December 2011

3.479 Identity Theft and Red Flags

Type of Policy ■ ***University*** □ ***Campus*** □ ***Department/Unit*** □ **Interim**	**Identity Theft and Red Flags Policy** **Policy 3.479**
Business Management Policies	**Effective date: October 31, 2009**

Policy History:	**Approved by:**	**Resolution**	**Date:**
	Board of Governors	**10.31.09:8**	**October 31, 2009**
Revised:			
Responsible Office:	**Responsible Administrator:**	**Contact information:**	**Applies to:**
Office of University Vice Chancellor / CFO	**Vice Chancellor / CFO**	**937-769-1304**	**All faculty, staff and students at all Units and Campuses of Antioch University**

I. Introduction and Purpose

The purpose of the Identity Theft Prevention Program is to provide information to assist individuals in detecting, preventing and mitigating identity theft in connection with a "covered account" or other university held account as well as provide guidance on reporting a potential security incident.

II. Background

In 2003, the US Congress enacted the Fair and Accurate Credit Transaction Act of 2003 ("FACTA") which required the Federal Trade Commission ("FTC") to issue regulations requiring "creditors" to adopt policies and procedures to prevent identity theft.

As a result, in 2007, the FTC issued a regulation known as the Red Flag Rule. The rule require" financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags.

The Red Flag Rule went into effect November 1, 2008 and enforcement of the rule begins August 1, 2009.

In addition, existing California law requires that any organization that owns computerized data that includes personal information shall disclose any breach of security of the system following discovery or notification of the breach in the security system to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Antioch University (the "university") is therefore adopting the following policy to adhere to the FTC regulation and provide a framework for reporting security incidents as required by California law.

III. Purpose and Scope

The purpose of the Identity Theft Prevention Program (the "program") is to ensure compliance with the FTC Red Flag Rules and California's Security Incident reporting laws. The Program will:

1. Identify relevant patterns, practices and activities dubbed "Red Flags," signaling possible identity theft;
2. Detect red flags;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the program is updated periodically to reflect changes in risks.

The FTC Red Flags Rule pertains to "covered accounts" as defined below. However, this Program will extend to all university accounts, whether financial or credit accounts, for which the university believes there is a reasonably foreseeable risk to the university, its students, faculty, staff or other constituents from identity theft.

These policies apply to all campuses and university departments within Antioch University. The campuses may choose to create additional guidelines that pertain to local policies and procedures, but those local policies cannot waive or replace any policy or procedure set forth herein.

IV. Definitions

Account – a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes.

Covered Account – The Red Flag regulations define the term "covered account" to mean:

(1) "an account that financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions…" ; and

(2) "any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers, or to the safety and soundness of the financial institution, or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks."

As noted above, for purposes of the university, a covered account shall extend to mean any university account or database for which the university believes there is a reasonably foreseeable risk to the university, its students, faculty, staff or other constituents from identity theft.

Credit – the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

Creditor – any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.

Examples that indicate a college or university is a creditor are:

1. Participation in the Federal Perkins Loan program;
2. Offering institutional loans to students, faculty or staff;
3. Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

Identity Theft – means fraud committed using the identifying information of another person.

Red Flag – a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Personal Information – Specific items of personal information identified in CA Civil Code Sections 1798.29 and 1798.3. This information includes an individual's first name or first initial and his or her last name in combination with any one more of the following data elements, when either the name or data elements are not encrypted or redacted: Social Security Number, driver's license/identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Security Incident – a collection of related activities or events which provide the evidence that personal information could have been acquired by an unauthorized person.

V. Identification of Red Flags

The following broad categories of Red Flags are potential indicators of warning signs of potential or actual identity theft or similar fraud. Any time a Red Flag, or a situation resembling a Red Flag, is apparent, it should be investigated for verification. The examples below are meant to be illustrative. Anytime an employee suspects a fraud involving personal information about an individual or individuals, the employee should assume that this program applies and follow the protocols established by his/her office for investigating, reporting and mitigating identity theft.

A. **Alerts** – alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies. In addition, unusual or inconsistent pattern of activity on a consumer report, such as an increase in inquiries, a number of new credit relationships, an account closed for cause or abuse, etc.

B. **Suspicious Documents** – such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.

C. **Suspicious Personal Identifying Information** – such as discrepancies in address, Social Security Number or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.

D. **Unusual Use or Suspicious Account Activity –** such as material changes in payment patterns, notification that the account holder is not receiving mailed statements, or that the account has unauthorized charges, change of address request followed by a request for additional authorized account users;

1. **Notice from Others Indicating Possible Identity Theft** – such as the institution receiving notice from a victim of identity theft, law enforcement, or another account holder reports that a fraudulent account was opened.

VI. Detection of Red Flags

Red Flags can be detected when opening new accounts as well as existing accounts by following the following procedures:

1. Obtaining and verifying identity;
2. Authenticating customers;
3. Monitoring transactions

A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the university or to a fraudulent web site may heighten the risk of identity theft and should be considered red flags.

VII. Responding to Red Flags

Once a Red Flag, or security incident, is identified, an employee must act quickly as a rapid response can protect customers and the university from the effects of identity theft. The employee should inform his or her supervisor as soon as possible after the actual or potential Red Flag, or a similar concern regarding identity theft, has been detected.

If it is determined that identity theft has occurred, the campus CFO as well as the University Vice Chancellor/CFO should be contacted immediately. The incident should be documented and retained in the relevant department files as part of the monitoring process of this Program.

If the Red Flag, or security incident, indicates that a fraudulent transaction has occurred, appropriate actions will be taken by the campus CFO or University Vice Chancellor/CFO as determined by the location and level of the fraud. Appropriate responses include, but are not limited to: canceling the transaction; not opening or closing the account in questions; notifying and cooperating with law enforcement; notifying appropriate senior management within the university; notifying the actual customer that fraud was attempted or occurred, changing passwords or other security devices that permit access to relevant accounts and/or databases; continued monitoring of the account or database for evidence of identity theft. In some cases it may be determined that no response is warranted after appropriate evaluation and consideration of the particular circumstances.

VIII. Training

Staff training is required for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the university or its customers.

The department head of each office that maintains a covered account under this program is responsible for ensuring that appropriate identity theft training for all requisite employees, officials and contractors occurs at least annually. As part of the training, all requisite employees, officials and contractors should be informed of the contents of the university's Identity Theft Prevention Program, and be provided with access to a copy of this document.

IX. Third Party Service Providers

The university remains responsible for compliance with the Red Flag Rules even if it outsources operations to a third party service provider. The written agreement between the university and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate that the service provider has been made aware of the university's Identity Theft Program and that they will report any Red Flags it identifies as soon as possible to the University Vice Chancellor and CFO.

X. Oversight of the Program

Responsibility for developing, implementing and updating this program lies with the Vice Chancellor and Chief Financial Officer. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of university's staff on the program, for reviewing any staff reports regarding the 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.

XI. Updating the Program

This program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the university from identity theft. At least once per year, the Program Administrator will consider the university's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the University maintains and changes in the university's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the program.

XII. Approval by the Board of Governors

Under the Red Flags Regulations, implementation and oversight of the program is the responsibility of the governing body or an appropriate committee of such governing body. Approval of the initial plan must be appropriately documented and maintained. After its initial approval of the program, however, the governing body may delegate its responsibility to implement and oversee the program. As the governing body of Antioch University, the Board of Governors, through its Governance Committee, as of the date above, hereby approved the initial Identity Theft Program. Having made such initial approval, the Board of Governors hereby delegates the responsibility for implementing, monitoring and overseeing the program to the Vice Chancellor and CFO.