## ST NORBERT COLLEGE

**IDENTITY THEFT PREVENTION PROGRAM**

## Program Adoption

St Norbert College developed this identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission's Red Flags Rule (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with oversight and approval of the Finance Committee of the Board of Trustees. After consideration of the size of the College's operations and account systems, and the nature and scope of the College's activities, the Board of Trustees determined that this Program was appropriate for St Norbert College, and therefore approved this Program in May, 2009.

## Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains 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 and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

## Definitions

**Identify theft** means fraud committed or attempted using the identifying information of another person without authority.

A **covered account** means:

1. An account that a creditor offers or maintains, primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions.
2. A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

## Covered Accounts

St Norbert College has identified six types of accounts, three of which are covered accounts administered by the College and three types of account that are administered by a service provider.

College covered accounts:

1. Refund of credit balances involving PLUS loans
2. Refund of credit balances, without PLUS loans
3. Deferment of tuition payments

Service provider covered account:

1. Tuition payment plan administered by TMS, refer to “Oversight of Service Provider Arrangements” on page 5.
2. On-line payments, administered by Sallie Mae, refer to “Oversight of Service Provider Arrangements” on page 5.
3. Perkins Loan balances, administered by University Accounting Services, refer to “Oversight of Service Provider Arrangements” on page 5.

## Identification of Relevant Red Flags

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts-- acceptance to the College and enrollment in classes requires all of the following information:
3. Common application with personally identifying information
4. High school transcript
5. Official ACT, SAT or TOEFL scores
6. High School Counselor or High School Teacher letter of recommendation
7. Entrance Medical Record
8. Medical history
9. Immunization history
10. Insurance waiver card or enrollment
11. Promissory and Disclosure Statement
12. The methods provided to access covered accounts:
    1. Disbursement obtained in person require picture identification
    2. Disbursements obtained by mail can only be mailed to an address on file
13. The methods provided that allow students to make an address change:

a. Address changes requested in person require picture identification

b. Address requests by phone require verification of College ID number or Social

Security number.

c. Address requests by mail only if accompanied with a payment stub.

1. The College’s previous history of identity theft. To date, none have been recorded.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-College issued E-mail account;
4. A request to make an address change via phone, and caller not able to provide College ID number or Social Security number.
5. A request to make an address change via mail, with no accompanying stub.
6. A request to mail something to an address not listed on file; and
7. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

## Detection of Red Flags

The Program will detect red flags relevant to each type of covered account as follows:

1. **Refund of a credit balance involving a PLUS loan** – As directed by federal regulation (U.S. Department of Education) these balance are required to be refunded in the parent’s name and mailed to their address on file within the time period specified. No request is required; however, a letter is sent to the parent requesting if they want this credit refunded or kept on the student’s account for future charges. The accompanied form needs to be completed and returned to the College. **Red Flag** – Request not coming from College generated form or signature on this form not the lenders.
2. **Refund of credit balance, no PLUS loan** – requests from current students must be made in person by presenting a picture ID, by mail with the College generated credit statement with completion of the College generated refund form, or in writing from the student’s college issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Refunds from students not currently enrolled or graduated from the college are generated by the College, and are mailed to the address on file. **Red Flag** – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.
3. **Deferment of tuition payment** – requests are made with a College generated form and require the student’s signature. **Red Flag** – none.
4. **Tuition payment plan** – Students must contact an outside service provider and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.
5. **On Line Payments** – Students must initiate the payment with the provider (Sallie Mae) and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.
6. **Perkins Loan Repayment** - Students must initiate the payment with the provider (University Accounting Service) and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.

## Response

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account (Knightline);
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

## Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the Vice President for Business and Finance. The Program Administrator will be responsible for the Program administration, for ensuring training of the appropriate College’s 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.

## Updating the Program

This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the College from identity theft. At least once per year in October, the Program Administrator will consider the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College'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 Program Administrator will update the Program.

## Staff Training

College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

## Oversight of Service Provider Arrangements

The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Currently, the College uses Tuition Management Services (TMS) to administer the Tuition Payment Plan, Sallie Mae to administer on-line payments, and University Accounting Service to administer the Perkins Loan repayment. Students contact these providers directly through its website or by telephone and provide personally identifying information to be matched to the records that the College has provided to said providers, if appropriate. In December 2008 a letter was sent and response has been received verifying that all three service providers have a Red Flag policy and are in compliance.