SAINT MARY'S COLLEGE
IDENTITY THEFT PREVENTION PROGRAM

SECTION I. BACKGROUND

1.1 The risk to Saint Mary's College (the "College"), its employees, students and customers from data loss and identity theft is of significant concern to the College and can be reduced only through the combined efforts of every employee.

1.2 The College adopts this identity theft prevention Program (the "Program") to help protect employees, students, customers, contractors and the College from damages related to the loss or misuse of sensitive information.

SECTION II. PURPOSE

2.1 To establish the 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 in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

2.2 The Program will:

(a) Define sensitive information;
(b) Describe the physical security of data when it is printed on paper;
(c) Describe the electronic security of data when stored and distributed;
(d) Place the College in compliance with federal law regarding identity theft protection;
(e) Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
(f) Detect risks when they occur in covered accounts;
(g) Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
(h) Update the Program periodically, including reviewing the accounts that are covered and the identified risks that are part of the Program.

SECTION III. DEFINITIONS

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

3.2 **Covered account** means:

(a) An account that the College offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, utility accounts, checking accounts and savings accounts; and
(b) Any other account that the College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of

the College from identity theft, including financial, operational, compliance, reputation or litigation risks.

3.3 **Sensitive information** includes the following items whether stored in electronic or printed format:

(a) Credit card information, including any of the following:
  (i) Credit card number (in part or whole);
  (ii) Credit card expiration date;
  (iii) Cardholder name;
  (iv) Cardholder address; and
  (v) Three digit security information.

(b) Tax identification numbers, including:
  (i) Social Security number;
  (ii) Business identification number; and
  (iii) Employer identification numbers.

(c) Payroll information, including, among other information:
  (i) Paychecks; and
  (ii) Pay stubs.

(d) Cafeteria plan check requests and associated paperwork.

(e) Medical information for any employee, customer or student, including but not limited to:
  (i) Doctor names and claims;
  (ii) Insurance claims;
  (iii) Prescriptions; and
  (iv) Any related personal medical information.

(f) Other personal information belonging to any customer, employee, student or contractor, examples of which include:
  (i) Date of birth;
  (ii) Address;
  (iii) Phone numbers;
  (iv) Maiden name;
  (v) Names; and
  (vi) Customer number.

3.4 College personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If employees are uncertain of the sensitivity of a particular piece of information, they should contact their supervisor.

3.5 **Electronic transfer information** includes:

(a) Account number; and
(b) Routing number.

3.6 **Personal check information** includes:

(i) Account number;
(ii) Routing number; and
(iii) Signature.

3.7 **Red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

SECTION IV. THE PROGRAM

4.1 The College establishes the Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

(a) Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program;
(b) Detect red flags that have been incorporated into the Program;
(c) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
(d) Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

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

SECTION V. IDENTIFICATION OF RELEVANT RED FLAGS

5.1 The Program shall include relevant red flags from the following categories as appropriate:

(a) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
(b) The presentation of suspicious documents;
(c) The presentation of suspicious personal identifying information;
(d) The unusual use of, or other suspicious activity related to, a covered account; and
(e) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

5.2 The Program shall consider the following risk factors in identifying relevant red flags for covered accounts as appropriate:

(a) The types of covered accounts offered or maintained;
(b) The methods provided to open covered accounts;
(c) The methods provided to access covered accounts; and
(d) Its previous experience with identity theft.

5.3 The Program shall incorporate relevant red flags from sources such as:

(a) Incidents of identity theft previously experienced;
(b) Methods of identity theft that reflect changes in risk; and
(c) Applicable supervisory guidance.

