2703 Identity Theft Prevention

SECTION:	**INTERNAL CONTROLS**
EFFECTIVE:	**MAY 1, 2009**
REVISED:	
RESPONSIBLE OFFICE:	**VPAF**
APPROVAL:	**VPAF**

PURPOSE

In late 2007, the Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The regulation is intended to reduce the risk of identity theft by requiring stronger fraud prevention to protect consumers' personal data. The GTU is considered a "creditor" under terms of the regulations because it participates in the Federal Perkins Loan Program, offers institutional loans to students, and offers a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

This policy creates the program required by FTC regulations. In addition to the legal requirement for the GTU to have such a plan, the GTU is acting to protect the records covered under this policy in order to protect the privacy of its students, faculty, staff, vendors, donors and others. The GTU believes that it is prudent to make a concerted effort to safeguard personal and private information for all of its constituents given the increase in identity theft in recent years.

POLICY

This policy establishes the Identity Theft Prevention Program at the GTU, 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 includes reasonable policies and procedures to:

- Identify relevant red flags for covered accounts it offers or maintains, and incorporate those red flags into the program.
- Detect red flags that have been incorporated into the program.
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- Ensure the Program is updated periodically to reflect changes in risks to consumers 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.

Covered account means a consumer 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. Covered accounts include, but are not limited to, credit (debit) cards, loans, and unpaid or partially unpaid student accounts.

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

Creditor means any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month.

POLICY SECTIONS

2703.1 Administration

The Identity Theft Prevention Program Team shall be responsible for developing and implementing the Program.

The Identity Theft Prevention Program Team members shall train staff, as necessary, to implement the Program effectively within the individual departments' needs.

The Chair of the Identity Theft Prevention Program Team will provide a written report annually to the Vice President for Administration and Finance concerning annual activity and recommendations for continued administration.

Each department shall exercise appropriate and effective oversight of their service provider arrangements.

2703.2 Identification of relevant red flags

The GTU Identity Theft Prevention Program includes red flags from the following categories:

1) *Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.* Examples include a fraud or active duty alert that is included with a consumer report, presentation of notice of a credit freeze in response to a request for a consumer report, and a consumer report agency providing notice of address discrepancy.

2) *The presentation of suspicious documents.* This could include documents provided for identification that appear to have been altered or forged, documents that contain a photograph or physical description that is not consistent with the applicant or customer presenting the identification, or documents that are not consistent with readily accessible information that is on file.

3) *The presentation of suspicious personal identifying information.* Examples include personal identifying information provided that is inconsistent when compared against external information sources such as a social security number or address, the presentation of personally identifying information that is identical to that presented by another person, or the failure to provide all required personal identifying information.

4) *The unusual use of, or other suspicious activity related to, a covered account.* For example, an account that has been inactive for a lengthy period of time is used or, mail sent to a

customer is returned repeatedly although transactions continue to be conducted in connection with the customers covered account.

5) *Notice from "customers", victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.*

In addition, the GTU considers the following risk factors in identifying relevant red flags for covered accounts:

1) The types of covered accounts offered or maintained.

2) The methods provided to open covered accounts.

3) The methods provided to access covered accounts.

4) GTU's previous experience with identity theft.

The program also incorporates relevant red flags from sources such as incidents of identity theft previously experience, methods of identity theft that reflect changes in risk, and applicable regulatory or professional guidance.

2703.3 Covered accounts

The GTU considers the following types of accounts covered under the FTC Red Flag regulations. This list is by way of example and is not intended to be exhaustive.

1) Student accounts under a payment plan.
2) Student accounts participating in the Federal Perkins Loan Program
3) Student accounts participating in the emergency student loan program.
4) Student accounts with tuition and/or fees due after the start of classes.
5) Information contained on the NAE screen of Colleague.
6) The service provider covered accounts at ACS.
7) Credit card information (OIA).
8) Employee parking fees if paid in arrears.

2703.4 The detection of red flags

The Program addresses the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by obtaining identifying information about, and verifying the identity of, a person opening a covered account, and by authenticating "customers", monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

2703.5 Response

The Program shall provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed.

Appropriate responses may include:

1) Monitor a covered account for evidence of identity theft.

2) Contact the "customer".

3) Change any passwords, security codes or other security devices that permit access to a covered account.

4) Reopen a covered account with a new account number.

5) Not open a new covered account.

6) Close an existing covered account.

7) Notify law enforcement.

8) Determine no response is warranted under the particular circumstances.

2703.6 Updating the program

The Program shall be updated periodically to reflect changes in risks to "customers" or to the safety and soundness of the organization from identity theft based on factors such as:

- The experiences of the organization with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent and mitigate identity theft.
- Changes in the types of accounts that the organization offers or maintains.
- Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

OVERSIGHT OF THE PROGRAM

Oversight of the Program shall include:

- Assignment of specific responsibility for implementation of the Program.
- Review of reports prepared by staff regarding compliance.
- Approval of material changes to the Program as necessary to address changing risks of identity theft.

Reports shall be prepared as follows:

- Staff responsible for development, implementation and administration of the Program shall report to the Vice President for Administration and Finance at least annually on compliance by the organization with the Program.
- The report shall address material matters related to the Program and evaluate issues such as 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.