Vanderbilt University
Identity Theft Prevention Policy

Purpose
To establish and maintain an Identity Theft Prevention 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.

Policy
Each operating unit of Vanderbilt University that opens or maintains covered accounts is responsible for establishing and maintaining processes and procedures to prevent identity theft as well as detect and mitigate its effects in the event that identity theft prevention measures fail.

Definitions and Regulatory Terms
1. Covered Account – (a) An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. (b) Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.
2. Identify Theft – Fraud committed or attempted using the identifying information of another person without authority.
3. Operating Unit – A college, department, or other university or medical center unit.
4. Red Flag – A pattern, practice, or specific activity that indicates the possible existence of identity theft.
5. Service Provider – A person or organization that provides a service directly to the creditor.

Vanderbilt’s identity theft compliance program consists of two parts:
- an institutional responsibility for risk assessment and oversight, and
- operating unit responsibility for appropriate processes, procedures, training and reporting program activities.

Institutional Responsibilities

Governance. This policy is authorized by the institution’s Board of Trust.

Risk Assessment. Vanderbilt will periodically determine whether it offers or maintains covered accounts by means of a risk assessment taking into account the methods to open and access accounts, and previous experiences with identity theft. Program updates shall be implemented as appropriate based upon the results of each risk assessment.

Oversight. The Board of Trust delegates program oversight to the Program Oversight Committee, consisting of the Vice Chancellor for University Affairs, General Counsel, and Secretary of the University [chair], the Vice Chancellor for Administration, the Senior Vice President and Chief Financial Officer for Vanderbilt Medical Center, and the Assistant Vice Chancellor for Internal Audit and Risk Management.

Reporting. The Identity Theft Program Oversight Committee will report, at least annually, regarding compliance with this policy to the Audit Committee of the Board of Trust.
Vanderbilt University
Identity Theft Prevention Policy

Unit Requirements and Responsibilities
All units that offer or maintain one or more covered accounts are responsible for developing and implementing written policies and procedures to prevent, detect, and mitigate identity theft.

Necessary Elements. Each unit is responsible to:
- Identify and document the relevant red flags for covered accounts opened and/or maintained by the unit;
- Implement and document processes to detect, and procedures to respond to, red flags when encountered in the course of operations;
- Train new and existing staff regarding identity theft prevention and the unit’s processes and procedures;
- 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;
- Review and update policies, processes, and procedures periodically to reflect changes in risk and previous experiences with identity theft; and
- 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.

Related Policies
- OP 10-40.10: Response to Claims of Identity Theft
- Vanderbilt University Compliance Program (as revised 10/2006)
- HR-025: Electronic Communications Policy
  [http://hr.vanderbilt.edu/policies/hr-025.pdf]
- Computer Privileges and Responsibilities
  [http://www.vanderbilt.edu/aup.html]

References
Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (November 9, 2007 Federal Register, p. 63771 – 63773.)

Approval
Approved by the Vanderbilt University Board of Trust on May 1, 2009.