SECTION VI. DETECTION OF RED FLAGS

6.1 The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

(a) Alerts, notifications or warnings from a consumer reporting agency;
(b) A fraud or active duty alert included with a consumer report;
(c) A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
(d) A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

6.2 Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

(a) A recent and significant increase in the volume of inquiries;
(b) An unusual number of recently established credit relationships;
(c) A material change in the use of credit, especially with respect to recently established credit relationships; or
(d) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

6.3 Suspicious documents include the following:

(a) Documents provided for identification that appear to have been altered or forged.
(b) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
(c) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
(d) Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.
(e) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

6.4 Suspicious personal identifying information includes the following:

(a) Personal identifying information provided is inconsistent when compared against external information sources used by the College. For example:
    (i) The address does not match any address in the consumer report;
    (ii) The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
    (iii) Personal identifying information provided by the customer is not consistent with other personal identifying information provided by

the customer. For example, there is a lack of correlation between the SSN range and date of birth.

(b) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College. For example, the address on an application is the same as the address provided on a fraudulent application.

(c) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example:

(i) The address on an application is fictitious, a mail drop, or a prison; or

(ii) The phone number is invalid or is associated with a pager or answering service.

(d) The SSN provided is the same as that submitted by other persons opening an account or other customers.

(e) The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

(f) The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

(g) Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

6.5 Unusual use of, or suspicious activity related to, the covered account includes:

(a) Shortly following the notice of a change of address for a covered account, the College receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

(b) A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.

(c) A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

(i) Nonpayment when there is no history of late or missed payments;

(ii) A material change in purchasing or usage patterns

(d) A covered account that has been inactive for a lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

(e) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

(f) The College is notified that the customer is not receiving account statements.

(g) The College is notified of unauthorized charges or transactions in connection with a customer's covered account.

(h) The College receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the College

(i) The College is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

SECTION VII. RESPONDING TO RED FLAGS

7.1 Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the College from damages and loss.

(a) Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

(b) The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

(c) If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

(i) Canceling the transaction;

(ii) Notifying and cooperating with appropriate law enforcement;

(iii) Determining the extent of liability of the College; and/or

(iv) Notifying the actual customer that fraud has been attempted.

SECTION VIII. PERIODIC UPDATES TO PLAN

8.1 At periodic intervals established in the Program, or as required, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment.

8.2 Periodic reviews will include an assessment of which accounts are covered by the Program.

8.3 As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

8.4 Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the College and its customers.

SECTION IX. PROGRAM ADMINISTRATION

9.1 The Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.

9.2 The Program is the responsibility of the governing body. Approval of the initial plan must be appropriately documented and maintained.

9.3 Operational responsibility of the Program is delegated to the Controller.

9.4 Oversight of the Program shall include:

(a) Assignment of specific responsibility for implementation of the Program;
(b) Review of reports prepared by staff regarding compliance; and
(c) Approval of material changes to the Program as necessary to address changing risks of identity theft.

9.5 Reports shall be prepared as follows:

(a) Staff responsible for development, implementation and administration of the Program shall report to the Controller at least annually on compliance by the College with the Program.
(b) The report shall address material matters related to the Program and evaluate issues such as:
    (i) The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
    (ii) Service provider agreements;
    (iii) Significant incidents involving identity theft and management's response; and
    (iv) Recommendations for material changes to the Program.

9.6 Staff training:

(a) Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the College or its customers.
(b) The department head for each area is responsible for ensuring identity theft training for all requisite employees and contractors and ensuring their familiarity with this policy.
(c) To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Program are made.

9.7 Oversight of service provider arrangements:

(a) It is the responsibility of the College to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

(b) A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

(c) Any specific requirements should be specifically addressed in the appropriate contract arrangements.

9.8 Duties Regarding Addressing Discrepancies:

(a) The College shall develop policies and procedures designed to enable the College to form a reasonable belief that a credit report relates to the consumer for whom it was requested if the College receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report.

(b) The College may reasonably confirm that an address is accurate by any of the following means:
   (i) Verification of the address with the consumer;
   (ii) Review of the College's records;
   (iii) Verification of the address through third-party sources; or
   (iv) Other reasonable means.

(c) If an accurate address is confirmed, the College shall furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:
   (i) The College establishes a continuing relationship with the consumer; and
   (ii) The College, regularly and in the ordinary course of business, furnished information to the consumer reporting agency.