


Name of Policy: <u>Identity theft detection, prevention, and mitigation.</u> Policy Number: 3364-15-12 Approving Officer: President Responsible Agent: Compliance Officer Scope: All University of Toledo Campuses			 Initial effective date: May 1, 2009
X	New policy proposal		Minor/technical revision of existing policy
	Major revision of existing policy		Reaffirmation of existing policy

(A) Policy statement

The University of Toledo will take appropriate action to detect, prevent, and mitigate identity theft associated with financial credit accounts.

(B) Purpose

Identity theft, including identity theft committed in order to obtain medical treatment, poses a risk to patients and students of The University of Toledo (the “university”), as well as the university. The university has established these reasonable policies and procedures to address the risks of identity theft to its patients, students, and other customers and to the safety and soundness of the university.

(C) Scope of policy

The requirements of this policy applies to all university departments that defer payment for services rendered and/or regularly extends, renews, or continues credit or regularly arranges for the extension, renewal, or continuation of credit.

(D) Definitions

All terms used in this policy that are defined in 16 C.F.R. 681.2 shall have the same meaning provided in that section.

(E) Establishment of an identity theft program

The university hereby establishes an identity theft program (the “program”) to detect, prevent, and mitigate identity theft in connection with the opening of covered accounts and existing covered accounts. The program shall enable the university to:

(4) Oversight of Service Providers. The university is ultimately responsible for compliance with 16 C.F.R. 681.2, even when it engages a service provider to perform an activity in connection with one or more covered accounts. Therefore, the university shall require each such service provider by contract to:

- (a) Abide by this identity theft policy and the program; and
- (b) Cooperate with the university to prevent or mitigate the risks of identity theft arising from red flags detected under the program.

(G) Identification, sources, and categories of red flags

The university shall look to any covered accounts it offers and maintains, the methods it provides to open and access those covered accounts, and any previous experiences with identity theft to identify relevant red flags under the program. It shall incorporate relevant red flags from sources including its past incidents of identity theft, changes in methods of identity theft, and any applicable laws, rules, or regulations. Categories of relevant red flags include:

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) Presentation of suspicious documents or suspicious personal identifying information, such as a suspicious address change;
- (3) Unusual use of, or other suspicious activity related to, a covered account; and
- (4) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with the university's covered accounts.

Examples of red flags from each category are attached to this policy as Appendix A. The university may choose which of these red flags to incorporate into its program, none are mandatory or prescriptive. Therefore, the university will incorporate into the program, whether singly or in combination, red flags from Appendix A that affect the risk of identity theft to the university, its covered accounts, and its patients, students, and other customers.

(H) Detecting red flags

The program shall detect red flags in connection with covered accounts by:

- (1) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, by presenting positive proof of identification (i.e. physically presenting photo ID, official government ID, or valid system credentials (user ID and password)); and
- (2) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts, through the following methods: presentation of positive proof of

identification.

(I) Responding to red flags (prevention and mitigation)

The university must act promptly and effectively to respond to red flags. To this end, the university shall utilize the following protocol:

- (1) Any person detecting a red flag shall immediately gather all related documentation, write a description of the incident, and report this information to the compliance and privacy officer.
 - (2) The compliance and privacy officer shall evaluate the incident and report his or her findings to the senior vice president for finance and administration.
 - (3) Not all detected red flags will require a response. If a response is warranted under the circumstances, then the compliance and privacy officer and the senior vice president for finance and administration shall take action appropriate to the level of risk presented. This action may include:
 - (a) Monitoring a covered account for evidence of identity theft;
 - (b) Contacting the customer;
 - (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
 - (d) Reopening a covered account with a new account number;
 - (e) Not opening a new covered account;
 - (f)
- (d)

The university shall comply with any other applicable legal requirements when implementing, operating, and updating the program.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>June 11, 2009</u> Date</p> <p><i>Review/Revision Completed by:</i> Compliance Officer</p>	<p>Policies Superseded by This Policy:</p> <ul style="list-style-type: none">• <i>None</i> <p>Initial Effective Date: May 1, 2009 Review/Revision Date: Next review date: May 1, 2012</p>
---	---

Appendix A

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
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, as defined in § 681.1(b) of this part.
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.

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.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the university. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The social security number (SSN) has not been issued, or is listed on the social security administration's death master file.

3364-15-12 Identity theft detect

- a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry);
or
 - b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
- a. Nonpayment when there is no history of late or missed payments;
 - b. A material increase in the use of available credit;
 - c. A material change in purchasing or spending patterns;
 - d. A material change in electronic fund transfer patterns in connection with a deposit account; or
 - e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The university is notified that the customer is not receiving paper account statements.
25. The university is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the University

- 26.