AMERICAN UNIVERSITY WASHINGTON, D.C.

University Policy: Identity Theft Prevention Policy

Policy Category: Ethics, Integrity and Legal Compliance Policies

Subject: Detection, prevention and mitigation of identity theft

Office Responsible for Review of this Policy: Office of Finance and Treasurer

Procedures: Developed within departments responsible for Covered Accounts

Related University Policies: Gramm-Leach Bliley Information Security Plan, American University Information Technology Security Policies

---

I. SCOPE

This Policy applies to the creation, modification, and access to Identifying Information from Covered Accounts connected to American University; including, but not limited to, the following:

- Federal Perkins Loan program
- Institutional loan programs
- Tuition payment plans
- Eagle Bucks program

II. POLICY STATEMENT

The purpose of this Identity Theft Prevention Policy is intended to comply with the Fair and Accurate Credit Transaction Act of 2003 in protecting American University customers from Identity Theft. The Policy is intended to establish procedures to facilitate the detection, prevention and mitigation of Identity Theft in connection with opening new Covered Accounts and activity in existing Covered Accounts.

This Policy does not replace or repeal any previously existing policies addressing some or all of the activities that are the subject of this Policy, but rather it is intended to supplement any such existing policies.

III. DEFINITIONS

When used in this Policy, the following terms have the meanings below, unless the context clearly requires that the term be given a different meaning:

Customer: The term "customer" means any individual (student, parent, faculty, staff, or other third party with whom the University interacts) who receives a financial service from the University and who, in the course of receiving that financial service, provides the University with Identifying Information about themselves.

Covered Account: The term "Covered Account" means an account that American University offers or maintains primarily for personal, family, or household purposes that involves or is designed to allow multiple payments of transactions. The term "Covered Account" also includes other accounts offered or maintained by the University for which there is a reasonably foreseeable risk of Identity Theft. Examples of Covered Accounts include Student accounts established for various transactions, and faculty/staff accounts established to process institutional loan transactions.

Identity Theft: The term "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

Identifying Information: The term "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number.

Red Flag: The term "Red Flag" means a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

IV. POLICY

Identification of Relevant Red Flags

American University has considered the guidelines and the illustrative examples of possible Red Flags from the FTC's Identity Theft Rules and has reviewed the University's history with instances of Identity Theft, if any. The University determined that the following are the relevant Red Flags for purposes of this Policy given the relative size of the University and the limited nature and scope of the services it provides to its customers.

A. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.

1. A fraud or active duty alert is included with a consumer report or an identity verification response from a credit reporting agency.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity that is 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.

B. The presentation of suspicious documents.

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. The presentation of suspicious personal identifying information, such as a suspicious address change.

10. Personal identifying information provided is inconsistent when compared against external information sources used by the University.
11. 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.
12. Personal identifying information provided is associated with known fraudulent activity as indicted by internal or third-party sources used by the University.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity. For example, the billing address on an application is fictitious, a mail drop, or a prison or the phone number is invalid or associated with an answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. The address and telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the Covered Account or the customer fails to provide all the required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

D. The unusual use of, or other suspicious activity related to, a Covered Account.

18. A Covered Account with a stable history shows irregularities.
19. Mail sent to the customer is returned repeatedly as undeliverable although usage of services continues in connections with the Covered Account.
20. The University is notified that the customer is not receiving paper account statements, if applicable.
21. The University is notified of unauthorized use of products or services in connection with a customer's Covered Account.

E. Notice of possible Identity Theft.

22. The University 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.

Detection of Red Flags

The employees of American University who interact directly with customers on relevant transactions shall have the initial responsibility for monitoring the information and documentation provided.

To detect any of the Red Flags identified above associated with opening of a new Covered Account, employees should take the following steps to obtain and verify the identity of the Customer opening a Covered Account:

- Require certain identifying information which may include but not limited to name, date of birth, AU ID; and
- Verify the person's identity.

To detect any of the Red Flags identified above associated with an existing Covered Account, employees should take the following steps to monitor transactions:

- Verify the identification of customers if they request information;
- Verify the validity of requests to change billing addresses; and
- Verify changes in banking information given for billing and payment purposes.

Management employees shall be responsible for making the final decision on any such unresolved Red Flag issues.

Response to Detected Red Flags

Once a potentially fraudulent activity is detected, an employee should gather all appropriate information and documentation regarding the alleged incident to the designated Management employee. The Management employee will make the determination if there was a fraudulent transaction. If a transaction is determinate to be fraudulent, appropriate action will be taken. Appropriate responses to prevent or mitigate Identity Theft when a Red Flag is detected include:

- Contacting the customer
- Closing an existing Covered Account
- Not attempting to collect on a Covered Account or not submitting the Account to a debt collection agency.
- Notifying the University's Security Plan Coordinator (x3284) or Chief Information Officer (x2612) for assistance with additional mitigation measurers.

Program Updates – Risk Assessment

The Policy, including relevant Red Flags, is to be updated as often as necessary but at least annually to reflect changes in risks to customers from Identity Theft. Factors to consider in the Policy update include:

1. An assessment of the risk factors identified in this Policy.
2. Any identified Red Flag weaknesses in associated account systems or procedures.
3. Changes in methods of Identity Theft.
4. Changes in methods to detect, prevent, and mitigate Identity Theft.

5. Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Training and Oversight

All staff and third-party service providers performing any activity in connection with one or more Covered Accounts are to be provided appropriate training and receive effective oversight to ensure that the activity is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

V. EFFECTIVE DATE:

This Policy is effective November 1, 2008; Last reviewed February 2009; December 2010

VI. SIGNATURE, TITLE, DATE OF APPROVAL

This Policy is effective November 1, 2008.

The initial adoption and approval of the Identity Theft Prevention Policy shall be by the Board of Trustees, or an appropriate Committee of the Board. Thereafter, senior management shall oversee the development, implementation, and maintenance of the Policy.

Approved by American University Board of Trustees: February 27, 2009
(Date approved)

Approved:

Donald L. Myers, Vice President of Finance and Treasurer

Date Approved: 2/27/09