THE UNIVERSITY OF GEORGIA IDENTITY THEFT PREVENTION PROGRAM

I. Overview

The University of Georgia (UGA) developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

II. Objective / Purpose

The purpose of this policy is to identify, detect, prevent and mitigate identity theft in connection with covered accounts (defined herein) operated by UGA.

III. Scope

The UGA Identity Theft Prevention Program applies to all faculty, staff, students, affiliates, prospective students, customers, contractors and sub-contractors who interact with UGA systems and processes, electronic or otherwise.

The requirements of this policy apply to UGA, its regional campuses and any third parties with whom UGA contracts to perform certain covered functions on its behalf.

IV. Definitions

Definitions mandated by Red Flags Rule Regulations:

A. Covered Account:

1) An account that UGA offers or maintains, primarily for personal, family, or household purposes, that involves or is designated to permit multiple payments or transactions, such as a credit card account, student account or other financial accounts; and

2) Any account that UGA maintains for which there is a reasonably foreseeable risk to customers from identity theft.

B. Identity Theft: Fraud committed using the personal identifying information of another person.

C. Personal Identifying Information: Any name or number used, alone or in conjunction with any other information, to identify a specific person including:

1) name

2) address
3) telephone number
4) social security number
5) date of birth
6) government issued driver's license
7) government issued identification number
8) alien registration number
9) government passport number
10) employer or taxpayer identification number
11) student identification number

D. Program Administrator: The individual designated with the primary responsibility for oversight of the program. See: Section IX.A.

E. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

F. Service Provider: A person that provides a service directly to UGA.

V. Identification and Detection of Red Flags

In order to identify relevant Red Flags, UGA and the Program Administrator shall consider the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access accounts, and its previous experiences with identity theft. The Program Administrator, in coordination with UGA departments and units, will identify a list (Red Flags List) of potential Red Flags that may indicate the existence of an identity theft in UGA covered accounts. The Red Flags List will be reviewed and amended by the Program Administrator as new Red Flags are discovered and identified.

VI. Detection of Identified Red Flags

In order to detect any of the Red Flags included on the Red Flags List, University personnel will take steps to obtain and verify the identity of the student or customer opening an account, transacting business within an existent account, or related to the use of consumer and/or credit checks in the personnel process. These steps may include, but are not limited to, the following:

A. New Covered Accounts:

1) Require relevant identifying information such as name, date of birth, home address and other necessary information; and
2) In the case of student enrollment, verify the student's identity at the time of issuance of student identification card by review of driver's license or other government-issued photo identification.

B. Existing Covered Accounts:

1) Verify identification of student or customer if they request information;
2) Verify validity of requests to change billing addresses by mail or email and provide the student of reasonable means of promptly reporting incorrect billing address changes; and
3) Verify changes in banking information given for billing and payment purposes.

C. Identifying Address Discrepancies in Consumer or Credit Report Requests

1) Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2) In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

VII. Response, Prevention and Mitigation of Detected Red Flags

In the event UGA personnel detect any Red Flags identified on the Program Administrator's Red Flags List, such personnel shall take appropriate actions depending on the type of Red Flag identified, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and other factors. These steps may include, but are not limited to, the following:

A. Cancel the transaction;
B. Continue to monitor a covered account for evidence of ongoing actions associated with Identity Theft;
C. Contact affected student or customer;
D. Change any passwords or other security devices that permit access to the covered account(s);
E. Do not open additional covered account(s);
F. Provide student/customer with new student identification number and/or account number;
G. Notify Program Administrator for determination of the appropriate step(s) to take;
H. Notify law enforcement when applicable; and
I. In appropriate situations, determine that no response is warranted under the specific circumstances.

VIII. Oversight of Third Party Service Providers

It is the responsibility of UGA to ensure that the activities of all service providers are conducted in compliance with the FTC Red Flags Rule. Before UGA may engage a service provider to perform an activity in connection with one or more of UGA's covered accounts, UGA must take the following steps to ensure the service provider performs its activities in accordance with FTC regulations:

A. UGA must require by contract that the service provider has such policies and procedures in place to achieve compliance with the FTC Red Flags Rule; and

B. UGA must require by contract that the service provider is aware of UGA Comprehensive Privacy Policy and Identity Theft Prevention Program, and will report to UGA any Red Flags it identifies as soon as possible.

IX. Program Administration

A. Program Administrator

As permitted by the Red Flags Rule regulations, responsibility for overseeing the administration of the Identity Theft Prevention Program has been delegated by the Board of Regents of the University System of Georgia by and on behalf of the Office of the President of the University of Georgia to the Director of the Internal Auditing Division (IAD).

IAD will be responsible for ensuring appropriate training of UGA staff on the Program, for reviewing any reports regarding detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Oversight

Successful implementation of this Program is dependent upon the cooperation of each UGA department, unit, and office that maintains covered accounts, and the UGA community as a whole. The Program Administrator, on an annual basis, will confer with UGA offices that maintain covered accounts to review compliance, training, policies, procedures and practices as they relate to this Program.

C. Training

UGA staff shall be trained, as necessary, to effectively implement the Program either by or under the direction of the Program Administrator in the identification and detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. At least annually, or as directed by Program

Administrator, UGA offices that maintain covered accounts shall report to the Program Administrator on compliance with the Program. The report should address such issues as effectiveness of the policies and procedures in addressing t he risk of identity theft in connection with covered accounts, service provider agreements, consumer or credit report requests, and any significant incidents involving indentify theft and management response.

D. Program Updates

By the delegated authority of the Board of Regents of the University System of Georgia, the Office of the President of the University of Georgia authorizes the Program Administrator to periodically review and update certain content of UGA's **Identity Theft Prevention Program**, to reflect changes in risk and the soundness of the Program generally. In doing so, the Program Administrator should consider specific incidents of identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in UGA's business and contractual arrangements with other entities. After considering these factors, the Program Administrator shall promptly notify the Office of the President and the UGA community of any changes to the Identity Theft Prevention Program.

X. References

A. Graham Leach Bliley Act

http://www.uga.edu/audit/glba/index.html

B. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

https://infosec.uga.edu/policies/hipaa.php

C. The Family Educational Rights and Privacy Act of 1974 (FERPA)

https://infosec.uga.edu/policies/ferpa.php

D. UGA Privacy Policy

https://infosec.uga.edu/policies/privacy.php

E. Identity Theft and Fraud Resources

https://infosec.uga.edu/sate/idtheft.php

F. What is Sensitive Information?

https://infosec.uga.edu/sate/sensitive.php

G. UGA Password Policy

https://infosec.uga.edu/policies/documents/UGA_Password_Policy_v3.8.4.pdf

H. Protection from disclosure social security number(s)

O.C.G.A §10-1-393.8

http://law.justia.com/georgia/codes/10/10-1-393.8.html

I. Laws Relevant to Information Security

https://infosec.uga.edu/policies/management/laws.php