

St. Lawrence University  
Identity Theft Program

Program:

The Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, requires financial institutions and creditors (including colleges and universities) to develop and implement an "Identity Theft Prevention Program". A college is considered a creditor if it participates in the Federal Perkins loan program, offers institutional loans, or offers a payment plan for tuition throughout the semester. Identity Theft means fraud committed or attempted using the identifying information of another person without authority and Red Flags are the activities which may signal attempted identity theft.

The University's Identity Theft Prevention Program shall, as appropriate, incorporate existing policies and procedures such as the Information Security Program. The employees responsible for coordinating the Information Security Program are also responsible for the administration and oversight of the Identity Theft Program.

Red Flags:

Potential "Red Flags" that university employees should pay careful consideration to when conducting university business include the following.

1. Notice or report from a credit agency indicating a discrepancy in information reported by the applicant or possible fraudulent activity on a credit account.
2. Presentation of identification documents that appear to be forged or inauthentic.
3. Presentation of identifying information that is inconsistent with other information on file or presented (examples: inconsistent birth dates or social security numbers).
4. Failure to complete personal identifying information on an application when reminded to do so.
5. Receipt of returned mail as undeliverable to student addresses that are on file.
6. Breach in the university's computer system security and/or detected unauthorized access to student account information.
7. Receipt of notice that someone with an account has been engaged in or victimized by Identity Theft.

Detection:

In order to detect any of the Red Flags described above, University personnel will take the following steps to verify identification of students.

1. Require certain identifying information be provided such as name, date of birth, academic records, home address.
2. Before issuing a student identification card, verify the student's identity by reviewing a driver's license or other government issued photo identification.

3. Verify the identity of a student or supporting parent if they request information on the student's account.
4. Verify the validity of requests to change billing addresses and banking information.

Prevention:

In the event that University personnel detect any identified Red Flags, one or more of the following steps, depending on the assessed degree of risk of Identity Theft, will be taken.

1. Monitor the account for other evidence of identity theft.
2. Contact the student.
3. Change passwords that permit access to covered accounts.
4. Provide student with a new identification number.
5. Notify law enforcement.
6. Determine that no response is warranted under the particular circumstances.

The VP of Finance will be consulted prior to notifying law enforcement of possible risks of Identity Theft.

In order to prevent the likelihood of Identity Theft occurring, the University's internal operating procedures include controls such as the following.

1. Ensure that the website is secure or provide clear notice that it is not secure.
2. Ensure complete and secure destruction of paper documents and computer files containing student account information.
3. Ensure that access to student account information is password protected.
4. Whenever possible, avoid use of social security numbers.
5. Ensure computer virus protection is up to date.
6. Require and keep only the kinds of student information that are necessary for University purposes.

Administration:

Responsibility for developing, implementing and updating the University's Identity Theft Program lies with the same employees designated to coordinate the University's Information Security Program. These employees will meet at least once year to discuss appropriate communication and training of staff, Red Flags identified during the year, if any, and steps taken to mitigate these, new prevention measures to consider, testing requirements, and any other issues relevant to the program.

The employees responsible for the Program will communicate the requirements of the Program to directors of departments impacted by the Program. Directors are responsible for training appropriate university staff in their departments regarding the requirements of this Program. Directors are also responsible for ensuring that any third party organization their department may use for services in connection with students accounts and loans comply with the FTC's Red Flags Rule. Such assurances will include written confirmation that service providers have policies and procedures in place to Identify

Red Flags and that service providers review the University's Program and report any Red Flags to the University employee with primary oversight of the service provider relationship.