3359-11-10.8 Identity theft detection, prevention and mitigation policy.

(A) Introduction. 11- e 0 J 0 Tw ( )Tj EMC,(nt)-7 e 0 /so3enTw ( )Tj EMC(i)2(gn.)]Td mw ( )Tj EtT
identity theft associated with financial credit accounts. The purpose of this policy is to enable appropriate university officials to develop and implement policies and procedures to address the risks of identity theft to its students, faculty, staff, vendors and other customers.

(2) This policy incorporates by reference university policies and procedures to the extent

University shall require each 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.

(F) Identification, sources, and categories of red flags.

(1) 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 applicable laws, rules, or regulations. Categories of relevant red flags include:

(a) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(b) Presentation of suspicious documents or suspicious personal identifying information, such as a suspicious address change;

(c) Unusual use of, or other suspicious activity related to, a covered account; and

(d) 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.

(2) 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, whether singly or in combinat

(Dtctectigr(d)-4( )-10(f)-1lcags

The pragram salldhetct red flags(i)-2(n c)4(on

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 immediately shall gather all related documentation, write a description of the incident, and report this information to the associate vice president and controller.

(2) The associate vice president and controller shaidS2(dS2(dS2 Tw [()-1(i)-2(0n)-2(on o)-6(i)-6(n)-3.9 I

(5) Changes in the university's business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

(J) Other legal requirements.

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

Replaces:	3359-11-10.8
Effective:	01/31/2015

(8) Personal identifying information provided is not consistent with personal identifying information that is on file with the university.

(9) If the University uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

(D)

(7) The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

(E) 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

(1) 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.