstances.

PROTECT STUDENT IDENTIFYING INFORMATION

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the Law School will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to Covered Account information are password protected;
4. Avoid use of social security numbers;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of student information necessary for Law School purposes.

PROGRAM ADMINISTRATION

Responsibility for this Program lies with an Identity Theft Committee ("Committee") for the Law School. The Committee is comprised of the Vice President for Finance and Business (Program Administrator), and the Director of Human Resources and Associate Dean for Student Affairs. The Program Administrator is responsible for ensuring appropriate training of Law School staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program. The Program Administrator or Committee shall report to President and Dean, at least annually, on compliance by the Law School with this Program.

Law School staff employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the Law School's failure to comply with this Program.

SERVICE PROVIDER ARRANGEMENTS

The Law School will take the following steps to ensure that service providers that perform activities with one or more Covered Accounts (i.e. University Accounting Services ("UAS"), collection agencies, student health insurance, TuitionPay/Sallie Mae, ELM) perform its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft:

1. Require that service providers have such policies and procedures in place; and
2. Require that service providers report any Red Flags to the Program Administrator or the Law School employee with primary oversight of the service provider relationship.

PROGRAM UPDATES

This Program was adopted by the Audit Committee of the Law School's Board of Trustees on May 5, 2009. The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the Law School from Identity Theft. In doing so, the Committee will consider the Law School's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the School's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.