Vanderbilt University has adopted an Identity Theft Compliance (ITC) Program designed to prevent, detect and mitigate identity theft in connection with the creation and maintenance of covered accounts in compliance with all applicable legal and regulatory requirements.

Pursuant to that policy, the Office of Student Accounts and Student Loans has implemented the following operational policies and procedures.

1. **Relevant Red Flags.** "Each unit must identify and document the relevant red flags for covered accounts opened and/or maintained by the unit.[1]"

    a. The Office of Student Accounts and Student Loans has identified the following covered accounts:
        i. Federal Loans (such as the Perkins Loan program)
        ii. Institutional Loans
        iii. Student Account Deferral Agreements

    b. Student Accounts and Student Loans works with the following Service Providers that handle covered accounts on behalf of Vanderbilt University:
        i. Sallie Mae for the tuition payment service known as the "Vandy Plan"

2. **Program Design**. This identity theft compliance program considers the following risk factors in identifying relevant red flags for covered accounts:

    i. **Types** of covered accounts as noted above.

    ii. **Methods to open** covered accounts. Admission to Vanderbilt University and enrollment in classes is required to open one of the covered accounts listed above. Admission generally requires the following information:
        (1) Admission application with personally identifying information
        (2) Transcripts from high schools, colleges or universities
        (3) Official test scores (ACT, SAT, GRE, GMAT, MCAT, etc)
        (4) Letters of recommendation

    iii. **Methods to access** covered accounts.
        (1) Disbursements obtained in person require photo identification.
        (2) Disbursements obtained by mail are only mailed to the address of record.
        (3) Account inquiries are only allowed for individuals authorized for account access by the student. Identifying information is required to obtain account information.

    iv. **Previous history** of identity theft at the institution.

[1] Text in quotes comes from the Vanderbilt Identity Theft Prevention Policy

3. **Processes to Detect and Procedures to Respond to Red Flags**. "Implement and document processes to detect and procedures to respond to red flags when encountered in the course of operations."

   a. This program **identifies** the following red flags for this office:

      i. Suspicious Documents.
         (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 person presenting the identification.
         (3) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

      ii. Suspicious Personal Identifying Information
         (1) The Social Security Number[2] provided is the same as that submitted by other persons opening an account or other customers.

      iii. Notice of Possible Identity Theft
         (1) The financial institution or creditor 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.

   b. Detection of and Response to Red Flags. Admission to Vanderbilt University and enrollment in classes is required to open one of the covered accounts listed above. Red flags would be detected in the following situations:

      i. Suspicious Documents

         (1) Detection: For in-person requests for information or disbursements, the student identification card presented at time of request appears to be altered or forged.
            (a) *Response*: Staff logs into the student identification system to access the photograph of record for student in question. If the photographs are not consistent, access would be denied until other information is available to eliminate the red flag. Notifications would also be sent to the Dean of Students and the Card Office.

         (2) Detection: For in-person requests for information or disbursements, the photo identification of someone other than the student (parent, guarantor, etc) is presented at time of request appears to be altered or forged.
            (a) *Response*: Deny access to the covered account.

[2] Vanderbilt University uses a Student Account Identification number for access to account information.

(3) Detection: For in-person request, the photograph on the student identification card is not consistent with the appearance of the person presenting the identification.
   (a) *Response*: Deny access to the covered account, notify the Dean of Students, and notify the Card Office.

(4) Detection: For in-person request, the photograph on the photo identification of someone other than the student (parent, guarantor, etc) is not consistent with the appearance of the person presenting the identification.
   (a) *Response*: Deny access to the account.

(5) Detection: An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

   (a) *Response*: For the *Student Account Agreement* - Deny access to the account, contact the student, and contact the parent.

   (b) *Response*: For a *Student Loan application* – Applications for student loans do not flow through this office. Applications flow through the Office of Financial Aid and individual colleges and schools.

ii. Suspicious Personal Identifying Information
(1) The Social Security Number[3] provided is the same as that submitted by other persons opening an account or other customers.
   (a) Detection: For Student Accounts –
      (i) *Response*: Because of the way in which accounts are established by the Admissions Office, this does not occur.

   (b) Detection: For Student Loans –
      (i) *Response*: Because of the way in which accounts are established by the Office of Financial Aid, this does not occur.

iii. Notice of Possible Identity Theft
(1) The Office of Student Account and Student Loans 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.

   (a) Detection: If notified by a customer (student or other authorized individual), a victim of identity theft (current or former student), or any other person of a fraudulent account.
      (i) *Response*: Flag the account, have the customer give us a password to identify them, and advise them to contact the Vanderbilt Police Department.

[3] Vanderbilt University uses a Student Account Identification number for access to account information.

(b) Detection: If notified by a law enforcement authority
(i) *Response*: Flag the account; contact the customer for further instruction.

4. **Staff Training**. "Train (at implementation and on-going) new and existing staff regarding identity theft prevention and the unit's processes and procedures."

   a. All staff are trained to observe operating unit procedures regarding appropriate identification and potential red flags as listed above.

5. **Oversight of Service Provider Arrangements**. "Exercise appropriate and effective oversight of service provider arrangements. Any unit that contracts with a third party must obtain assurance from the contractor in writing that the contractor has identity theft policies and procedures in place at least equivalent to those of the unit."

   a. The Manager of Student Accounts oversees the relationship with Sallie Mae. Periodically (generally on an annual basis), Vanderbilt will review the vendor's identity theft program for suitability.

6. **Review Process**. "Review and update policies, processes, and procedures periodically to reflect changes in risk and previous experiences with identity theft."

   As a part of the Annual Reporting process (see below), this office will evaluate whether changes to the existing program are needed based on institutional risk and the office's previous experience with identity theft.

7. **Annual Reporting**. "Report, at least annually, on compliance to the Program Oversight Committee on the unit's program, its activities and, if necessary, incidents during the prior reporting period."

   By August 31 of each year, this office will submit a report to the Identity Theft Compliance Program Oversight Committee. The reporting period will be the fiscal year ending on June 30 each year.

   This office will address material matters related to the ITC Program and evaluate issues such as:

   - the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and maintaining existing covered accounts;
   - service provider arrangements;
   - significant incidents involving identity theft and this office's response; and
   - recommendations for material changes to the ITC Program.

   For service provider arrangements, the report will provide for confirmation of appropriate identity theft programs by the service provider and notification of any significant incidents and service provider's response occurring during the reporting period.