

3364-15-12 Identity theft detection, prevention and mitigation.**(A) Policy statement**

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

(B) Purpose of policy

UT’s identity theft program “the program” will detect, prevent, and mitigate identity theft in connection with new and pre-existing covered accounts. Additional information can be found on UT’s institutional compliance webpage.

(C) Scope

University colleges/units, including the medical center, that collect and maintain personal information for the purpose of allowing their customers to obtain goods, services or credit. Departments that process student loans, accounts receivable, patient financial accounts, medical records, gift shop credit accounts, tuition payment plans, parking permits, health insurance plans, memberships, etc., are among those to which this policy most directly applies.

(D) Administration the identity theft program

- (1) In administering the program, the compliance officer shall inform proper departments of any suspected identity theft. Examples of types of identity theft can be found on UT’s institutional compliance webpage.**
- (2) UT will exercise appropriate/effective oversight of service provider arrangements.**

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

The federal trade commission red flags rule requires organizations to implement an identity theft prevention program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations. UT defines “red flags” on its institutional compliance webpage.

UT 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. A covered account is generally:

- (1) An account that a 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; or
- (2) Any other account that poses a reasonably foreseeable risk to customers of identity theft. Further guidance on covered accounts is contained on UT's institutional compliance webpage.

(F) Prevention and mitigation of red flags/updating the program/other legal requirements/definitions

UT must act promptly to respond to red flags, as defined in paragraph (E) of this policy. UT shall comply with all legal requirements when implementing, operating, and updating the program. All terms in this policy have the same meaning as is defined in 16 C.F.R. 681.1.

(G) Procedure/references

UT's institutional compliance webpage:

<http://www.utoledo.edu/offices/internalaudit/pdfs/identitytheftdetectionpreventionandmitigationprocedures.pdf>

16 C.F.R. 681.1: <https://www.ecfr.gov/cgi-bin/text-idx?SID=510c40578b4aeb619f067a363ae7257&mc=true&node=pt16.1.681&rgn=div5>

Effective: 7/9/2018

CERTIFIED ELECTRONICALLY

Certification

06/29/2018

Date

Promulgated Under: 111.15
Statutory Authority: 3364
Rule Amplifies: 3364